Contents

Disclosures

Because this is a white paper on law, I'm obligated to advise you the reader that I'm not a Lawyer and do not claim to be. This white paper is not meant to be all inclusive regarding cyber law. This document does not provide legal advice in any way. If you the reader feel like you need legal advice regarding cyber laws, it is recommended that you seek legal advice from a bar certified attorney.

The audience for this white paper is undergraduate students taking a Cyber Law introduction course. Because of this, the context in this document is not all inclusive. This is intended to give a foundation of some cyber concepts and potential legal concerns. Some laws in this paper may include many other provisions not covered because they are beyond the scope of an undergraduate cyber law class. I encourage you, the reader, to use this as a tool to get some ideas for further research into this subject.

Introduction

This white paper will provide some foundational knowledge of the tools we use to make sense of the information age that we live in. Then it will introduce laws that are put in place to regulate the information and the tools we use to manage that information. These laws will bridge civil and criminal statutes. It will demonstrate different levels of laws between state, federal, international, and non-US domestic. As we delve into this topic you will learn about laws that protect certain groups of people, certain types of information, and certain types of cyber actions. When you finish this white paper, you should have an introductory knowledge of cyber law.

Law Overview

Adjudication

Civil

In civil cases, adjudication involves resolving disputes between individuals or organizations over rights, obligations, and liabilities. Common examples include:

- Contract disputes
- Property disputes
- Family law matters (e.g., divorce, child custody)
- Tort claims (e.g., personal injury, defamation)

Criminal

In criminal cases, adjudication involves determining whether an individual accused of a crime is guilty or not guilty. Common examples include:

- Ransomware
- Identity Theft
- Cyber Espionage
- Credit Card Fraud

Jurisdiction

U.S.A. State Laws

The jurisdiction of U.S. state laws refers to the legal authority that individual states within the United States have to create and enforce laws within their own territories. Each state has its own legal system, which operates independently of the federal legal system, though both systems can sometimes overlap. The jurisdiction of U.S. state laws is defined by the state's territorial boundaries and extends to residents, property, and activities within those boundaries. States have broad authority to regulate a wide range of matters, including criminal, civil, family, and property law. While state laws operate independently, they must also coexist with federal laws, and conflicts between the two are resolved under the Supremacy Clause.

United States Federal Laws

These are laws that are domestic to the United States. These laws are at the national level. The jurisdiction of United States federal laws is defined by the U.S. Constitution and encompasses a wide range of areas. The federal government of the USA has jurisdiction over national matters and issues that cross state boundaries or affect the country as a whole. Federal jurisdiction is broad and encompasses a variety of legal areas, from constitutional issues to specific federal statutes and regulations. The U.S. Constitution and federal laws delineate the scope and limits of federal jurisdiction, ensuring a balance between federal and state powers.

International Law

International laws are agreements and treaties between countries. They are not enforced by a single global authority but are respected and enforced by the signatory countries. The jurisdiction of international law is a complex and multifaceted area that involves the rules and principles governing the relationships and interactions between sovereign states, international organizations, and, in some cases, individuals. International law governs the conduct of states and international entities, with jurisdiction based on principles like territoriality, nationality, and universality. It is enforced through a combination of international courts, diplomatic measures, and domestic legal systems. Despite its complexities and challenges, international law plays a crucial role in maintaining global order and addressing transnational issues.

Non-U.S. Domestic Laws

These are the laws of other countries, each with its own jurisdiction within its national boundaries. The jurisdiction of non-U.S. domestic laws refers to the legal authority and scope of laws enacted by countries other than the United States. Each country has its own legal system, which governs the conduct of individuals, businesses, and government entities within its borders. The jurisdiction of non-U.S. domestic laws is determined by a combination of territoriality, nationality, subject matter, and international agreements. Different countries have different legal systems, which influence how jurisdiction is applied and enforced. Understanding these principles is crucial for navigating legal issues in a globalized world.

Collisions

This is regarding multiple laws that provide provisions for the same mandates. In some cases, this causes collisions that require one of the conflicting laws to be authoritative. An example would be when the PATRIOT Act allows law enforcement to set aside protections awarded by FERPA and HIPPA.

One case where this would happen is if law enforcement needs to investigate potential terrorists on educational visas. The other case is law enforcement gaining access to biometrics and medical information to identify terrorists.

- USA Patriot Act
- The Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPPA)

Baseline

A baseline is the creation of a minimum level of legal obligation and regulation to achieve compliance. Take for instance a company that needs to adhere to multiple legal frameworks. For example, consider the teaching hospital at the University of Colorado. This university will need to adhere to both "Family Education Rights and Privacy Act" and "Health Insurance Portability and Accountability Act". Because of this someone for the University of Colorado is going to need to make a minimum level of legal obligation that fulfills the provisions of both acts. In some cases, the companies will create their security standards with this baseline as the minimum requirement for success to meet the obligations defined in the standards. If the company meets the security standards that are built on this baseline, essentially, they have met the obligations of each of these acts.

The following are some laws that you might need to consider when building a legal baseline for a medical school.

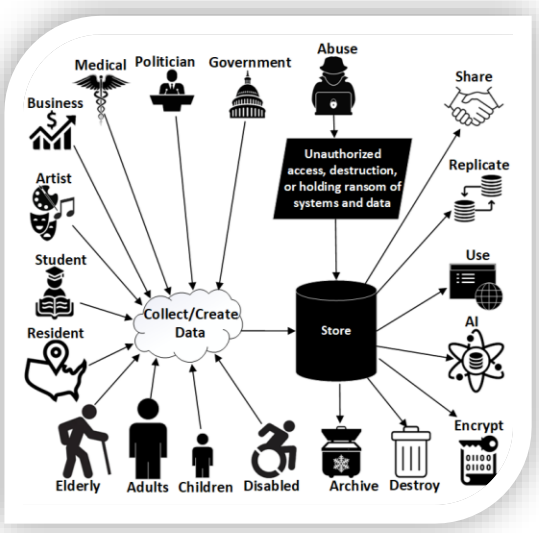
- The Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPPA)
- USA Patriot Act

Below here is an example of a potential legal baseline for the Colorado College medical school example. This also demonstrates potential collisions of different laws.

Legislation	Provision
The Family Educational Rights and Privacy Act (FERPA)	Privacy of educational records
The Family Educational Rights and Privacy Act (FERPA)	Provide parents and eligible students with the right to access and review educational records
The Family Educational Rights and Privacy Act (FERPA)	Control the disclosure of educational records to third parties
Health Insurance Portability and Accountability Act (HIPPA)	Privacy of health status, provided health care, and payment for health care
Health Insurance Portability and Accountability Act (HIPPA)	Limiting who can gain access to this information excluding the patient
USA Patriot Act	It authorizes the disclosure of educational records in the pursuit of terrorists
USA Patriot Act	It authorizes the disclosure of medical records in the pursuit of terrorists

Information Lifecycle

Like anything that lives on earth, information has its own lifecycle. Information can be created, stored, archived, used, replicated, shared, destroyed, and abused. This lifecycle drives a lot of our data security laws and standards. This next section will give you more details on this lifecycle and include any laws that you should consider regarding the different stages of the lifecycle. Please remember that this is not meant to be an all-inclusive list of every law that could apply. Also, many of these laws only apply in certain industries and use cases.



Collect/Create

This involves generating new data, which may be collected from individuals or groups, gathered via sensors (e.g., temperature probes, humidity gauges), or produced through data analysis (e.g., deep learning). Any action that introduces new data into a system constitutes data creation. We will also review laws protecting certain groups whose data is collected.

The following are some laws that you might need to consider for data collection.

- Gramm-Leach-Bliley Act
- Texas Identity Theft Enforcement and Protection Act
- Fair Credit Reporting Act
- Digital Millenium Copyright Act (DMCA)
- European Union - General Data Protection Regulation
- Singapore - Personal Data Protection Act (PDPA)
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)
- Brazilian - General Data Protection Law (LGPD)

Children

This is anyone under the age of 13. The following law applies to the collection, use, and sharing of data for children under the age of 13.

- Children's Online Privacy Protection Act (COPPA)

Adults

This is anyone that is over the age of 13. Even though some laws consider you an adult at the age of 18, in this context you lose protections awarded to children at the age of 13. This is the category of user that is awarded the least number of protections. Granted there are some protections granted to all users that this group is included in, just nothing specifically for them.

Elderly

This is anyone above the age of 65. Some criminal laws will increase the punishment for the criminal actor if the cyber-attack targeted an elderly person. It is looked at as an exacerbating factor.

- Ohio Unauthorized use of property - computer, cable, or telecommunication property
- Computer Fraud and Abuse Act

Disabled

This is anyone that has a mental or physical disability. Some criminal laws will increase the punishment for the criminal actor if the cyber-attack targeted a disabled person. It is looked at as an exacerbating factor.

- Americans with Disabilities Act (ADA)
- Ohio Unauthorized use of property - computer, cable, or telecommunication property

Residents

This is anyone that is a resident of a certain state within the USA. Some protections are awarded to you if you live in a state that has a data privacy act.

- California Consumer Privacy Act
- Colorado Privacy Act
- Massachusetts Data Security Regulations
- New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act
- Texas Identity Theft Enforcement and Protection Act
- Illinois Personal Information Protection Act

Students

This is anyone attending an educational institution regardless of age. In some cases, these laws also cover persons within an age group to be covered under mandated education laws, such as those under the age of 18. They may also provide language specific to student parents.

- The Family Educational Rights and Privacy Act (FERPA)

Artist

This is anyone that creates some form of art including but not limited to music, acting, painting, drawing, etc. This is the largest group of people impacted by piracy.

- Digital Millenium Copyright Act (DMCA)

Business

This is any company out there that collects information on their customers. There are many protections and regulations out there for businesses.

- European Union - General Data Protection Regulation
- Sarbanes Oxley Act (SOX)

Medical

Any form of data collected from all the different types of users that has to do with medical is protected. These provisions can be found in the following law.

- Health Insurance Portability and Accountability Act (HIPPA)

Politician

This is anyone that works as a politician. Some criminal laws increase the punishment for the criminal actor if the cyber-attack targeted a politician. It is looked at as an exacerbating factor.

- District of Columbia Protection of District public officials § 22-851
- Computer Fraud and Abuse Act
- European Union - General Data Protection Regulation
- UK General Data Protection Regulation

Government

This is any agency that works as a governing body of the nation, state, or community. Some criminal laws increase the punishment for the criminal actor if the cyber-attack targeted any government agency. It is looked at as an exacerbating factor.

- Alabama-2012-HB400
- Computer Fraud and Abuse Act
- USA Patriot Act

Store

This includes the short-term storage of data. This could be done actively in memory, statically on a storage drive, or statically in the cloud. Some laws regulate where this can be stored, how long it must be stored, protections required for storage, how access to this storage should be secured, and disclosure requirements for law enforcement.

The following are some laws that you might need to consider for data storage.

- New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act
- Health Insurance Portability and Accountability Act
- Gramm-Leach-Bliley Act
- European Union - General Data Protection Regulation
- Singapore - Personal Data Protection Act (PDPA)
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)

Archive

This is the long-term storage of data. This could be done actively in memory, statically on a storage drive, or statically in the cloud. Some laws regulate where this can be stored, how long it must be stored, protections required for storage, how access to this storage should be secured, and disclosure requirements for law enforcement.

The following are some laws that you might need to consider for data archive.

- Health Insurance Portability and Accountability Act (HIPPA)

- Gramm-Leach-Bliley Act
- European Union - General Data Protection Regulation

Use

This is the processing, viewing, analyzing, selling, purchasing, and general utilization of data. This activity is heavily regulated by various laws. There are laws regarding what a company can do with the data, who is legally allowed to access the data, the analytics that can be performed against the data, and many more.

The following are some laws that you might need to consider for data use.

- Gramm-Leach-Bliley Act
- Americans with Disabilities Act (ADA)
- Health Insurance Portability and Accountability Act (HIPPA)
- New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)
- Brazilian - General Data Protection Law (LGPD)

Share

This is the exchanging of data between a provider of data and a receiver of data. In some cases, this is a bidirectional exchange of data between two entities. This could also be a one-to-many relationship. For example, this could be one provider giving it to many receivers. This behavior also has many laws regulating who can legally provide and receive the data. In some cases when the data is monetized, it regulates things like what markets it can be sold to and other trade laws.

The following are some laws that you might need to consider for data sharing.

- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPPA)
- Digital Millenium Copyright Act (DMCA)
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act)
- USA Patriot Act
- Arms Export Control Act
- European Union - General Data Protection Regulation
- United Kingdom - General Data Protection Regulation
- Switzerland - Federal Act on Data Protection
- UK Terrorism Act of 2000
- UK Terrorism Act of 2006

Replicate

This is the duplication of data to make backup copies.

The following are some laws that you might need to consider for data replication.

- Digital Millenium Copyright Act (DMCA)
- California Consumer Privacy Act

- New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act

Destroy

This is the destruction of data. Some ways to do this include simple deletions, cryptographic erasure, or physical destruction. Either way you chose, you intended to achieve the same results. The level of level of destruction is dependent on the security classification of the data. The higher the risk of the data the more secure of destruction method you will need to use.

The following are some laws that you might need to consider for data destruction.

- California Consumer Privacy Act
- New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act
- European Union - General Data Protection Regulation

Encrypt

This is the conversion of plain text into cipher text using a cipher key. This renders the data unusable without decrypting the data. This prevents snooping on the data when at rest or in motion.

The following are some laws that you might need to consider for encryption.

- New York DFS
- Wassenaar Arrangement
- Digital Millenium Copyright Act (DMCA)
- Health Insurance Portability and Accountability Act (HIPPA)
- Trans-Atlantic Data Privacy Framework (DPF)

Abuse

This is the malicious attacks against the users, information, information systems, and applications by an adversary. This is the tactics and techniques deployed to gain an unfair strategic advantage over the victim. This could include espionage, extortion, privacy violations, theft, etc.

The following are some laws that you might need to consider for abuse.

- Computer Fraud and Abuse Act
- Computer Misuse Act
- Electronic Communications Privacy Act
- USA Patriot Act
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

Cloud

Recently the IT world was hit by a tidal wave. This technological evolution is the cloud. Per the NIST definition “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Since the cloud is only the abstraction and sharing of resources, the law that applied to traditional information systems and data also applies to cloud technology.

Globalization

This is the transmitting of data across national boundaries and the storage of data inside different countries. Global replication of your data allows the data to be available if other copies in other countries are destroyed. It also allows your remote offices in those countries to get quick access to the data since they are physically closer to it.

One major concern of global replication is data sovereignty. This is regarding the laws and regulations that countries have regarding data inside their country. This data is subject to the laws and regulations that govern the country where the data is being stored. This business model may need to adhere to the laws in the country the business is incorporated in, the laws in the country that is hosting the remote business, and any data trafficking laws that might apply to the data in transit.

Another scenario you need to consider is follow the sun support. Some businesses want to be able to support their customers 24 hours a day. The most cost-effective way to do this is to replicate your data in many countries across the globe and employ people near the data repositories to answer the calls when they come in. This would oblige you to adhere to every data sovereignty law in every country that you store or transmit your data.

The following are some laws that you might need to consider for globalization.

- Gramm-Leach-Bliley Act
- Wassenaar Arrangement
- European Union - General Data Protection Regulation
- United Kingdom - General Data Protection Regulation
- Trans-Atlantic Data Privacy Framework (DPF)
- Arms Export Control Act
- Switzerland - Federal Act on Data Protection
- UK Terrorism Act of 2000
- UK Terrorism Act of 2006

Artificial Intelligence

Artificial Intelligence (AI) refers to the field of computer science that focuses on creating systems or machines that can perform tasks typically requiring human intelligence. These tasks include learning,

reasoning, problem-solving, perception, language understanding, and decision-making. AI systems can be designed to mimic cognitive functions such as recognizing patterns, understanding natural language, and performing complex calculations.

The following are some laws that you might need to consider regarding feeding your data models to artificial intelligence.

- European Union – Artificial Intelligence Act (EU AI)

Sanctions

In this paper's context, a sanction is a punishment enforced on other countries by the United States for participating in or providing support for actions against the interests of the United States. This results in the prohibition of exchanging of items deemed contraband (hardware, software, data, etc.).

The following are some laws that you might need to consider when conducting international business.

- USA Patriot Act
- Wassenaar Arrangement

Munitions

These technologies are so advanced that if an adversary of the United States were to acquire them, it would allow them to substantially advance their abilities to attack the United States (also known as military grade technologies). This includes technologies like super-fast computers, photon computers, neural computing, quantum encryption ciphers, assault software, etc.

The following are some laws that you might need to consider when your product or service could be linked to technologies on the munitions grade export control lists.

- USA Patriot Act
- Wassenaar Arrangement

Breach Notifications

There currently isn't a single legal framework that specifically governs breach notification only. There are however laws inside of larger acts that address breach notification. There are also state breach rules that exist (here). Because of this, to fully understand your breach responsibilities, you must investigate these disparate laws to get the holistic view of the protections afforded to those they protect.

The following example laws cover the data that is protected under it, the conditions that trigger the breach notification, and in some cases a timeframe to notify the affected parties.

- HIPPA Breach Rules
    - 45 CFR §§ 164.400-414,
    - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
    - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
    - Individual Notification
        - "These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to

the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable)."hhs.gov

- Media Notification
  - "Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice."hhs.gov
- Secretary Notification
  - "If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach" hhs.gov
  - "If a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis." Hhs.gov

- Gramm-Leach-Bliley Safeguards Rule
  - https://www.federalregister.gov/documents/2023/11/13/2023-24412/standards-for-safeguarding-customer-information
  - "requires financial institutions to report notification events, defined as the unauthorized acquisition of unencrypted customer information, involving at least 500 customers to the Commission." federalregister.gov

Common Cyber Provisions

Through all the countries and their disparate laws, you will find some common threads regarding what they want enforced. Below is a list of a few common provisions.

1. Protected Data Subjects
2. Consent to collect
3. Opt Out
4. Purposeful Collection (aka Data Minimization)
5. Anti-collection Retaliation Prevention
6. Discrimination and Bias Protections
7. Right to access
8. Right to limit
9. Right to delete
10. Right to correct
11. Data Anonymization
12. Transparency in Processing Logic and Calculations

13. Privacy Framework Obligations
14. Monetization of data
15. 3rd party handling
16. Breach Notification Rules
17. Terrorism Obligations
18. Prohibited Exchange of Contraband
19. Exacerbating Factor Penalization
20. Computer Crime Penal Code

Conclusion

Cyber law is a broad topic with endless laws to review. It includes but is not limited to data privacy regulations and criminal code. This paper demonstrated how these laws apply to many concepts within information systems. We specifically covered the topics of data lifecycle, data sovereignty, protected data subjects, law collisions, and computer crime. All these topics and more are vital to understanding your legal and ethical responsibilities as an information security practitioner.

The data lifecycle showed us how laws apply to the data lifecycle phases. It raised awareness of the protected data subjects like children, disabled, elderly, students, artists, businesses, politicians, hospitals and government agencies. This also educated us on how laws apply to the different phases including collection, creation, storing, archiving, using, sharing and replicating of data. It then delved into more complex topics like data sovereignty, legal baselines and prohibited exchange of contraband.

To assure the core values of information security, we must understand all the different laws that apply to our use cases. We need to build security standards that account for all the applicable laws and collisions that these laws might have. This core should be used to build the remaining of your processes and procedures for the company. The goal is to use this baseline as the minimum bar of success when handling the data that your company needs to conduct business. The objective is to exceed this minimum to assure you are ready for the changes that will present itself in the future.

It is important that an information security practitioner has a foundational knowledge in cyber law to assure they are being ethical and legal with their actions. It is important that they understand the responsibility for laws within the origin state, origin country, destination country, destination state, and for laws governing exchanges across each border. In scenarios like follow the sun support and globalization, this task could be daunting.

To make this even more pain staking, these laws are constantly changing, so your company needs to be in a continuous state of research and evolution. This especially holds true with the example provided of the cross-border data trafficking laws between the United States and European Union. In the past few decades, these laws experienced multiple iterations of creating new laws, determined those created laws to be insufficient, and new laws created to replace them. To keep up with this, the information security practitioner will need to constantly sharpen their axe to cut out the old dead growth and then nurture the new growth that satisfies their current legal obligations.

The root theme to this paper is that companies need to protect the data. Ask yourself should you be collecting it? Is it mission critical to your purpose? If not, then do not collect it. If you absolutely need to collect it, then make sure you are taking every possible action to protect it. Do not wait for legal

provisions to tell you to be a good custodian. Just do it. Use the golden rule to help you decide. Think of it from the perspective of what would I want if it was a company collecting my data.

Appendix I – Law Catalog

Alabama-2012-HB400

https://legiscan.com/AL/text/HB400/id/640745/Alabama-2012-HB400-Enrolled.pdf

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

HB400 142837-2

Date Enacted

May 10th, 2012.

History

Alabama House Bill 400 (HB400), passed in 2012, is a piece of legislation aimed at protecting consumer privacy and enhancing the security of personal information within the state of Alabama. The bill was introduced in response to growing concerns over data breaches and identity theft, particularly regarding the protection of sensitive information handled by businesses and government entities. HB400 reflects Alabama's effort to join other states in adopting measures to safeguard personal information and provide clear guidelines on how to respond to data breaches.

What does it protect

This protects the residents and government of Alabama.

What does it enforce

This legislation covers many topics, but the reason why I'm including it in this paper is due to it demonstrates that laws are in place to protect the government. This law defines what is a computer

crime and then provides harsher punishments if these crimes are committed against a government agency.

Cyber Provisions

HB400 includes specific provisions related to cybersecurity, focusing on the protection of electronic data and the responsibilities of entities in the event of a data breach:

Encryption Requirements:

While not explicitly stated, the law implies the importance of encrypting personal information as a security measure. Data that is encrypted to industry standards may not trigger breach notification requirements if the encryption key remains secure.

Electronic Records Management:

Entities are required to maintain secure systems for handling electronic records containing PII. This includes implementing safeguards to prevent unauthorized access and ensuring that data is stored and transmitted securely.

Cyber Incident Response:

The law emphasizes the importance of having a response plan in place for cybersecurity incidents. Entities must act promptly to investigate breaches, mitigate harm, and notify affected individuals as required.

Coordination with Law Enforcement:

In the event of a significant data breach, entities may be required to coordinate with law enforcement agencies to ensure that the breach is properly investigated and that any criminal activity associated with the breach is addressed.

California Consumer Privacy Act

https://oag.ca.gov/privacy/ccpa

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

TITLE 1.81.5

Date Enacted

This was enacted on June 28, 2018 and amended on November 3rd, 2020.

History

The California Consumer Privacy Act was created based on the observations that technology was advancing, and the amount of data being collected was growing exponentially. Californians were also voicing concerns about the number of new breaches occurring. Since California has a large technology industry, they wanted to get ahead of the issue of data privacy asap. Legislators in California observed that the GDPR was just released which they used as inspiration for the new law. Since it was made law, several amendments have been made to it for refinement and expansion of powers.

What does it protect

This act specifically protects the residents of California only. This doesn't protect corporations or businesses. It also doesn't apply to any non-residents of California.

What Does it Enforce

This gives California residents more control of their personal information. This act requires for-profit businesses that operate in California to provide more transparency into what their consumers data is being used for and to give the consumers more control of their collected data.

Cyber Provisions

Right to know

This gives the consumer transparency into the information that the business collects on them.

Right to delete

This gives the consumer the ability to have the collected information destroyed.

Right to Opt-Out

This allows the consumer the ability to not participate in the sale or sharing of their personal information

Right to non-discrimination

This prevents business from discriminating against customers that chose to opt-out their personal information.

Right to correct

This allows the consumer to correct the information that was collected by the business.

Right to limit

This allows the consumer to selectively choose what personal information is allowed to be shared.

Colorado Privacy Act

Protect Personal Data Privacy | Colorado General Assembly

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

SB21-190

Date Enacted

July 7, 2021

History

In the wake of high-profile data breaches and scandals such as the Equifax data breach of 2017 and the Cambridge Analytica Scandal of 2018, consumers demanded increased protections for personal data. The Colorado Privacy Act (CPA) was enacted in response to the need for comprehensive protection regulations in the absence of an overarching federal data privacy legislation. The act was modeled on other successful state laws such as those of California and Virginia.

What does it protect

The CPA protects Colorado residents by granting the right to access, port, correct, delete and obtain a copy of their personal data. It also provides those citizens the right to opt out of the processing of personal data for targeted advertising, sale, or profiling.

What Does it Enforce

The act obligates businesses to provide clear privacy notices detailing data collection categories, processing purposes, and consumer rights. It also mandates data protection assessments, especially in regards to high-risk processing activities related to targeted advertising and the sale of personal data. It includes antidiscrimination language and provides language regarding data security requirements.

Specifically, the opt-in default requirement only applies to the processing of personal data for consumers under the age of 13. For children under 13, businesses must obtain verifiable parental consent before collecting or processing their personal data. This requirement aligns with the federal Children's Online Privacy Protection Act (COPPA).

The CPA authorizes the Colorado Attorney General and district attorneys to protect citizens' rights by enforcing the CPA via civil litigation, resulting in fines. The act does not grant individual consumers a private right of action, enforcement is solely the responsibility of the Attorney General and district attorneys. There are no criminal penalties for violations.

Cyber Provisions

The act applies to businesses that collect or process personal data of Colorado residents and meet certain thresholds, such as controlling or processing data of 100,000 or more consumers per year or deriving revenue from the sale of personal data from more than 25,000 consumers. The goal of this legislation is to ensure transparency, give individuals control over their personal information, and safeguard consumer privacy rights.

District of Columbia Protection of District public officials § 22-851

https://codes.findlaw.com/dc/division-iv-criminal-law-and-procedure-and-prisoners/#!tid=NF52BF780FD7211DB9C90DF511833162A

Jurisdiction

U.S.A. State Laws

Adjudication

Civil and Criminal

Legal Code or Statute

DC CODE § 22-851

Date Enacted

December 18, 2019

History

The "Protection of District Public Officials" law, codified as **D.C. Code § 22-851**, was enacted to address threats, intimidation, and harassment directed at public officials in Washington, D.C. The law aims to

ensure the safety and security of individuals serving in public office by criminalizing actions that interfere with or threaten their duties. This legislation is part of a broader effort to maintain public order and protect the integrity of governmental operations in the District of Columbia. It was implemented as a response to concerns about the increasing risks faced by public officials, particularly in light of rising political tensions and the potential for targeted violence.

What does it protect

The law protects a wide range of public officials within the District of Columbia, including but not limited to:

- Elected officials (e.g., the Mayor, members of the Council)
- Appointed officials (e.g., heads of departments and agencies)
- Judicial officers (e.g., judges)
- Law enforcement officers involved in the execution of their duties
- Government employees acting in an official capacity

The law extends protections to these individuals when they are performing their official duties or when they are targeted due to their official roles.

What Does it Enforce

The primary focus of D.C. Code § 22-851 is to criminalize actions that pose a threat to public officials or that obstruct their ability to perform their duties. The key provisions include:

1. Criminalization of Threats and Intimidation (D.C. Code § 22-851):

   The law makes it illegal to threaten, intimidate, or harass a public official with the intent to influence their actions, decisions, or duties. This includes any verbal or written threats that are directed at public officials because of their official status.

   Violation of this provision is considered a criminal offense and can lead to prosecution, with penalties that may include fines and imprisonment.

2. Obstruction of Official Duties:

   The law prohibits actions that obstruct or impede public officials in the performance of their official duties. This could include acts of physical interference, cyber harassment, or other forms of disruption that prevent officials from carrying out their responsibilities effectively.

3. Protection against Retaliation:

   The statute also protects public officials from retaliation for actions they have taken in their official capacity. This includes protection from threats or actions taken against them after they have made a decision, signed an order, or taken any official action that may be unpopular or controversial.

Cyber Provisions

While D.C. Code § 22-851 does not specifically mention "cyber" provisions, it is broad enough to cover threats and intimidation that occur through digital means, such as:

1. Cyber Threats and Harassment:

   The law applies to online threats, including those made via email, social media, or other digital platforms. Threatening or intimidating a public official through cyber channels is treated the same as physical or verbal threats under this law.

2. Digital Obstruction:

   Actions that digitally obstruct or impede a public official's ability to perform their duties, such as hacking, cyberstalking, or DDoS (Distributed Denial of Service) attacks on government systems, could be prosecuted under this statute if they target officials.

3. Electronic Communications:

   The statute's language is inclusive enough to cover communications made electronically, ensuring that public officials are protected from both traditional and modern forms of harassment and threats.

New York DFS

https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

23 NYCRR 500

Date Enacted

March 1, 2017

History

The regulation was introduced in response to the growing threat of cyberattacks on financial institutions and the need for robust cybersecurity measures to protect sensitive financial data. It was one of the first

comprehensive state-level regulations in the United States specifically focused on cybersecurity, aiming to strengthen the defenses of financial institutions operating within New York State. The regulation was developed after extensive consultation with industry stakeholders and experts to ensure that it effectively addressed the evolving cybersecurity landscape.

What does it protect

The regulation protects consumers, customers, and the overall financial system by requiring covered entities—such as banks, insurance companies, and other financial institutions regulated by the NYDFS—to implement stringent cybersecurity measures. The goal is to safeguard personal information, financial data, and other sensitive information from unauthorized access, data breaches, and cyber threats.

Covered Entities Include:

- State-chartered banks
- Licensed lenders
- Insurance companies
- Mortgage companies
- Other financial services firms regulated by NYDFS

What Does it Enforce

The NYDFS Cybersecurity Regulation enforces a wide range of cybersecurity requirements to ensure that covered entities have comprehensive and effective cybersecurity programs in place. Key provisions include:

- Cybersecurity Program (Section 500.02):

  Covered entities must establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of their information systems. This includes identifying and assessing cybersecurity risks, implementing appropriate security controls, and regularly testing the effectiveness of those controls.

- Cybersecurity Policy (Section 500.03):

  Entities must develop a written cybersecurity policy approved by the board of directors or a senior officer. The policy should address key aspects of cybersecurity, including data governance, asset management, access controls, and incident response.

- Chief Information Security Officer (CISO) (Section 500.04):

  Covered entities must designate a qualified individual to serve as the Chief Information Security Officer (CISO). The CISO is responsible for overseeing and implementing the cybersecurity program and reporting on its effectiveness to the board of directors.

- Penetration Testing and Vulnerability Assessments (Section 500.05):

  The regulation requires regular penetration testing and vulnerability assessments of information systems. Entities must conduct annual penetration tests and bi-annual vulnerability assessments to identify and address potential weaknesses in their systems.

- Multi-Factor Authentication (MFA) (Section 500.12):

  Covered entities are required to implement multi-factor authentication (MFA) for accessing internal systems and sensitive data. MFA is a security measure that requires more than one method of authentication to verify a user's identity, thereby reducing the risk of unauthorized access.

- Third-Party Service Provider Security (Section 500.11):

  The regulation mandates that covered entities assess and manage the cybersecurity risks posed by third-party service providers. This includes implementing policies to ensure that third-party providers meet the entity's cybersecurity standards.

- Incident Response Plan (Section 500.16):

  Entities must establish a written incident response plan to respond to and recover from cybersecurity events. The plan should outline the procedures for handling incidents, including the roles and responsibilities of key personnel, communication strategies, and post-incident reviews.

- Reporting of Cybersecurity Events (Section 500.17):

  The regulation requires covered entities to report any cybersecurity event that has a reasonable likelihood of materially harming the organization's operations or affecting its customers. Reports must be submitted to the NYDFS within 72 hours of the event.

Cyber Provisions

The NYDFS Cybersecurity Regulation is comprehensive in its focus on cybersecurity, addressing the full spectrum of risks that financial institutions face in the digital age. Key cyber provisions include:

- Encryption of Nonpublic Information (Section 500.15):

  Entities must implement encryption to protect nonpublic information both in transit and at rest. If encryption is not feasible, entities must implement alternative compensating controls to protect the data.

- Cybersecurity Awareness Training (Section 500.14):

  Covered entities are required to provide regular cybersecurity awareness training to employees. This training ensures that staff are aware of cybersecurity risks and the importance of safeguarding sensitive information.

- Continuous Monitoring (Section 500.06):

  Entities must implement continuous monitoring of their information systems to detect unauthorized access or other malicious activities in real time. This may include the use of automated tools to monitor network traffic and system activities.

- Risk Assessment (Section 500.09):

The regulation mandates periodic risk assessments to identify and evaluate cybersecurity risks. The results of these assessments should guide the implementation of cybersecurity controls and the overall cybersecurity strategy.

New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act

https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

https://legislation.nysenate.gov/pdf/bills/2019/S5575B

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

5575-B

Date Enacted

July 25, 2019

History

This act was put in place to strengthen New York's Information Security Breach and Notification Act.

What does it protect

This act specifically protects the residents of New York only. This doesn't protect corporations or businesses. It also doesn't apply to any non-residents of New York.

What Does it Enforce

SHIELD is a broad law that applies to any person or business that collects data on New York residents. This applies to all businesses and not just the ones inside of NY. This requires that protections are awarded to personal identifiable information. These protections must include physical and technological safeguards to prevent unauthorized access to the data. The law also defines breach notification requirements.

Cyber Provisions

Provisions

1. The company assigns responsible employees to maintain an Information Security program.
2. The company performs risk assessments.
3. The company regularly tests its security controls to verify they are working as expected.
4. The company has an information security educational program for their employees.
5. The company works with only 3rd parties that have been verified as providing the same level of protection as the company is required to fulfill.
6. The company verifies it is still meeting the information security requirements after a change has been made to the company.
7. The company is actively looking for risks with the following
    a. Network
    b. Applications
    c. IAM
        i. Authorization
        ii. Authentication
    d. Data Lifecycle
        i. data processing
        ii. data in motion
        iii. data at rest
        iv. data destruction.
8. The company has an incident response program to handle physical security, information security and information technology attacks/failures.
9. The company has a data retention policy and assures destruction after this period has expired.

Massachusetts Data Security Regulations

https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth/download

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

201 CMR 17.00

Date Enacted

March 1, 2010

History

Because of the atmosphere of high-profile breaches after 2000, Massachusetts legislators created the 2007 Massachusetts Data Security Law that required the creation of laws to protect personally identifiable information.

What does it protect

This protects Massachusetts residents and their personally identifiable information.

What Does it Enforce

This requires that companies that individuals that store or use personally identifiable information of Massachusetts residents protect that information that was entrusted to them.

Cyber Provisions

The companies and individuals collecting information from Massachusetts residents must do the following.

1. Create an Information Security program to protect the data by
    a. Designating employee(s) to maintain the program
    b. Perform risk assessments
    c. Develop policies to regulate the data lifecycle
    d. Impose punishments for policy violations
    e. Prevent unauthorized access to data
    f. Assure 3rd party affiliates honor the security practices of this program
    g. Maintaining physical security to prevent access to information systems
    h. Continuous review of the program to assure efficiency
    i. Verifying that security controls are affective and updating the control based on change
    j. Maintaining an incident response program to address issues that occur
    k. Maintain an identity and access management program to assure only authorized individuals can access the data.
    l. Encrypt all data at rest and in motion
    m. Maintain a monitoring and alerting program
    n. Maintain a currency program of your security controls and software
    o. Maintain a vulnerability management program
    p. Maintain an information security education program of your employees

Ohio Unauthorized use of property- computer, cable, or telecommunication property

https://codes.ohio.gov/ohio-revised-code/section-2913.04

Jurisdiction

U.S.A. State Laws

Adjudication

Criminal

Legal Code or Statute

Section 2913.04

Date Enacted

March 23, 2018

History

The rise of digital technology and telecommunications in the late 20th century led to an increased need for legal frameworks to protect against unauthorized access and misuse of computer systems and telecommunication networks. The statute was developed to address gaps in the law concerning the unauthorized use of computer systems and other forms of telecommunication property. The aim was to protect both private and public entities from unauthorized access that could lead to data breaches, fraud, and other forms of cybercrime.

What does it protect

The statute is designed to protect individuals, businesses, government entities, and service providers from unauthorized access to their computer systems, cable networks, and telecommunication services. This includes protection against hackers, unauthorized users, and those who misuse services without permission.

What Does it Enforce

Unauthorized Access: The statute makes it illegal to knowingly access or use a computer, cable service, or telecommunication service without the owner's consent. This includes accessing data, programs, or services for any purpose other than those authorized by the owner.

Tampering and Interference: The statute also prohibits tampering with or interfering with computer systems, networks, or telecommunication services in a way that disrupts or degrades their normal functioning.

Targeting Elderly or Disabled Victims:

If the offender knowingly targets an elderly or disabled individual in committing the offense, the penalties are elevated. This enhancement reflects the increased vulnerability of these populations and the state's intent to provide them with additional protection under the law.

Increased Penalties:

Enhanced Classification: The offense, when committed against an elderly or disabled person, may be elevated from a misdemeanor to a felony, depending on the circumstances of the case.

Harsher Sentences: The enhanced classification typically results in longer prison sentences, higher fines, and more severe legal consequences overall.

Cyber Provisions

Cybercrime Focus: The statute specifically targets cyber-related offenses by criminalizing unauthorized access to computer systems and networks. This includes hacking, data breaches, and other forms of cyber intrusion.

Application to Digital and Online Activities:

Data Access and Theft: The statute applies to situations where individuals unlawfully access and extract data from computer systems, including personal information, financial data, and proprietary information.

Service Misuse: Unauthorized use of cable and telecommunication services, such as intercepting or tapping into cable lines or phone networks, is also covered under this law.

Texas Identity Theft Enforcement and Protection Act

https://law.justia.com/codes/texas/business-and-commerce-code/title-11/subtitle-b/chapter-521/subchapter-b/

Jurisdiction

U.S.A. State Laws

Adjudication

Civil and Criminal

Legal Code or Statute

TITLE 11 CHAPTER 521

Date Enacted

April 1, 2009

History

The Texas Identity Theft Enforcement and Protection Act (TITEPA) was enacted in 2005 as part of a broader effort to combat the growing problem of identity theft in Texas. The act was introduced to strengthen the state's response to identity theft, providing clear guidelines for businesses, public entities, and individuals regarding the protection of personal information. The legislation has since been amended to adapt to evolving cybersecurity challenges and the increasing prevalence of data breaches.

What does it protect

TITEPA protects individuals residing in Texas from identity theft by safeguarding their personal identifying information (PII). PII includes any data that can be used to identify an individual, such as Social Security numbers, driver's license numbers, financial account numbers, and other sensitive information. The act applies to businesses, state agencies, and other entities that collect, maintain, or use the personal information of Texas residents.

What Does it Enforce

TITEPA enforces several key provisions aimed at preventing identity theft and protecting personal information:

Protection of Personal Information (Tex. Bus. & Com. Code § 521.052): Businesses and other entities must implement reasonable procedures to protect the personal information they collect, use, and maintain. This includes taking steps to prevent unauthorized access, use, or disclosure of PII.

Notification of Breach (Tex. Bus. & Com. Code § 521.053): In the event of a data breach involving unencrypted or unredacted PII, entities must notify affected individuals promptly. The notification must be made as quickly as possible and without unreasonable delay, except in cases where law enforcement requests a delay to avoid compromising an investigation.

Destruction of Records (Tex. Bus. & Com. Code § 521.052(b)): Entities must dispose of records containing PII in a manner that renders the information unreadable or undecipherable, such as shredding, erasing, or otherwise modifying the information.

Civil Penalties (Tex. Bus. & Com. Code § 521.151): Violations of TITEPA can result in civil penalties. The Texas Attorney General has the authority to bring civil actions against entities that fail to comply with the act. Penalties can include fines of up to $500 per violation, with a maximum of $50,000 per breach, or more if the violation is deemed to be intentional.

Right to File a Civil Suit (Tex. Bus. & Com. Code § 521.151(b)): Individuals affected by identity theft may file a civil lawsuit against the entity responsible for the violation, seeking damages for any financial losses incurred as a result of the breach.

Cyber Provisions

TITEPA includes specific provisions related to cybersecurity, focusing on the protection and secure handling of electronic data:

1. **Encryption Requirements (Tex. Bus. & Com. Code § 521.002(a))**: The act emphasizes the importance of encrypting PII to protect it from unauthorized access. If a data breach involves encrypted information, the notification requirements may not apply, as long as the encryption key has not been compromised.
2. **Data Breach Notification (Tex. Bus. & Com. Code § 521.053)**: The act mandates that businesses and government entities notify individuals if their unencrypted personal information is exposed due to a cybersecurity breach. The notification must include details about the breach, the type of information exposed, and steps that individuals can take to protect themselves.
3. **Electronic Records and Disposal (Tex. Bus. & Com. Code § 521.052(b))**: TITEPA requires that entities securely dispose of electronic records containing PII. This involves ensuring that data is permanently deleted or rendered inaccessible, preventing recovery by unauthorized parties.
4. **Coordination with Law Enforcement (Tex. Bus. & Com. Code § 521.053(d))**: The act allows for delays in breach notification if law enforcement determines that immediate disclosure would impede a criminal investigation. This provision ensures that cybersecurity breaches can be investigated thoroughly without compromising the integrity of law enforcement efforts.

Illinois Personal Information Protection Act

https://idfpr.illinois.gov/content/dam/soi/en/web/idfpr/banks/cbt/welcnews/news/2007/personalinfoprotectionact.pdf

https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67

Jurisdiction

U.S.A. State Laws

Adjudication

Civil

Legal Code or Statute

815 ILCS 530

Date Enacted

January 1, 2006

History

This law is a product of the many recent breaches that have occurred. The Illinois legislature decided to take action to protect their residents from unauthorized access to their personally identifiable information. This made Illinois the second state to enact laws regulating breach notification requirements.

What does it protect

This act protects residents of Illinois. It does not apply to non-residents of Illinois.

What Does it Enforce

Businesses that conduct operations in Illinois must comply with this law. This law obligates the company to protect its collected personally identifiable information. This law also requires that the company communicates any unauthorized access to personally identifiable information.

Cyber Provisions

This act doesn't prescribe obligations for the company to take to prevent a breach. It only provides provisions after a breach has occurred.

Provisions

1. If any non-public unencrypted personal identifiable information is accessed without authorization the company must provide notification to the data subject.
2. The notification must be provided at no cost to the data subject.
3. The notification can only be delayed if it interferes with the law enforcement investigation.
4. The notification must be sent as soon as legally possible to the data subject
5. The notification must be sent in either written, electronic, or other method depending on what is the most efficient method to deliver this to the data subject.

Americans with Disabilities Act (ADA)

https://www.ada.gov/law-and-regs/ada/

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil

Legal Code or Statute

Title 42 Chapter 126

Date Enacted

July 26, 199

History

The Americans with Disabilities Act (ADA) was signed into law on July 26, 1990, by President George H.W. Bush. It was a landmark civil rights law aimed at eliminating discrimination against individuals with disabilities, similar to protections provided to individuals on the basis of race, color, sex, national origin, age, and religion. The ADA was modeled after the Civil Rights Act of 1964 and the Rehabilitation Act of 1973, particularly Section 504, which prohibited discrimination against people with disabilities in programs receiving federal financial assistance. The ADA has been amended several times, with significant updates under the ADA Amendments Act of 2008 (ADAAA), which broadened the definition of disability.

What does it protect

The ADA protects individuals with disabilities, defined as those who have a physical or mental impairment that substantially limits one or more major life activities. This includes people who have a history of such an impairment, or who are perceived by others as having such an impairment. The law protects these individuals from discrimination in various areas of public life, including employment, public services, public accommodations, transportation, and telecommunications.

What Does it Enforce

The ADA enforces broad protections across several key areas:

Employment (Title I): (42 U.S.C. §§ 12111–12117), the ADA prohibits discrimination against qualified individuals with disabilities in all aspects of employment, including hiring, promotion, compensation, and termination. Employers with 15 or more employees are required to provide reasonable accommodations to employees with disabilities, unless doing so would cause undue hardship.

Public Services (Title II): (42 U.S.C. §§ 12131–12165) prohibits discrimination against individuals with disabilities in public services, programs, and activities, including those provided by state and local governments. This includes ensuring accessibility in public transportation, government buildings, and services.

Public Accommodations (Title III): (42 U.S.C. §§ 12181–12189) prohibits discrimination in public accommodations, such as restaurants, hotels, theaters, retail stores, and private schools. Businesses

must make their facilities accessible to individuals with disabilities and remove barriers where it is readily achievable.

Telecommunications (Title IV): (42 U.S.C. § 225) requires telephone and internet companies to provide nationwide relay services that allow individuals with hearing or speech disabilities to communicate over the phone.

Miscellaneous Provisions (Title V): (42 U.S.C. §§ 12201–12213) includes various provisions, including protection from retaliation for asserting ADA rights and clarification that the ADA does not override other federal, state, or local laws that provide equal or greater protection.

Cyber Provisions

The ADA's applicability to the digital world has been an evolving area, particularly with the rise of the internet and digital communication. While the original ADA did not explicitly address websites and digital accessibility, courts and regulatory agencies have increasingly interpreted the law to apply to digital spaces:

1. **Website Accessibility (Title III)**: Courts have ruled that Title III's requirements for public accommodations apply to websites, especially those associated with physical places of business. This means that websites must be accessible to individuals with disabilities, such as by providing text alternatives for images (for the visually impaired) and ensuring that navigation can be performed via keyboard (for individuals with motor impairments).
2. **Web Content Accessibility Guidelines (WCAG)**: While not explicitly part of the ADA, the Department of Justice and courts often refer to the WCAG as a standard for ensuring websites are ADA-compliant. The WCAG provides guidelines on how to make web content more accessible to people with disabilities.
3. **Mobile Applications**: Similar to websites, mobile apps provided by businesses must also be accessible to individuals with disabilities. This includes ensuring that apps can be used with screen readers, offer alternative text, and are navigable by users with various disabilities.
4. **Telecommunications (Title IV)**: The ADA requires telecommunications services to be accessible to individuals with disabilities, which has been extended to include modern communication technologies. This includes captioning for video services, and text-to-speech functionality.

The Family Educational Rights and Privacy Act (FERPA)

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html#:~:text=The%20Family%20Educational%20Rights%20and,privacy%20of%20student%20education%20records.

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil

Legal Code or Statute

20 U.S.C. § 1232g; 34 CFR Part 99

Date Enacted

August 21, 1974

History

The 1960s saw a rise in awareness about personal privacy, partly driven by the advent of new technologies. In the 1970s, concerns over the privacy of educational records emerged against a backdrop of increased data collection and surveillance, reflecting broader anxieties about personal privacy. For example, the **Nixon Administrations landmark Supreme Court case that** addressed privacy issues related to presidential records, reflecting broader concerns about personal data and privacy (Nixon, 1977). Reports, such as the 1972 U.S. Advisory Committee on Family Educational Rights (The Hew Report), highlighted significant deficiencies in how educational institutions managed student records, including inadequate privacy protections and unauthorized access (U.S. Advisory Committee on Family Educational Rights, 1972).

Student social activism and protests during this period underscored the misuse of educational records, with instances of institutions using such records to monitor and retaliate against politically active students, further amplifying privacy concerns (Schroeder, 1974). These issues galvanized legislative action, leading to the enactment of the Family Educational Rights and Privacy Act (FERPA) in 1974. FERPA aimed to address these deficiencies by establishing clear guidelines for record access, restricting unauthorized disclosure, and enhancing overall privacy protections (U.S. Department of Education, 2024).

What does it protect

FERPA applies to all educational institutions that receive funds from the U.S. Department of Education. It is designed to safeguard the privacy of educational records for specific groups. Primarily, FERPA protects current and former students of educational institutions that receive federal funding. FERPA specifies access and control of all student information is retained by the parents of underage children and subsequently by students of legal age. This includes ensuring that students have the right to access and review their own education records, control the disclosure of these records to third parties, and request amendments to records they believe are inaccurate or misleading (U.S. Department of Education, 2024).

FERPA's protections are linked specifically to institutions that receive federal funding, leaving private institutions that do not receive such funding outside its scope. This means that while many educational settings are covered by FERPA, those not benefiting from federal funds are not legally required to adhere to its privacy standards. Some of these institutions may still choose to implement similar privacy

measures or adhere to state regulations that offer comparable protections. This funding-based approach has been criticized for potentially leaving gaps in privacy protections for students in non-federally funded institutions, suggesting that FERPA's reach might not fully address privacy concerns across all educational environments (Bennett & Dervan, 2015).

What Does it Enforce

FERPA mandates that educational institutions receiving federal funding must provide parents and eligible students with the right to access and review education records, request amendments to records they believe are inaccurate or misleading, and control the disclosure of these records to third parties. Institutions must obtain written consent from parents or eligible students before releasing personally identifiable information from education records, except under specific circumstances such as to school officials with legitimate educational interests or in response to a legal order (U.S. Department of Education, 2024).

The U.S. Department of Education's Family Policy Compliance Office (FPCO) is responsible for enforcing FERPA. If a school fails to comply with FERPA, parents and eligible students can file a complaint with the FPCO. Institutions found in violation may face the loss of federal funding and accreditation, which can significantly impact their operations and financial stability (Schroeder, 1974). While FERPA does not specify criminal penalties, the potential financial repercussions underscore the importance of adherence to its provisions.

Cyber Provisions

The main requirements are detailed in the who and how of FERPA. The law governs educational institutions, students, and parents. Annual notification of FERPA rights to students and parents is obligatory, detailing their rights regarding access, amendment, and disclosure of information. Additionally, institutions must maintain stringent safeguards to protect the confidentiality and security of education records, implementing appropriate administrative, technical, and physical measures (U.S. Department of Education, 2024).

Cybersecurity Implications

FERPA has significant cybersecurity implications for educational institutions, necessitating robust measures to ensure compliance and protect sensitive student information. While not specifically mandated by FERPA, evolving and robust cybersecurity controls are necessary to comply with broader language protecting the confidentiality and integrity of education records. Institutions must implement comprehensive data security practices, including encryption and secure access controls, to safeguard these records from unauthorized access and breaches (U.S. Department of Education, 2024).

Effective access management involves enforcing multi-factor authentication, role-based access controls, and continuous monitoring to detect potential intrusions. Institutions also need to develop and maintain incident response plans to manage data breaches, including procedures for breach identification, containment, notification, and remediation (Bennett & Dervan, 2015). Addressing cybersecurity requirements is crucial for protecting student privacy and maintaining institutional trust.

Gramm-Leach-Bliley Act

https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6801&edition=prelim

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

15 U.S.C. §§ 6801-6809, §§ 6821-6827

Date Enacted

November 12, 1999

History

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, emerged from decades of changes in the financial industry since the Great Depression. One goal of the GLBA was to reform the Glass-Steagall Act of 1933, which had mandated the separation of commercial banking, investment banking, and insurance companies to prevent another economic crisis. However, increasing international financial integration and competitive pressures led to calls in the financial sector for repealing these separation requirements.

In 1999, just before the GLBA was enacted, Citicorp, a commercial bank, merged with Travelers Group, an insurance company, to form Citigroup, a conglomerate in violation of Glass-Steagall. The Federal Reserve granted a waiver for this violation, highlighting regulatory leniency. The push for deregulation was further driven by technological advancements and the industry's desire to modernize its operations and offerings, leading to the eventual repeal of these legacy restrictions.

Who does the law impact

This act introduced multiple changes that benefited different groups, primarily the finance and insurance industries, and private citizens. The changes put in place by this act provided strategic restructuring for current financial institutions. It also introduced privacy protections for consumers' personal financial information.

What Does it Enforce

The act requires that financial institutions establish privacy policies and requires that these policies are disclosed to their customers. It requires the institution identify how it will fulfill these policies of protecting its customers' sensitive data. Then it requires that these methodologies of restricting access to customer personal data be put into practice. This act established regulation enforcement authority for the Federal Reserve, Office of the comptroller of the Currency, and state insurance regulators.

Important Cyber Provisions

Privacy (Title V, Subtitle A)

This part of the law establishes multiple requirements for the institutions to follow. It requires institutions to provide customers privacy notices that includes their information collection, sharing, and use policies. It also requires that the customers are made aware of who could potentially be the receiver of their personal information. Finally, this requires that the institution provides a method for the consumer to opt-out of sharing their information with third parties.

Safeguards (Title V, Subtitle A)

This part of the law requires institutions to create an information security program. It requires the institution to document this information security program in the company's policy and standards. This program should be specifically created to secure the consumer's personal information that was entrusted to them. The companies are required to perform a risk assessment to identify and remediate gaps in their information security program. The goal here is to have continuous improvement of the security needed to protect the consumer data and the company as a whole. Finally, this rule requires that the same protections are extended to the data that is utilized by any third-party affiliate that the company choses to share it with.

Pretexting (Title V Subtitle B)

This part of the law prohibits obtaining personal information under false pretenses. This requires that they guard against unauthorized access to customer information. This necessitates the need to identify people that are requesting access to the data and also verifying they are authorized to gain this access.

Health Insurance Portability and Accountability Act (HIPPA)

https://www.congress.gov/bill/104th-congress/house-bill/3103/text

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

H.R.3103

Public Law 104-191

Date Enacted

August 21, 1996

History

It is stated that the Health Insurance Portability and Accountability Act (HIPPA) was created to make the coverage between different jobs comparable. It was also driven by the need to have the health insurance coverage applied to pre-existing medical conditions. These changes caused the cost to increase for the insured, so congress also amended the act to resolve fraud, waste, and abuse. Because of advancements in technology this information was being transacted digitally which brought about the need for additional privacy provisions to be put in place to address the risks of these advancements.

What does it protect

This act specifically provides protections to the insured. It protects the insured by giving them a guarantee of coverage in most cases and also protects their private health information. Even though it isn't a protection, this act does give the insurance companies help through addressing fraud, waste, and abuse. It also provides the employer assistance through tax breaks.

What Does it Enforce

Title I - Health Care Access, Portability, and Renewability

Title II - Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform

Title III - Tax-related health provisions governing medical savings accounts

Title IV - Application and enforcement of group health insurance requirements

Title V - Revenue offset governing tax deductions for employers

Important Cyber Provisions

Protected Health Information was defined as health status, provided health care, and payment for health care. This requires this type of information to be guarded as private. This requires limiting who can gain access to this information excluding the patient, allows the ability for the patient to correct the information, and for the patient to be able to acquire any accounting details. Portions of this law require that entities maintain an information security program, employ information security practitioners to run their program, train their employees on security mandates, and establish an incident response program.

Additionally regulated entities are required to have physical security policies that limit physical access to the data and limit physical access to the facilities. limit the systems

Digital Millenium Copyright Act (DMCA)

https://www.govinfo.gov/content/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

PUBLIC LAW 105–304—OCT. 28, 1998 H.R. 2281

17 USC 101, 17 U.S.C. § 512, 17 U.S.C. § 1201-1202

Date Enacted

October 12, 1998

History

The Digital Millenium Copyright Act (DMCA) was enacted in direct response to two treaties, the "WIPO Copyright Treaty of 1996" and "Performances and Phonograms Treaties Implementation Act of 1998." These treaties were a response to the transformative impact of the internet and digital media on the distribution and protection of copyrighted works. These treaties required member states to update their copyright laws to address digital challenges and improve international copyright protection. Rapid proliferation of digital formats in the late 1990's, such as CDs and MP3s, coupled with the emergence of peer-to-peer networks like Napster, facilitated widespread unauthorized copying and sharing of content, posing significant challenges to traditional copyright enforcement (Samuelson, 1999).

These technological advancements and international obligations were compounded by economic pressures from the entertainment industry, which faced substantial revenue losses due to digital piracy. Existing U.S. copyright laws were not adequately equipped to handle the complexities introduced by digital technology. These pressures coupled with international treaty requirements led to Congressional action, and with the input of diverse stakeholders, a comprehensive set of regulations emerged as the DMCA.

What does it protect

Various stakeholders, including copyright holders including creators and organizations, technology companies, OSP's including platform and internet service providers, and consumer advocacy groups, were involved in the legislative process. Their input helped shape the provisions of the DMCA to balance different interests. The DMCA addressed these challenges by implementing anti-circumvention provisions to protect digital rights management systems and establishing safe harbor provisions to limit the liability of online service providers, thereby balancing the interests of copyright holders, technology companies, and consumers (Litman, 2001, 122-130).

However, the DMCA has faced substantial criticism regarding its effectiveness and fairness. Critics argue that the anti-circumvention provisions are overly restrictive, impeding legitimate activities such as security research and educational use (Samuelson, 1999). Furthermore, the notice-and-takedown system has been criticized for being prone to abuse, where content can be removed without proper verification of infringement, potentially silencing legitimate speech and stifling innovation (Litman, 2001, 80-90). These issues highlight significant flaws and loopholes in the DMCA, affecting its capacity to balance the interests of copyright holders with the broader public good.

What Does it Enforce

The DMCA is aimed at regulating digital copyright protection and online content management. Among these are the anti-circumvention provisions and the safe harbor protections for online service providers. Specifically, Sections 1201 and 1202 of the DMCA prohibit the circumvention of technological protection measures (TPMs), such as digital rights management (DRM) systems, and address the removal or alteration of copyright management information (CMI) intended to facilitate copyright infringement (United States Copyright Office, 1998). These provisions are designed to safeguard the integrity of digital content and prevent unauthorized access and distribution.

Section 512 provides safe harbor protections for online service providers (OSPs), limiting their liability for user-uploaded content, as long as they follow the DMCA's notice-and-takedown procedures. This requires OSPs to act promptly if they receive a valid notice of infringement to maintain their immunity from liability (Litman, 2001). The DMCA also includes specific exclusions, such as exemptions for reverse engineering aimed at interoperability and certain academic and research activities, so long as these do not infringe on copyrights (United States Copyright Office, 1998). However, these provisions are not intended to stifle legitimate uses of copyrighted material that fall under fair use or similar exemptions. For instance, activities such as reverse engineering for interoperability, academic research, or criticism that involve bypassing TPMs but do not infringe on the copyright holder's rights are not covered by the DMCA's prohibitions (Ginsburg, 1997, pp 90-100).

Penalties for violating the DMCA's anti-circumvention provisions can be severe, including both civil and criminal penalties. Civil remedies may involve statutory damages ranging from $200 to $2,500 per work infringed, while criminal violations can lead to fines up to $500,000 and imprisonment for up to five years for repeat offenders (Litman, 2001, 80-90). These penalties underscore the DMCA's rigorous enforcement framework aimed at protecting intellectual property in the digital age.

Cyber Provisions

The DMCA requires adherence to several specific requirements to implement protections. Copyright holders must issue formal DMCA takedown notices to OSPs to address alleged infringements. These notices must contain specific details, including a description of the copyrighted work and the location of the infringing material, and must be accurate to avoid potential liability for damages (17 U.S.C. § 512(c)(3).

OSPs seeking to benefit from safe harbor protections under Section 512 must follow established notice-and-takedown procedures. This involves promptly removing or disabling access to the alleged infringing material upon receiving a valid notice from a copyright holder. Additionally, OSPs must designate and register an agent with the U.S. Copyright Office to handle DMCA notices, and must also manage counter-notices if users dispute the removal of content (17 U.S.C. § 512(c)(1)(C).

Compliance with the DMCA's anti-circumvention provisions is mandatory for all parties. Section 1201 prohibits the bypassing of technological protection measures (TPMs) that safeguard copyrighted works. This prohibition extends to both individuals and organizations, and includes not distributing tools designed for circumvention. However, the Act acknowledges certain exemptions, such as those for interoperability and non-commercial research, which allow for specific non-infringing uses of copyrighted material (17 U.S.C. § 1201). Noncompliance can result in significant penalties for copyright holders, OSPs, and consumers.

Fair Credit Reporting Act

https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf

https://www.ecfr.gov/cgi-bin/text-idx

https://www.law.cornell.edu/uscode/text/15/1681

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

15 U.S.C § 1681

Date Enacted

October 26, 1970

History

The Fair Credit Reporting Act (FCRA) is a U.S. federal law enacted to promote fairness, accuracy, and privacy in the consumer credit reporting industry. Its enactment was a response to growing concerns about the consumer credit reporting industry's lack of transparency, accuracy, and privacy protections.

Several legal cases underscored these concerns, such as *Ralph J. Sarver v. Experian* (1968), where the plaintiff sued for damages caused by inaccurate credit reporting, demonstrating the need for consumer access to their credit information and mechanisms to correct errors Similarly, *Jones v. Credit Bureau of Huntington* (1968) emphasized the necessity for consumer consent before sharing personal credit information, further stressing the importance of privacy protections.

The act identifies its purpose as solidifying public trust in the banking system. It specifies the need to ensure that consumer reporting agencies report information with "fairness, impartiality and a respect for the consumer's right to privacy."

What does it protect

The FCRA established essential rights for consumers, setting the stage for more robust consumer protection laws in the financial sector. Over the years amendments such as the Fair and Accurate Credit Transactions Act (FACTA) of 2003 have enhanced consumer rights by providing free annual credit reports and measures against identity theft and regulatory bodies like the CFPB have strengthened its provisions, reflecting the ongoing importance of consumer rights in credit reporting.

What Does it Enforce

The FCRA creates an extensive set of rules and definitions on the construction and use of credit reports.

Accuracy of Information:

- Credit reporting agencies are required to "follow reasonable procedures to assure maximum possible accuracy" of the information they report (15 U.S.C. § 1681e(b)).
- Agencies must promptly correct or delete inaccurate, incomplete, or unverifiable information after a consumer dispute (15 U.S.C. § 1681i(a)).
- Consumer Access and Dispute Rights: Consumers have the right to obtain a free credit report annually from each of the three major credit reporting agencies (15 U.S.C. § 1681j(a)).
- Consumers can dispute inaccuracies, and agencies must investigate disputes within 30 days, extending to 45 days if additional information is provided by the consumer (15 U.S.C. § 1681i(a)).

Privacy and Data Security:

- The FCRA limits access to credit reports to those with a "permissible purpose," such as creditors, insurers, employers (with consent), and landlords (15 U.S.C. § 1681b).
- Employers must obtain written consent from job applicants or employees before accessing credit reports for employment purposes (15 U.S.C. § 1681b(b)(2)).

Notification Requirements:

- Consumers must be notified when information in their credit report has been used to take adverse action against them, such as denial of credit, employment, or insurance (15 U.S.C. § 1681m(a)).
- Adverse action notices must include the name, address, and phone number of the credit reporting agency that provided the report, as well as information about the consumer's right to obtain a free copy of the report and dispute its accuracy (15 U.S.C. § 1681m(b)).

Limitations on Reporting:

- The FCRA limits the reporting of adverse information, such as bankruptcies (10 years) and other negative items (generally 7 years), to prevent outdated information from influencing credit decisions (15 U.S.C. § 1681c(a)).

Identity Theft Protections:

- Consumers can place fraud alerts and credit freezes on their credit reports to prevent identity theft (15 U.S.C. § 1681c-1).
- Credit reporting agencies are required to block fraudulent information resulting from identity theft within four business days of receiving appropriate documentation from the consumer (15 U.S.C. § 1681c-2).
- These provisions collectively ensure that credit reporting agencies are held accountable for maintaining the accuracy, privacy, and security of consumer information, thereby safeguarding consumer rights and promoting fair credit practices.

Child Support Provisions:

- The FCRA specifies that state and local child support enforcement agencies may access a consumers credit report for the purpose of establishing, modifying, or enforcing child support obligations (15 U.S.C. § 1681b(a)(4)).
- These agencies may use the information found on consumer reports to verify income, determine the amount of support payments and the consumer's ability to pay, to locate a delinquent parent and to negatively impact a report for support arrearage.

Rules for Special Circumstances:

- The FCRA Restricts sharing of medical information in credit reports.
- Establishes limitations and right of notification for investigative reports covering information about a consumer's character, reputation, or lifestyle.
- Assigns limitations for the use of consumer reports for the purpose of marketing.
- Requires Adverse Action Notices to consumers when the information in the report has been used to take adverse action against a consumer.

Cyber Provisions

The FCRA specifies a number of requirements for Credit Reporting Agencies (CRAs), furnishers of information, and consumers.

CRA's:

- Must provide a free and up-to-date credit report for individual consumers once per year.
- With some exceptions, must obtain consumer permission prior to sharing credit information.

- Must provide consumers with notification if a credit report is used to deny credit or in the event of other negative reporting.
- Only release credit reports or information to authorized entities with consumer consent.
- Allow consumers to restrict their private information through security freezes and fraud alerts.
- Requirement to allow consumers to dispute inaccurate information. They are further required to investigate, correct or remove any inaccuracies within 45 days of notice.
- Obtain written consent for use of credit reports for employment purposes.
- Provide employment applicants with a copy of the report and summary of their rights before taking adverse action based on the report.

Furnishers of Information:

- These are (definitions apply) generally banks, businesses, corporations, collections agencies, and other entities that enact contracts of debt with consumers.
- Must provide accurate information and promptly correct any inaccuracies when discovered, or when notified by consumer.

Consumer Requirements:

- Consumers are required to regularly review and maintain the accuracy of their credit reports.
- They should understand and exercise their rights under the FCRA

Sarbanes Oxley Act (SOX)

https://www.govinfo.gov/content/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

Public Law 107-204

Date Enacted

July 30, 2002

History

The Sarbanes-Oxley Act (SOX) was enacted in response to a series of high-profile corporate scandals, including those involving Enron, WorldCom, and Tyco. These scandals highlighted significant lapses in corporate governance, financial reporting, and auditing practices. The act was named after its sponsors, Senator Paul Sarbanes and Representative Michael Oxley, and was designed to restore public confidence in the financial markets by improving corporate accountability and transparency. SOX introduced rigorous reforms to enhance financial disclosures, prevent accounting fraud, and establish stronger oversight of public companies and their auditors.

What does it protect

SOX primarily protects investors by ensuring the accuracy and reliability of corporate financial statements. It also protects the broader public and employees by enforcing higher standards of corporate governance and accountability. The act applies to all publicly traded companies in the United States, including their executives, boards of directors, and auditors. It also extends to foreign companies that are listed on U.S. stock exchanges.

What Does it Enforce

SOX enforces a range of provisions aimed at improving corporate governance, financial transparency, and the integrity of financial reporting:

1. **Corporate Responsibility for Financial Reports (Section 302, 15 U.S.C. § 7241)**: SOX requires senior executives, including the CEO and CFO, to personally certify the accuracy and completeness of the company's financial reports. False certification can result in severe penalties, including fines and imprisonment.
2. **Internal Control Requirements (Section 404, 15 U.S.C. § 7262)**: SOX mandates that companies establish and maintain an adequate internal control structure for financial reporting. Management must assess the effectiveness of these controls annually and disclose their findings in the company's financial reports. External auditors are required to attest to the accuracy of management's assessment.
3. **Enhanced Financial Disclosures (Section 409, 15 U.S.C. § 7261)**: Companies are required to provide timely and accurate disclosures of material changes in their financial condition or operations. This includes off-balance-sheet transactions, pro forma figures, and use of special purpose entities.
4. **Audit Committee Responsibilities (Section 301, 15 U.S.C. § 78j-1)**: SOX strengthens the independence and responsibilities of audit committees within corporate boards. The audit committee is directly responsible for the appointment, compensation, and oversight of the company's external auditors.
5. **Whistleblower Protections (Section 806, 18 U.S.C. § 1514A)**: SOX provides protection for employees who report fraudulent activities or violations of securities laws. Companies are prohibited from retaliating against whistleblowers, and employees can seek remedies, including reinstatement and compensation, through legal channels.

6. **Criminal Penalties for Fraud (Sections 802, 906, 18 U.S.C. §§ 1519, 1348)**: SOX imposes significant criminal penalties for corporate fraud, including fines and imprisonment for executives who engage in or certify fraudulent financial practices. It also criminalizes the destruction, alteration, or falsification of financial records.

Cyber Provisions

While SOX does not explicitly address cybersecurity, its provisions have significant implications for how companies manage and protect electronic financial data:

Data Security and Internal Controls (Section 404, 15 U.S.C. § 7262): To comply with SOX's internal control requirements, companies must implement robust information security practices to protect financial data. This includes safeguarding electronic records from unauthorized access, ensuring data integrity, and maintaining accurate audit trails.

Electronic Records Management (Section 802, 18 U.S.C. § 1519): SOX requires companies to retain financial records, including electronic records, for a specified period. The destruction or alteration of these records is a criminal offense. Companies must therefore ensure that their digital data storage and backup systems are secure and compliant with retention requirements.

IT Audits and Compliance (Sections 302, 404, 15 U.S.C. §§ 7241, 7262): SOX compliance requires regular IT audits to verify that financial systems and related technologies are secure and functioning as intended. This includes assessing the effectiveness of cybersecurity measures that protect financial information from threats such as data breaches or cyberattacks.

Disclosure of Cybersecurity Risks (Section 409, 15 U.S.C. § 7261): Although not specifically mandated by SOX, companies are increasingly disclosing cybersecurity risks and incidents in their financial reports as part of their obligations under Section 409. This reflects the growing recognition of cybersecurity as a critical component of financial risk management.

Computer Fraud and Abuse Act

https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)

https://www.justice.gov/jm/jm-9-48000-computer-fraud

https://www.congress.gov/bill/99th-congress/house-bill/4718

https://elibrary.law.psu.edu/pslr/vol124/iss3/4/

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

18 U.S.C. § 1030

Date Enacted

10/16/1986

History

This law was created to amend the federal computer crime statute introduced by the 1984 Comprehensive Crime Statute. Since this was the first computer crime statute ever codified, it had obvious gaps in its coverage. These gaps and advancement in technology required that we change these statutes to make the law more broadly applicable. Since then, this act has been amended many times to keep up with advancements in technology and to expand its powers.

What does it protect

This act protects the government, financial institutions, computers used for commerce, businesses and individuals.

What does it Enforce

This act puts in place criminal and civil penalties for the following violations.

1. Unauthorized access or exceeding the level of authorized access
2. Using a computer to commit theft through fraud
3. Causing alteration, damage, destruction, or preventing use of a computer
4. Trafficking of access credentials that allows you to gain unauthorized access
5. Distribution of malicious software
6. Extortion under threat of destruction or damage of a victim's information system

Electronic Communications Privacy Act

https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically.

https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

18 U.S.C. §§ 2510-2523

Date Enacted

October 21, 1986

History

This act amended the Federal Wiretap Act to account for the advancement in technology from hard land lines to using computer, digital, and electronic communication.

What does it protect

This act protects the citizens of the United States. This amendment protects wire, oral, and electronic communications.

What does it enforce

Title I – Wiretap Act

This prohibits the intentional and incidental interception of any wire, oral, or electronic communication. It also prohibits the submittance of any illegally intercepted wire, oral, or electronic communications as evidence in a court of law.

Title II – Stored Communications Act

This prohibits unauthorized access to the subscriber's information and artifacts at the internet service provider.

Title III

This prohibits unauthorized access to incoming and outgoing call log data. Essentially tracking the source and destination of call traffic.

USA Patriot Act

https://www.justice.gov/archive/ll/highlights.htm

https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

107–56

Date Enacted

October 26, 2001

The act has been reauthorized and extended several times, with significant reauthorization occurring in 2005, 2006, and 2011. Each reauthorization typically included extensions of provisions and sometimes additional modifications. The USA Freedom act of June 2, 2015 introduced additional reforms, restricting some of the broader surveillance provisions granted in the original Patriot Act.

History

In response to the September 11th terrorist attacks on the United States the Patriot Act was put in place. The act was intended to make new tools to detect and prevent terrorism.

What does it protect

The citizens of the United States.

What Does it Enforce

The following summaries are not meant to be thorough or all-inclusive. It is recommended that you read the act to get a full understanding of what it does.

Title I: This provides funding to enforce the act, provides stipulations on using this act to prevent discrimination against Muslims, provides directives to create task forces, and grants emergency powers.

Title II: Grants authority to collect communications, share these communications, provide translation services, allows call log tracking, allows voice-mail collection, defines surveillance allowances, defines warrant procedures, and grants emergency powers.

Title III: This empowers the taking of action against money laundering. It encourages banks to communicate with law enforcement about suspicious activities on accounts. It also mandates due diligence to be taken for detection of laundering. This specifically prohibits accounts for foreign shell banks. It establishes obligations for banks to create anti-laundering programs. It creates regulations about currency smuggling.

Title IV: This establishes additional funding for the northern border patrol and enhances identity verification for U.S. entry applicants, including the use of criminal history information. It updates inadmissibility criteria, empowers border patrol to detain suspected terrorists, and facilitates sharing immigrant data with other countries for risk assessment. It authorizes a technological solution for entry-exit tracking linked to law enforcement, expands the foreign student monitoring program, and mandates machine-readable passports to prevent forgery. Additionally, it defines immigration options for terrorists, their families, and those affected by terrorist activities.

Title V: This allows the paying of rewards for information that leads to the capture or kill of terrorists. It allows the use of DNA to identify terrorists. It allows the coordination with law enforcement to capture terrorists. This defines jurisdiction for these investigations across multiple agencies. It authorizes the disclosure of educational records in the pursuit of terrorists.

Title VI: This regulates the benefits provided to officers and victims wounded that survived the domestic or international terrorist attacks and beneficiaries of those that died from the terrorist acts. It directs the compensation to be done without discrimination.

Title VII: This regulates the federal-state-local information sharing to respond to terrorism. This allocates funding for the creation of a secure information sharing system.

Title VIII: This regulation strengthens criminal laws for mass transit system attacks and defines domestic terrorism. It details crimes and punishments for harboring terrorists, updates codes for crimes against U.S. personnel and property abroad and enhances penalties for supporting terrorism. It expands asset forfeiture to include both domestic and international terrorist assets, clarifies conflicts with the Trade Sanctions Reform and Export Enhancement Act, and removes the statute of limitations for terrorism. It also updates penalties for various forms of terrorism and conspiracy, strengthens post-release supervision, includes terrorism in racketeering laws, introduces provisions for prosecuting cyberterrorism, and expands biological weapons statutes. Additionally, it funds and directs the development of cybersecurity forensic capabilities.

Title IX: This title creates guidance of better intelligence collection and sharing. This title expanded the scope of intelligence gathering to include international terrorist. This defines how sharing of foreign criminal intelligence will take between the director of the central intelligence agency and the attorney general. This defines how foreign terrorist assets are tracked. This establishes the translation center for translating foreign language intelligence. This establishes training of officials to use the newly collected foreign intelligence.

Title X: This title addresses discrimination against Sikh-Americans, designates venues for money laundering cases, and bars entry to money laundering suspects. It mandates studies on using biometric data at entry ports and on the FBI providing the TSA with a terrorist no-fly list. It allows the military to use non-military resources for base protection and permits telemarketing for charitable donations. It limits hazmat licenses, funds bioterrorism preparedness, expands crime identification technologies, and strengthens critical infrastructure protections.

Arms Export Control Act

https://www.govinfo.gov/content/pkg/USCODE-2023-title22/pdf/USCODE-2023-title22-chap39-subchapI-sec2751.pdf

https://www.law.cornell.edu/uscode/text/22/2751

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

22 U.S.C. § 2751

Date Enacted

Originally enacted on April 23, 1976, the AECA has been updated to identify and define cyber weapons in 2013, 2014, 2017, and 2020 via various acts, executive orders, and DoD memorandums.

History

The Arms Export Control Act (AECA) is an evolving framework of laws passed as part of a larger movement in the international community in the 1970's to control the proliferation of various types of weapons including emerging computer technologies. It's stated goals are to promote international security and support global stability by controlling exports of U.S. military technologies to prevent misuse or proliferation. The objective being to align weapons exports to U.S. foreign policy philosophy and law.

What does it protect

The AECA protects the U.S. government and citizens. It's stated purpose is to "foster world peace and the security and foreign policy of the United States." By establishing a framework of licenses and compliance specifications, the AECA regulates the definition of weapons and who is allowed to access them. In theory, non-proliferation acts protect all the citizens of the world by reducing access to weapons and military grade technologies.

What Does it Enforce

The AECA enforces strict controls over the export and import of defense articles and services. Key provisions include:

1. **Defense Articles and Services Control (22 U.S.C. § 2778)**: The AECA grants the President the authority to control the export and import of defense articles and services. This authority is typically delegated to the Secretary of State. The law requires the creation of the U.S. Munitions List (USML), which identifies items that are subject to export controls.
2. **Export Licensing (22 U.S.C. § 2778(b))**: U.S. companies and individuals must obtain a license from the Department of State before exporting or importing items on the USML. The licensing process involves a thorough review to ensure that exports align with U.S. foreign policy and national security interests.
3. **Foreign Military Sales (FMS) (22 U.S.C. § 2761)**: The AECA governs the sale of defense articles and services by the U.S. government to foreign governments. Such sales must be consistent with U.S. foreign policy and require congressional notification and approval.
4. **End-Use Monitoring (22 U.S.C. § 2785)**: The AECA mandates the establishment of procedures to monitor the end-use of exported defense articles and services. This ensures that items are used for their intended purpose and do not end up in the hands of unauthorized users.
5. **Arms Embargoes and Sanctions (22 U.S.C. § 2778(g))**: The AECA authorizes the President to impose arms embargoes or sanctions on countries that engage in activities contrary to U.S. interests, such as supporting terrorism or violating human rights.
6. **Congressional Oversight (22 U.S.C. § 2776)**: The AECA requires that certain arms transfers, particularly those involving significant military equipment or large monetary values, be reported to Congress, which has the authority to block or modify such transfers.

Cyber Provisions

While the AECA primarily focuses on traditional defense articles and services, it has been adapted to address the export of sensitive technologies, including those with cybersecurity implications:

1. **Control of Cybersecurity Items (22 U.S.C. § 2778)**: The AECA extends to the export of cybersecurity technologies that can be used for military or intelligence purposes. This includes software, hardware, and related services that could be used to conduct cyber operations or enhance the cyber capabilities of foreign entities.
2. **Licensing and Compliance (22 U.S.C. § 2778(b))**: Cyber-related exports, like other defense articles, require a license. The licensing process involves evaluating the potential impact on U.S. national security and the risk of technology being used for malicious cyber activities.

3. **End-Use and End-User Monitoring (22 U.S.C. § 2785)**: The AECA's end-use monitoring provisions apply to cybersecurity exports, ensuring that exported technologies are used by authorized recipients for legitimate purposes and are not diverted to malicious actors.
4. **Prohibition on Transfers to Adversarial Entities (22 U.S.C. § 2778)**: The AECA prohibits the export of cybersecurity technologies to countries or entities that pose a threat to U.S. security, including state-sponsored cyber threat actors and nations under U.S. arms embargoes.

Children's Online Privacy Protection Act (COPPA)

https://www.congress.gov/bill/105th-congress/senate-bill/2326

https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy

https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter91&edition=prelim

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute

S.2326 — 105th Congress (1997-1998)

The Child Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, P.L. No. 105-277, 112 Stat. 2681-728.

Date Enacted

October 21, 1998

History

The Children's Online Privacy Protection Act (COPPA), enacted in 1998, was driven by concerns over children's online privacy and data misuse. With the rise in internet use among children, investigations revealed that websites were collecting and using children's personal information without proper parental consent. The controversy surrounding *Toysmart.com*, an online toy retailer that planned to sell customer data, including information about children, during its bankruptcy, highlighted the need for protective legislation. The Federal Trade Commission (FTC) also highlighted gaps in privacy practices through its reports, contributing to COPPA's creation (Federal Trade Commission, 1998; *The New York Times*, 2000).

Since its enactment in 1998, COPPA has undergone several significant updates to address evolving online practices and technologies. The FTC revised COPPA in 2005 to broaden the definition of personal information and adapt parental consent methods to digital advancements (Federal Register, 2005). Further amendments in 2013 expanded protections to include mobile devices and social media platforms, reflecting technological progress and new data practices (Federal Trade Commission, 2013). In 2021, the FTC proposed additional updates to strengthen data protection and enforcement in response to ongoing technological changes (Federal Trade Commission, 2021). These modifications aim to enhance the law's effectiveness in safeguarding children's privacy in the digital age.

COPPA has faced criticism for being outdated and insufficiently comprehensive in addressing modern digital practices. Critics argue that the law's definition of "personal information" is too narrow, failing to account for emerging data collection techniques such as behavioral tracking and big data analytics (Hoffman & Johnson, 2016). Additionally, enforcement challenges and the evolving nature of online platforms make it difficult to apply COPPA effectively across diverse digital environments (Solove, 2017). These criticisms suggest that while COPPA has made strides in protecting children's privacy, it requires significant updates to keep pace with technological advancements and data practices.

What does it protect

COPPA directly protects children age 13 and under. It does not provide any direct protections to older people, however it does set a precedent for how personal information should be handled online and influences general data protection practices and standards beneficial to users of all ages.

High-profile enforcement actions by the Federal Trade Commission (FTC) underscore the significance of COPPA in protecting children's online privacy. The FTC has imposed substantial fines and mandated changes in data collection practices for several prominent companies found in violation of COPPA. For example, in 2019, YouTube was fined $170 million for collecting personal information from children without obtaining parental consent (Federal Trade Commission, 2019). These actions highlight COPPA's critical role in safeguarding children's privacy online and affirming parental authority over the collection and use of their children's personal data.

What Does it Enforce

COPPA enforces key requirements to safeguard the personal information of children under 13. Operators of child-directed websites and online services must obtain verifiable parental consent before collecting or using personal data (Federal Trade Commission, 1999). They are also required to provide clear privacy notices detailing their data practices, implement reasonable security measures, and allow parents to review and delete their child’s information (Federal Trade Commission, 1999). These provisions aim to ensure robust privacy protections and parental control over children's online data.

COPPA imposes penalties for non-compliance, including substantial fines. Violations of the Act can result in civil penalties up to $50,000 per violation, with the total fines potentially reaching millions of dollars depending on the severity and number of infractions (Federal Trade Commission, 1999). These penalties are intended to enforce compliance and ensure the protection of children's online privacy.

Cyber Provisions

The main requirements of COPPA with which a website operator must comply include: the development of a comprehensive privacy policy detailing the types of information collected from users; obtaining verifiable parental consent before collecting personal data from children under 13; informing parents about any data collected on their children; granting parents the right to revoke consent and delete their child's information; limiting the collection of personal information during participation in online games and contests; and ensuring the confidentiality, security, and integrity of any collected data (Electronic Privacy Information Center, n.d.). The Act was designed to enhance parental oversight in children's online activities, ensure their safety, and protect their personal information.

COPPA's requirements extend beyond website operators to include third-party service providers, mobile app developers, and social media platforms. Third-party services, including advertising networks and analytics companies, must comply with COPPA if their services are used on child-directed sites or apps, adhering to parental consent and data protection standards. Mobile app developers targeting children must also obtain verifiable parental consent and ensure data security (Federal Trade Commission, 2013). Similarly, social media platforms that collect data from users under 13 must update their privacy policies and manage consent (Federal Trade Commission, 2013).

Department of Defense Law of War

https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF

Jurisdiction

USA National Laws (Federal Laws)

Adjudication

Civil and Criminal

Legal Code or Statute and link

XVI – Cyber Operations

Date Enacted

June, 2015

History

Military conventions and what is considered honorable wartime behavior evolve and change over time, and particularly in response to emerging technologies. The scope and scale of destruction in the World

Wars created a need for specific defined laws of war which were established with the Hague (1899, 1907) and Geneva (1949) conventions and the charter of the United Nations (1945). In 2001, the U.S. began a more formal effort to consolidate a legal framework that could apply to the evolving nature and technologies of warfare. In 2015, the first edition of the "Department of Defense Law of War Manual" was published. It continues to be revised to reflect changes in national and international law. The following discussion is specific to Chapter XVI – Cyber Operations.

What does it protect

The DOD Law of War is formatted as a discussion on the merits and limitations of specific acts of war and differing levels of use of force and intelligence gathering. In combining many different sources of knowledge on international law as well as national legal documents such as those issued by the DOD Office of the General Counsel and other legal doctrine, the manual provides a roadmap for soldiers and military leaders to help influence their philosophy and actions in engagements during times of war and peace. In providing this guidance, it helps members of the military remain in compliance with the spirit and letter of the law, thus protecting military and civilians from unauthorized or unlawful acts.

This chapter is specifically designed to ensure that U.S. cyber operations protect the following:

- **Civilians:** Cyber operations should avoid harming civilian populations.
- **Neutral States and Their Infrastructure:** Operations should not target or negatively impact the infrastructure of neutral countries.
- **Critical Infrastructure:** Essential services such as electricity, water, and communications, which are vital to civilian life, should be protected from cyber attacks.
- **Medical and Humanitarian Operations:** Medical facilities and humanitarian efforts should remain unharmed by cyber operations.
- **Combatants and Military Objectives:** While combatants and military targets can be lawfully targeted, operations must adhere to the principles of proportionality and necessity. Any incidental harm to civilians or civilian objects should be minimized, and the military response should be proportional to the military advantage gained.

What Does it Enforce

The Cyber Operations portion of this book provides an overview of how current legal codes apply to the cyber domain including:

- Introduction and definitions:
    - Key Terminology: Defines terms related to cyber warfare, such as cyber-attacks, cyber operations, and cyber capabilities.
    - Scope: Describes the range of activities considered under cyber operations, including offensive and defensive actions. Example, operations that use computers as a function of command and control would not generally be considered cyber.
- Application of the Laws of War:
    - Essentially states that the laws and principles of war would still apply to cyber operations even when no specifically applicable law affecting the cyber domain applies.

    - It states that the laws of war are often not framed in terms of specific technology or weapon, but the types of acts. For example prohibiting attack on medical facilities or personnel wouldn't matter if the attack was by knife, bomb, or malware.
- Use of Force
    - Defines and Prohibits the use of cyber operations that constitute illegal uses of force
    - Provides examples such as triggering a nuclear plant meltdown or opening a dam above a populated area.
    - Defines intelligence and counterintelligence activities that may be considered illegal such as unauthorized intrusions into computer networks solely to acquire information, which might be considered a hostile act.
- Law of Neutrality
    - Discusses the unique circumstances of neutral states in cyber operations. The laws of war typically prohibit infringement on neutral states, however because of the interconnected nature of cyberspace, cyber operations in one state may create unintended effects in another state.
- Conduct of Hostilities (Jus in Bello)
    - Distinction: Requires that cyber operations distinguish between military objectives and civilian objects, ensuring that only legitimate military targets are affected.
    - Proportionality: Ensures that any collateral damage to civilians or civilian objects is not excessive in relation to the anticipated military advantage.
    - Precaution: Mandates that all feasible precautions are taken to minimize harm to civilians and civilian infrastructure during cyber operations. Specifies that acts resulting in economic loss or constituting a mere inconvenience to non-military objectives are acceptable.
- Legal Review of cyber-weapons.
    - Specifies that DoD policy requires the legal review of the acquisition of cyber weapons and weapons systems but reifies the commitment to prevent indiscriminate attacks with an example of a virus that would destroy civilian systems uncontrollably.
    - Confirms commitment to compliance with International Law.

Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf

Jurisdiction

International Law

Adjudication

Civil and Criminal

Legal Code or Statute

The CLOUD Act amends several sections of the U.S. Criminal Code, specifically Title 18 of the U.S. Code. The primary sections affected by the CLOUD Act are:

1. **18 U.S.C. § 2713**: This section is amended to allow the U.S. government to obtain data from service providers even if the data is stored outside the U.S., as long as the provider is within the jurisdiction.
2. **18 U.S.C. § 2703**: This section, relating to the disclosure of stored wire and electronic communications and transactional records, is updated to account for cross-border data requests.

Date Enacted

March 23, 2018

History

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is a significant piece of legislation enacted to address the complexities of cross-border data access in the digital age. This law represents a critical update to U.S. data privacy and law enforcement policies, aiming to resolve longstanding issues related to the extraterritorial reach of U.S. legal orders and international data privacy standards.

A confluence of significant events in the early days of computing culminated in several distinct occurrences in the 2010's highlighting the limitations of U.S. and international law. In particular, the Microsoft Ireland case *Microsoft Corp. v. United States* (2018) saw Microsoft corporation contesting a U.S. warrant demanding access to emails stored on servers located in Ireland. Microsoft argued that U.S. law could not compel the disclosure of data stored overseas without violating international sovereignty and privacy laws. This case highlighted the limitations of existing U.S. statutes, particularly the Stored Communications Act (SCA), in addressing the global nature of data storage and access (Hwang, 2018).

Evolving international data privacy standards were another critical factor, especially the European Unions General Data Protection Regulation (GDPR), effective from May 2018, which established a standard of stringent data protection requirements. Simultaneously, the EU-U.S. Privacy Shield framework was established to facilitate data transfers between the U.S. and EU while ensuring adequate protection of European citizens' data (European Commission, 2016). These developments underscored the need for a legal framework capable of reconciling U.S. data access demands with international privacy standards.

In response to these challenges, Congress introduced the CLOUD Act as part of a larger omnibus spending bill. The CLOUD Act sought to clarify the authority of U.S. law enforcement to access data stored abroad and to create a legal basis for bilateral agreements with other nations for data sharing. By addressing the deficiencies exposed by the Microsoft case and aligning U.S. law with international privacy norms, the CLOUD Act aimed to enhance global data access and cooperation in criminal investigations (CLOUD Act, 2018).

What does it protect

The CLOUD Act is designed to address the complexities of international data access while balancing various interests. Primarily, it aims to enhance the ability of U.S. law enforcement agencies to access electronic data stored overseas, which is essential for effective criminal investigations and maintaining the integrity of U.S. legal processes (Hwang, 2018). By clarifying the obligations of electronic communication service (ECS) and remote computing service (RCS) providers, the Act provides a structured framework for responding to data requests, thereby reducing legal ambiguity and facilitating compliance in international contexts (CLOUD Act, 2018).

The Act also incorporates protections for international data privacy standards by establishing a framework for bilateral agreements between the U.S. and other countries. These agreements must ensure that data access requests adhere to robust procedural privacy protections and data minimization procedures set by partner countries (Bracha, 2018). This aspect of the CLOUD Act aims to respect the sovereignty of foreign governments and safeguard the privacy of their citizens, aligning U.S. data access practices with global privacy norms.

Overall, the CLOUD Act seeks to harmonize international data access with privacy protections, benefiting U.S. law enforcement and service providers while also addressing global privacy concerns. By facilitating structured international cooperation and compliance with privacy standards, the Act contributes to a more coherent and balanced approach to cross-border data management (Davenport, 2019).

However, the Act's framework for cross-border data access, which allows U.S. law enforcement to compel data production regardless of location could be perceived as a violation of the sovereign rights of other countries. It can also clash with the legal and cultural norms of countries that prioritize privacy protections and data sovereignty.

What Does it Enforce

The CLOUD act provides trans-border access to communications data in criminal law enforcement investigations. EPIC's amicus brief in *Microsoft Corp. v. United States* underscores the need for respecting international privacy standards and cautions that a ruling favoring the government could lead other nations to disregard sovereign authority (EPIC, n.d.).

The CLOUD Act does not provide specific operational procedures for law enforcement but establishes a broad framework for data access and international cooperation:

1. **Data Requests**: U.S. law enforcement can issue warrants or court orders to compel data production from service providers, regardless of data location (CLOUD Act, 2018).
2. **International Agreements**: The Act outlines the need for bilateral agreements with foreign governments, requiring privacy protections and data minimization, but does not detail specific procedural guidelines for law enforcement (CLOUD Act, 2018).
3. **Judicial Oversight**: Data requests must be approved by a U.S. court, ensuring judicial review but not specifying detailed handling procedures (Hwang, 2018, pp. 1180-1210).
4. **Compliance Challenges**: Providers can challenge requests if compliance would breach foreign laws, though the Act does not prescribe specific actions for law enforcement in such cases (Bracha, 2018, pp. 45-67).

Companies operating in multiple jurisdictions need to navigate these complex legal environments carefully to avoid conflicts and ensure compliance with all applicable laws. Consumers should be aware of their rights and the circumstances under which their data can be accessed by law enforcement.

Cyber Provisions

1. Bilateral Agreements

The CLOUD Act allows the U.S. to establish bilateral agreements with other nations to facilitate cross-border data sharing. To be valid, these agreements must ensure that the partner countries provide robust privacy protections and adhere to data minimization procedures. Specifically, partner nations must implement strong procedural safeguards to protect individuals' privacy and limit data collection to what is necessary for the investigation (CLOUD Act, 2018).

2. Service Provider Compliance

U.S. electronic communication service (ECS) and remote computing service (RCS) providers are required to comply with data requests issued under the CLOUD Act. This obligation extends to disclosing data stored abroad, as authorized by U.S. warrants or court orders. Providers may challenge such requests if compliance would violate foreign laws or if the data pertains to non-U.S. persons residing outside the United States (Hwang, 2018, pp. 1180-1210; Bracha, 2018, pp. 45-67).

3. Judicial Oversight

Requests for data must be sanctioned by U.S. courts, ensuring that data access is legally authorized and subject to judicial review. Additionally, the implementation of the CLOUD Act necessitates transparency and accountability to prevent misuse and ensure that data access complies with legal and privacy standards (Davenport, 2019, pp. 89-104; CLOUD Act, 2018).

The CLOUD Act does not provide detailed specifications for the privacy safeguards that partner countries must implement. Instead, it outlines general requirements for these safeguards, which are to be included in bilateral agreements between the United States and other nations.

Privacy Shield

https://www.ftc.gov/business-guidance/privacy-security/privacy-shield

Jurisdiction

International Law

Adjudication

Civil

Date Enacted

July 12, 2016

History

The Privacy Sheild framework was an important data transfer agreement between the European Union (EU) and the United States (US) designed to standardize the security protocols of international personal data transfers. It was enacted to replace the Safe Harbor Framework of 2000, which had been rejected by the European Court of Justice in 2015. The European Court of Justice invalidated the Privacy Sheild framework in 2020 due to concerns over its inadequate protections and over US government surveillance practices. Privacy Sheild was replaced with the U.S.-EU Safe Harbor Framework. As of July 2020, the FTC has declared its expectation that companies continue to comply with Privacy Sheild while the countries negotiate new data privacy agreements.

Privacy Sheild has been replaced by the EU-U.S. Data Privacy Framework effective July 10, 2023.

Safe Harbor

https://www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework

Jurisdiction

International Law

Adjudication

Civil

Date Enacted

October 26, 1998

History

The Safe Harbor program was enacted in July 2000 to provide a legal framework for US companies to transfer personal data internationally due to the more restrictive requirements of the European Union. Safe Harbor was rejected by the European Union as inadequate on October 6, 2015 and replaced with Privacy Sheild in 2016.

Trans-Atlantic Data Privacy Framework (DPF)

https://www.dataprivacyframework.gov/

https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

https://eur-lex.europa.eu/eli/dec_impl/2023/1795

https://www.justice.gov/d9/pages/attachments/2022/10/07/dprc_final_rule_signed.pdf

https://www.justice.gov/opcl/executive-order-14086

Jurisdiction

International Law

Adjudication

Civil

Legal Code or Statute

EO 14086, AG -28 CFR Part 201-Data Protection Review Court

Date Enacted

July 10, 2023

History

The United States does not have a comprehensive overarching federal law protecting data privacy or establishing data privacy as a fundamental human right, as required by the European Union GDPR in order to transmit personal data internationally. Instead, the US has a patchwork of laws addressing some aspects of data privacy in specific circumstances. In addition, many states have their own specific data privacy requirements.

As such, the EU Justice Commision has rejected previous trans-atlantic data privacy agreements such as Safe Harbor, and Privacy Shield as inadequate to protect the private data of their citizens. This is largely due to concerns over US government mass surveillance practices, and the lack of an established court system for which EU citizens and entities may seek redress in the event of breach or violation. These two main inadequacies were addressed by Executive Order 14086, signed by President Biden in 2023, and the Attorney General CFR Part 201, establishing a data protection review board October 14, 2022.

The DPF provided a data privacy framework to meet EU requirements sufficient to be approved as of July 10, 2023, and effective as of October 12, 2023 but is anticipated to receive additional legal challenges. The United Kingdom and Switzerland both subsequently approved the DPF as "qualifying states for purposes of implementing the redress mechanism established in Executive Order 14086."

What does it protect

The DPF primarily protects EU citizens. U.S. and EU companies are required by the DPF to commit to compliance with stringent data protection policies and practices for EU citizens only, however it is likely to be more cost effective for those companies to utilize those standards for all customers, which should also benefit customers of other nationalities, including U.S. citizens. Non-EU citizens, including US citizens do not retain the same right of redress or remedy under this agreement.

What Does it Enforce

The DPF is an overarching framework that enacts significant privacy protections, some of which were covered under previous frameworks like Safe Harbor and Privacy Shield. Specific enhancements provided through EO 14086 and the establishment of the Data Protection Review Court under the AG – 28 CFR Part 201 enable US provisions to adequately meet the requirements of EU courts. The framework enacts protections for transatlantic transmission of EU citizens personal data.

The Executive Order 14086 "enhancing safeguards for United States Signals Intelligence Activities" clarifies and restricts mass electronic surveillance to only issues of national security and ensures rigorous oversight of those data collection.

- The order sets out the specific types of data and circumstances under which US Intelligence agencies are able to monitor, access, control and disseminate data.
- It prohibits the collection of data for the purposes of suppressing free expression by individuals or the press, restricting legal counsel or disadvantaging persons based on their race, gender, religion, etc.
- It also specifically limits mass or "bulk" data collection and prioritizes "targeted" data collection.
- And finally, the EO directs the Attorney General to extablish a process for citizens to seek redress in the event of any violation.

Key Requirements for DPF Program Participating Organizations:

- Organizations must include declarations in its privacy policies a commitment to comply with DPF principles in such a way that they are enforceable under U.S. law and direct consumers to relevant websites for redress.
- They must provide free access to a mechanism of redress for consumers with notice to the relevant authorities and commit to binding arbitration at the request of the individual.
- Organizations must maintain data integrity and limit personal information collection to the purpose relevant for processing and comply with data retention provisions.
- The DPF includes specific provisions for ensuring accountability for data transferred to third parties.

Data Protection Principles

- Notice: Organizations must inform individuals about the collection and use of their personal data, including the purpose of processing and the types of third parties to which the data may be disclosed.
- Choice: Individuals must be given the option to opt out of having their personal data disclosed to third parties or used for purposes other than those for which it was originally collected.
- Accountability for Onward Transfer: Organizations must ensure that any third party to whom they transfer data provides the same level of protection as guaranteed under the DPF principles.
- Security: Organizations are required to take reasonable and appropriate security measures to protect personal data from loss, misuse, and unauthorized access or disclosure.
- Data Integrity and Purpose Limitation: Personal data must be relevant for the purposes for which it is processed, and organizations must take reasonable steps to ensure that data is reliable, accurate, and up-to-date.
- Access: Individuals have the right to access their personal data held by an organization and correct, amend, or delete information that is inaccurate or processed in violation of the DPF principles.
- Recourse, Enforcement, and Liability: Organizations must provide robust mechanisms for complaints and disputes, including the availability of binding arbitration, and must be subject to oversight by the U.S. Department of Commerce and the Federal Trade Commission (FTC).
- Exceptions, amendments, and specifications for certain situations are spelled out in detail in the supplemental principles of the data privacy framework website.

Cyber Provisions

To participate, certain US companies must self-certify and publicly commit to comply with the EU-U.S. DPF Principles, which are enforceable under U.S. law.

The DPF requires an annual certification process and register their participation in the DPF by submitting certification through the DPF website.

Wassenaar Arrangement

https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf

Jurisdiction

International Law

Adjudication

Civil

Legal Code or Statute

DUAL-USE LIST - CATEGORY 4 - COMPUTERS

DUAL-USE LIST - CATEGORY 5 – PART 2 – "INFORMATION SECURITY"

Date Enacted

December 19, 1995

History

After the cold war, the countries that were part of the Coordinating Committee on Multilateral Export Controls (COCOM) got together to discuss risk to international security. On December 19, 1995 the member countries agreed to the Wassenaar Arrangement. This agreement was put in place to control the propagation of munitions grade technology. The provisions of this agreement went into effect November 1 1996.

What does it protect

This helps reduce the risk to the international community. The prevention of proliferation of these technologies reduces the probability of misuse of these technologies.

What Does it Enforce

The arrangement controls the export of the following controlled technologies:

Category 1– Special Materials and Related Equipment

Category 2 – Material Processing

Category 3 – Electronics

Category 4 – Computers

Category 5 – Part 1 – Telecommunications

Category 5 – Part 2 – Information Security

Category 6 – Sensors and Lasers

Category 7 – Navigation and Avionics

Category 8 – Marine

Category 9 – Aerospace and Propulsion

It also includes other military weaponry (Tanks, Drones, Large Caliber Artillery, etc.).

Major Cyber Provisions

In the Category 4 section on computers, it states that exports controls are in place for highly powerful computers that can process data at the rates of 70 TeraFLOPS a second, use light to represent data, mimic the behavior of a neuron, among other attributes. These machines are so powerful they can

easily crack encryption, perform sophisticated cyber-attacks on targets, and be used as an engine for a very advanced artificial intelligence (including autonomous weapon systems).

In Category 5 Part 2 on information security, it states that export controls are in place for multiple aspects of cryptography including quantum cryptography components. This section also states any systems which are explicitly created for defeating, weakening or bypassing "Information Security". This means tool specifically created for hacking (i.e. password cracking rigs, autonomous hackbots, etc.).

European Union- General Data Protection Regulation

https://gdpr.eu/

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil

Date Enacted

May 25, 2018

History

The European Union (EU) created data and privacy legislation that governs data lifecycle in the European Union. These regulations control the processing of personal data of the citizens of the European Union. This includes companies external of the union that wish to do business with citizens of the union. This legislation also empowers the countries to enforce the regulations through sanctions and fines.

Provisions

The following is the high-level checklist provided by the GDPR to become compliant.

Lawful basis and transparency

- Conduct an information audit to determine what information you process and who has access to it.
- Have a legal justification for your data processing activities.

- Provide clear information about your data processing and legal justification in your privacy policy.

Data Security

- Take data protection into account at all times, from the moment you begin developing a product to each time you process data.
- Encrypt, pseudonymize, or anonymize personal data wherever possible.
- Create an internal security policy for your team members, and build awareness about data protection.
- Know when to conduct a data protection impact assessment, and have a process in place to carry it out.
- Have a process in place to notify the authorities and your data subjects in the event of a data breach.

Accountability and governance

- Designate someone responsible for ensuring GDPR compliance across your organization.
- Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.
- If your organization is outside the EU, appoint a representative within one of the EU member states.
- Appoint a Data Protection Officer

Privacy rights

- It's easy for your customers to request and receive all the information you have about them.
- It's easy for your customers to correct or update inaccurate or incomplete information
- It's easy for your customers to request to have their personal data deleted.
- It's easy for your customers to ask you to stop processing their data.
- It's easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.
- It's easy for your customers to object to you processing their data.
- If you make decisions about people based on automated processes, you have a procedure to protect their rights.

European Union – Artificial Intelligence Act (EU AI)

https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil

Date Enacted

May 21, 2024

History

The EU AI Act was proposed in April 2021 in response to the rapid growth and deployment of AI technologies. The European Commission recognized the need to create a comprehensive regulatory framework that addresses both the opportunities and risks associated with AI. Concerns about AI's impact on privacy, security, and fundamental rights, as well as its potential for discrimination and misuse, motivated this initiative.

What does it protect

The EU AI Act is designed to protect all individuals within the European Union from potential harms associated with AI technologies. This includes protecting citizens, consumers, and workers from AI systems that may pose risks to their health, safety, or fundamental rights.

What does it enforce

The EU AI Act introduces a risk-based approach to regulating AI systems, classifying them into four categories:

- Unacceptable Risk: AI systems that pose a clear threat to safety, livelihoods, or rights (e.g., social scoring by governments) are prohibited.
- High Risk: AI systems that significantly affect people's lives (e.g., biometric identification, credit scoring, and recruitment) must comply with strict requirements for transparency, accuracy, and human oversight.
- Limited Risk: AI systems with limited risks (e.g., chatbots) require transparency measures, such as informing users that they are interacting with an AI system.
- Minimal Risk: AI systems with minimal or no risk (e.g., AI in video games) are largely unregulated.

Provisions

- Cybersecurity and Safety Measures: The Act requires that all high-risk AI systems be designed to ensure robust cybersecurity. This includes protection against data breaches, unauthorized access, and tampering.

- Data Governance: The Act mandates rigorous data management practices to ensure that datasets used for training AI systems are complete, accurate, and free from bias. This is crucial for protecting against discrimination and ensuring the fairness of AI outcomes.
- AI and Cyber Surveillance: The Act imposes restrictions on the use of real-time biometric identification systems in public spaces, such as facial recognition, except in cases of substantial public security threats (e.g., prevention of terrorism).
- Human Oversight Requirements: To mitigate the risks associated with AI, the Act emphasizes the importance of human oversight and sets guidelines for how such oversight should be implemented to prevent automated decision-making systems from infringing on human rights.

Computer Misuse Act

https://www.legislation.gov.uk/ukpga/1990/18/contents

https://www.nationalcrimeagency.gov.uk/who-we-are/publications/523-cyber-choices-hacking-it-legal-computer-misuse-act-1990/file

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Criminal

Legal Code or Statute

1990 c. 18

Date Enacted

June 29, 1990

History

In 1988 Robert Schifreen and Stephen Gold used stolen credentials to compromise British Telecom which resulted in the compromise of Prince Philip's email. The prosecution of this crime under the Forgery and Counterfeiting Act proved to be unsuccessful because of its lack of computer crime code. Because of this the British Parliament enacted the Computer Misuse Act.

What does it protect

This act protects computer systems and data.

What does it enforce

This act puts in place criminal and civil penalties for the following violations.

1. Unauthorized access to computer material
2. Unauthorized access with intent to commit or facilitate commission of further offences
3. Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer

3ZA. Unauthorized acts causing, or creating risk of, serious damage

3A. Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA (aka Manufacturing or trafficking of binaries to further a breach.)

United Kingdom- General Data Protection Regulation

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

https://www.gov.uk/data-protection

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil

Legal Code or Statute

Data Protection Act 2018 (2018 c.12)

Date Enacted

The UK GDPR came into effect on January 31, 2020, alongside the Data Protection Act 2018 (DPA 2018), which supplements the regulation.

History

The United Kingdom General Data Protection Regulation (UK GDPR) was introduced following the United Kingdom's exit from the European Union (Brexit). The UK GDPR is essentially a localized version of the EU General Data Protection Regulation (GDPR), which was retained in UK law under the European Union (Withdrawal) Act 2018. The UK GDPR aims to ensure that data protection standards remain high and align with those of the EU GDPR, maintaining robust privacy rights for individuals in the UK.

What does it protect

The UK GDPR protects the personal data of individuals (referred to as "data subjects") within the United Kingdom. It applies to any organization, whether based in the UK or elsewhere, that processes the personal data of individuals in the UK. The regulation is designed to protect data subjects' privacy rights by regulating how their personal data is collected, used, and managed.

What Does it Enforce

The UK GDPR enforces several principles and requirements that govern the processing of personal data, including:

1. **Lawfulness, Fairness, and Transparency (Article 5(1)(a))**: Data must be processed lawfully, fairly, and in a transparent manner, ensuring that individuals are informed about how their data is being used.
2. **Purpose Limitation (Article 5(1)(b))**: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data Minimization (Article 5(1)(c))**: The collection of personal data should be limited to what is necessary for the intended purposes.
4. **Accuracy (Article 5(1)(d))**: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or deleted without delay.
5. **Storage Limitation (Article 5(1)(e))**: Personal data should not be kept for longer than is necessary for the purposes for which it is processed.
6. **Integrity and Confidentiality (Security) (Article 5(1)(f))**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability (Article 5(2))**: Organizations must be able to demonstrate compliance with these principles and are accountable for their data processing activities.
8. **Legal Bases for Processing (Article 6)**: Organizations must have a lawful basis for processing personal data, such as consent, contract, legal obligation, vital interests, public task, or legitimate interests.
9. **Data Subject Rights (Articles 12-23)**: Individuals have rights under the UK GDPR, including the right to access their data, request correction or deletion, object to processing, and data portability.
10. **Data Protection Officer (DPO) (Articles 37-39)**: Organizations are required to appoint a DPO if they engage in large-scale systematic monitoring or processing of special categories of data.

Cyber Provisions

The UK GDPR contains several provisions focused on cybersecurity, ensuring that personal data is adequately protected:

Security of Processing (Article 32): Organizations must implement appropriate technical and organizational measures to secure personal data. This includes encryption, pseudonymization, access

controls, and ensuring the confidentiality, integrity, availability, and resilience of processing systems and services.

Data Breach Notification (Articles 33-34): Organizations are required to report data breaches to the Information Commissioner's Office (ICO) within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms. Affected individuals must also be notified if the breach is likely to result in a high risk to their rights and freedoms.

Data Protection Impact Assessments (DPIAs) (Article 35): Organizations must conduct DPIAs for processing activities that pose a high risk to individuals' rights and freedoms. The DPIA should assess the potential impact on privacy and security and identify measures to mitigate risks.

International Data Transfers (Chapter V, Articles 44-50): The UK GDPR restricts the transfer of personal data outside the UK unless the destination ensures an adequate level of protection. This may involve standard contractual clauses, binding corporate rules, or adequacy decisions.

UK Terrorism Act of 2000

https://www.legislation.gov.uk/ukpga/2000/11/contents

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Criminal

Date Enacted

February 19, 2001

Legal Code or Statute

2000 CHAPTER 11

History

This act was brought about based on the history of terrorism against the United Kingdom. This includes domestic terrorism related to Northern Ireland. This act was put in place shortly after the UK realized that the previously enacted legislation (Prevention of Terrorism Act) turned out to be insufficient.

What does it protect

This act protects the citizens, residents, public institutions, critical infrastructure, and government of the United Kingdom.

What Does it Enforce

The Act provides a broad definition of terrorism, covering activities intended to influence the government or intimidate the public for political, religious, or ideological purposes. This definition extends to actions involving serious violence, damage to property, and threats to public health and safety.

Cyber Provisions

This act doesn't explicitly address cybercrime, but if the crimes defined in this regulation are committed using technology it will be prosecuted as such.

Use of the internet for terrorism:

- Promote Terrorism
- Recruit Members
- Incite Violence
- Disseminating Bomb-Making Manuals
- Disseminating Propaganda

UK Terrorism Act of 2006

https://www.legislation.gov.uk/ukpga/2006/11/contents

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Criminal

Date Enacted

March 30, 2006

Legal Code or Statute

2006 CHAPTER 11

History

This act was brought about based on the history of terrorism against the United Kingdom. This includes the suicide bombing of London's public transportation system. This uncovered gaps that exist in the Terrorism Act of 2000.

What does it protect

This act protects the citizens, residents, public institutions, critical infrastructure, and government of the United Kingdom.

What Does it Enforce

This expands the powers of the Terrorism Act of 2000. This criminalizes the encouragement and glorification of Terrorism. This further expands the criminalization of dissemination of Terrorist publications. It also criminalizes the preparation of terrorist acts.

Cyber Provisions

This expands the Terrorism Act of 2000 to include the following in the definition of online locations:

- Websites
- Social Media
- Digital Publications

This act also empowers the government to remove any materials from the internet that violate either of the Terrorist acts.

Switzerland- Federal Act on Data Protection

https://www.fedlex.admin.ch/eli/cc/2022/491/en

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil

Legal Code or Statute

235.1

Date Enacted

September 25, 2020

History

Enacted as a comprehensive revision of prior versions of the FADP in response to evolving data protection landscape. In particular, the most recent revision was in response to the EU GDPR establishment. Switzerland is not a member of the EU, in large part because of its tradition of political neutrality. However, it is highly entwined with the EU economically, with an extensive series of bilateral agreements. The FADP was enacted to harmonize data protection with EU standards.

What does it protect

This act regulates the processing of personal data and data subjects' rights or actions that have an effect in Switzerland or affect Swiss citizens.

What Does it Enforce

1. The FADP sets out the following principles:
2. Protect Personal Data: It ensures that individuals' personal data is handled responsibly and kept private.
3. Grant Rights to Individuals: It gives people the right to know what data is collected about them, and to correct, move, or delete it if needed.
4. Anonymization: Specifies the requirement to destroy or anonymize data that is collected once no longer required for processing.
5. Regulate Data Handling: It sets rules for how organizations should collect, use, and store personal data, including security measures.
6. Supervise Compliance: It gives the Federal Data Protection and Information Commissioner (FDPIC) the power to oversee and enforce these rules, and to investigate complaints.
7. Consent requirements: It specifies that explicit consent is required for processing sensitive or personal data, and high-risk profiling by a private person or federal body.

Cyber Provisions

The FADP identifies the requirements of controllers of information including:

- Specifies types of controllers including domestic organizations, federal agencies, and international organizations.
- Data protection obligations including data security requirements, impact assessments.
- Duties to provide notification in specific circumstances to individuals or governing bodies.
- Special limitations and guidelines for federal bodies.

Singapore- Personal Data Protection Act (PDPA)

https://sso.agc.gov.sg/Act/PDPA2012

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil and Criminal

Legal Code or Statute

PDPA2012

Date Enacted

July 2, 2014

History

The Personal Data Protection Act (PDPA) was introduced as a response to growing concerns over personal data privacy in an increasingly digital and interconnected world. It was part of Singapore's broader effort to align its data protection standards with global practices and to bolster consumer trust in digital services.

What does it protect

The PDPA protects the personal data of individuals (both citizens and residents) in Singapore. It applies to all organizations that collect, use, or disclose personal data within Singapore, including both private sector companies and non-profit organizations. The law does not cover government agencies, which are subject to separate data protection frameworks.

What Does it Enforce

Consent: Organizations must obtain the individual's consent before collecting, using, or disclosing their personal data, with certain exceptions.

Purpose Limitation: Personal data must only be collected for purposes that a reasonable person would consider appropriate under the circumstances and must not be used beyond those purposes.

Notification: Organizations must inform individuals of the purposes for which their personal data is being collected, used, or disclosed.

Access and Correction Rights: Individuals have the right to request access to their personal data and request corrections if the data is inaccurate.

Data Protection Obligations: Organizations are required to implement reasonable security arrangements to protect personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.

Data Retention: Personal data should not be retained longer than necessary for the purposes for which it was collected.

Transfer of Data Outside Singapore: When transferring personal data overseas, organizations must ensure that the receiving party provides a comparable standard of data protection.

Data Breach Notification: Organizations must notify the Personal Data Protection Commission (PDPC) and affected individuals if a data breach is likely to result in significant harm to the individuals.

Cyber Provisions

Security Safeguards: Organizations must implement robust cybersecurity measures to protect personal data against unauthorized access, use, or disclosure. This includes both technical measures (e.g., encryption, secure storage) and organizational measures (e.g., access controls, employee training).

Data Breach Notification: If a data breach occurs that could lead to significant harm, the organization is required to notify the PDPC as soon as practicable, generally within 72 hours. Affected individuals must also be informed if the breach is likely to result in significant harm.

Accountability: Organizations must appoint a Data Protection Officer (DPO) responsible for ensuring compliance with the PDPA, including cybersecurity measures.

Third-Party Vendor Management: When engaging third-party vendors that handle personal data, organizations must ensure that these vendors are compliant with PDPA standards, including cybersecurity requirements.

Canada- Personal Information Protection and Electronic Documents Act (PIPEDA)

https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil

Legal Code or Statute

S.C. 2000, c. 5

Date Enacted

Enacted in April 2000, coming into full force on January 1, 2004

History

The Personal Information Protection and Electronic Documents Act (PIPEDA) was designed to promote consumer trust in electronic commerce and to align Canada's data protection framework with

international standards, especially in light of the rapid development of the internet and electronic commerce. Over the years, PIPEDA has been amended to strengthen privacy protections and to address emerging concerns related to digital privacy and security.

What does it protect

PIPEDA protects the personal information of individuals in Canada in the context of commercial activities conducted by private-sector organizations. It applies to all businesses and organizations across Canada, except those operating solely in provinces with their own comprehensive privacy laws deemed substantially similar to PIPEDA (such as Quebec, Alberta, and British Columbia). PIPEDA does not apply to non-commercial activities or to information collected, used, or disclosed by federal government institutions.

What Does it Enforce

PIPEDA outlines a framework for how organizations must handle personal information. Key provisions include:

1. Consent: Organizations must obtain an individual's consent before collecting, using, or disclosing personal information, with certain exceptions (e.g., in cases of legal or security obligations).
2. Purpose Specification: The purposes for which personal information is collected must be identified by the organization at or before the time of collection.
3. Limitation of Collection, Use, and Disclosure: Personal information should only be collected, used, or disclosed for the purposes for which it was collected, unless further consent is obtained.
4. Accuracy: Organizations are required to keep personal information as accurate, complete, and up-to-date as necessary for the purposes for which it is used.
5. Access and Correction Rights: Individuals have the right to access their personal information held by an organization and to request corrections if it is inaccurate.
6. Accountability: Organizations must appoint an individual responsible for ensuring compliance with PIPEDA and developing practices and policies to protect personal information.
7. Openness: Organizations must make their privacy policies and practices available to individuals.
8. Challenging Compliance: Individuals have the right to challenge an organization's compliance with PIPEDA and to lodge complaints with the Office of the Privacy Commissioner of Canada (OPC).

Cyber Provisions

PIPEDA includes several provisions that address cybersecurity, particularly in the context of protecting personal information:

1. **Security Safeguards**: Organizations must implement appropriate security safeguards to protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. These safeguards may include physical measures (e.g., locked filing cabinets),

organizational measures (e.g., staff training), and technological measures (e.g., encryption, firewalls).

2. **Breach Notification**: As of November 1, 2018, PIPEDA requires organizations to notify the OPC and affected individuals of any data breach that poses a "real risk of significant harm." This includes providing details on the breach, the information involved, and steps taken to mitigate harm.

3. **Data Retention and Disposal**: Organizations must retain personal information only for as long as necessary to fulfill the purposes for which it was collected. Once the information is no longer needed, it must be securely destroyed or anonymized.

4. **Cross-Border Data Transfers**: While PIPEDA does not prohibit cross-border data transfers, organizations must ensure that the personal information remains protected in compliance with PIPEDA standards, even when processed outside of Canada.

Brazilian- General Data Protection Law (LGPD)

https://www.gov.br/mds/pt-br/acesso-a-informacao/privacidade-e-protecao-de-dados/lgpd

https://gdpr.eu/gdpr-vs-lgpd/

Jurisdiction

Non-U.S. Domestic Laws

Adjudication

Civil

Legal Code or Statute

Lei Nº 13.709

Date Enacted

This was enacted on August 14, 2018, but took full effect on September 18, 2020

History

The Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, or LGPD) Law No. 13,709/2018 was influenced by the European Union's General Data Protection Regulation (GDPR) and represents Brazil's first comprehensive data protection regulation. The LGPD was created in response to increasing concerns over privacy and the need to protect personal data in the digital age, particularly

given the rapid growth of internet usage in Brazil. After multiple amendments and extensions, the LGPD came into full effect.

What does it protect

The LGPD protects the personal data of individuals (referred to as "data subjects") in Brazil, regardless of their nationality. It applies to any organization, both public and private, that processes personal data in Brazil or where the processing is aimed at offering goods or services to individuals in Brazil. The law covers data processing activities both within and outside the country if the data pertains to individuals located in Brazil.

What Does it Enforce

The LGPD establishes a set of rules and principles governing the processing of personal data, including:

1. Legal Bases for Processing (Article 7): Organizations must have a valid legal basis to process personal data, such as consent from the data subject, compliance with a legal obligation, execution of a contract, or protection of the data subject's life or health.
2. Consent (Article 8): Consent must be freely given, informed, and explicit. Data subjects must be clearly informed about the specific purposes for which their data is being processed.
3. Data Subject Rights (Articles 17-22): Individuals have the right to access their personal data, correct inaccurate data, request data portability, delete data, and withdraw consent. They also have the right to obtain information about how their data is being processed.
4. Purpose Limitation (Article 6, II): Personal data must be processed for legitimate, specific, and explicit purposes that are communicated to the data subject.
5. Data Minimization (Article 6, III): Data processing should be limited to the minimum necessary to achieve the stated purpose.
6. Transparency (Article 6, VI): Organizations must ensure transparency in their data processing practices by providing clear and accessible information to data subjects.
7. Security (Article 6, VII): Organizations are required to implement appropriate security measures to protect personal data from unauthorized access, loss, alteration, or destruction.
8. Accountability (Article 6, X): Organizations must demonstrate compliance with the LGPD through the implementation of effective data protection policies and practices.

Cyber Provisions

The LGPD includes several provisions specifically related to cybersecurity:

Security Measures (Article 46): Organizations must adopt technical and organizational measures to protect personal data from unauthorized access, accidental or unlawful destruction, loss, alteration, communication, or any type of inappropriate or unlawful processing. These measures should take into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of data processing.

Data Breach Notification (Article 48): In the event of a data breach that may result in significant risk or damage to data subjects, organizations are required to notify the National Data Protection Authority (ANPD) and the affected data subjects without undue delay. The notification should include details of the breach, the data affected, and measures taken to mitigate harm.

Data Protection Impact Assessment (DPIA) (Article 38): Organizations may be required to conduct a DPIA for processing activities that pose a high risk to data subjects' rights and freedoms. The DPIA should assess the impact of the processing on data protection and propose measures to mitigate risks.

Data Anonymization (Article 12): The LGPD encourages the use of anonymization techniques to reduce risks to data subjects. Anonymized data is not subject to the same stringent protections as personal data, provided it cannot be re-identified.

Appendix II – Quick Reference Table

Law/Regulation/Framework	URL
Alabama-2012-HB400	https://legiscan.com/AL/text/HB400/id/640745/Alabama-2012-HB400-Enrolled.pdf
California Consumer Privacy Act	https://oag.ca.gov/privacy/ccpa https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article
Colorado Privacy Act	https://leg.colorado.gov/bills/sb21-190
District of Columbia Protection of District public officials § 22-851	https://codes.findlaw.com/dc/division-iv-criminal-law-and-procedure-and-prisoners/#!tid=NF52BF780FD7211DB9C90DF511833162A
New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act	https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act https://legislation.nysenate.gov/pdf/bills/2019/S5575B
Massachusetts Data Security Regulations	https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth/download
Ohio Unauthorized use of property - computer, cable, or telecommunication property	https://codes.ohio.gov/ohio-revised-code/section-2913.04

Texas Identity Theft Enforcement and Protection Act	https://law.justia.com/codes/texas/business-and-commerce-code/title-11/subtitle-b/chapter-521/subchapter-b/
Illinois Personal Information Protection Act	https://idfpr.illinois.gov/content/dam/soi/en/web/idfpr/banks/cbt/welcnews/news/2007/personalinfoprotectionact.pdf https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
Americans with Disabilities Act	https://www.ada.gov/law-and-regs/ada/
The Family Educational Rights and Privacy Act	https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html#:~:text=The%20Family%20Educational%20Rights%20and,privacy%20of%20student%20education%20records
Access Device Fraud Law	https://www.justice.gov/archives/jm/criminal-resource-manual-1030-definitions#:~:text=%22Unauthorized%20access%20device%22%20is%20defined,546%2C%20549%20(2d%20Cir
Gramm-Leach-Bliley Act	https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6801&edition=prelim
Health Insurance Portability and Accountability Act	https://www.congress.gov/bill/104th-congress/house-bill/3103/text https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html
Digital Millenium Copyright Act	https://www.govinfo.gov/content/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf
Fair Credit Reporting Act	https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf https://www.ecfr.gov/cgi-bin/text-idx https://www.law.cornell.edu/uscode/text/15/1681
Sarbanes Oxley Act (SOX)	https://www.govinfo.gov/content/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

Computer Fraud and Abuse Act	https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim) https://www.justice.gov/jm/jm-9-48000-computer-fraud https://www.congress.gov/bill/99th-congress/house-bill/4718 https://elibrary.law.psu.edu/pslr/vol124/iss3/4/
Computer Misuse Act	https://www.legislation.gov.uk/ukpga/1990/18/contents https://www.nationalcrimeagency.gov.uk/who-we-are/publications/523-cyber-choices-hacking-it-legal-computer-misuse-act-1990/file
Electronic Communications Privacy Act	https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285
USA Patriot Act	https://www.justice.gov/archive/ll/highlights.htm https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
Arms Export Control Act	https://www.govinfo.gov/content/pkg/USCODE-2023-title22/pdf/USCODE-2023-title22-chap39-subchapI-sec2751.pdf https://www.law.cornell.edu/uscode/text/22/2751

Children's Online Privacy Protection Act	https://www.congress.gov/bill/105th-congress/senate-bill/2326 https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter91&edition=prelim
Department of Defense Law of War	https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF
Clarifying Lawful Overseas Use of Data Act (CLOUD Act)	https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf
Privacy Shield	https://www.ftc.gov/business-guidance/privacy-security/privacy-shield
Safe Harbor	https://www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework
Trans-Atlantic Data Privacy Framework (DPF)	https://www.dataprivacyframework.gov/ https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities https://eur-lex.europa.eu/eli/dec_impl/2023/1795 https://www.justice.gov/d9/pages/attachments/2022/10/07/dprc_final_rule_signed.pdf https://www.justice.gov/opcl/executive-order-14086
Wassenaar Arrangement	https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf
European Union General Data Protection Regulation	https://gdpr.eu/ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
United Kingdom General Data Protection Regulation	https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

	https://www.gov.uk/data-protection
UK Terrorism Act of 2000	https://www.legislation.gov.uk/ukpga/2000/11/contents
UK Terrorism Act of 2006	https://www.legislation.gov.uk/ukpga/2006/11/contents
Switzerland Federal Act on Data Protection	https://www.fedlex.admin.ch/eli/cc/2022/491/en
Singapore - Personal Data Protection Act (PDPA)	https://sso.agc.gov.sg/Act/PDPA2012
Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)	https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html
Brazilian - General Data Protection Law (LGPD)	https://www.gov.br/mds/pt-br/acesso-a-informacao/privacidade-e-protecao-de-dados/lgpd https://gdpr.eu/gdpr-vs-lgpd/

Appendix III- Update Log

Date	Document Version	Updater	Details
8/9/2024	1.0	Craig Peltier	Initial Version
8/25/2024	1.0.1	Craig Peltier	Context Update to include a few more acts and to make the verbiage more concise.
8/29/2024	1.0.2	Craig Peltier	Fixed some link issues, added EU AI, jurisdiction, and adjudication.
9/3/2024	1.0.3	Craig Peltier	Integration of peer review feedback on the context and conciseness.
4/7/2025	1.0.4	Craig Peltier	Switched the order of some paragraphs to make it clearer to the reader. Also uploaded this version to Github