Part two Notes for ethics and technology

In this section you will need to understand **what a law is** and how it applies and ethics there if you questions on the test that I can remember that scenario based, but it revolved around what is the law and the **different types of laws. You may also get scenarios that would revolve around how a lot influences an ethical decision or how an ethical decision would impact a law**. *just a reminder that I am going off work. I remember from my exam test can be anything*.

What is a law?

Law is a set of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (such the government , law-making bodies, etc).

Reminder use the study guide provide, and the PowerPoints for the laws ,they give really good details about each law, but the most common that I was asked on my test that I can remember

The Gramm–Leach–Bliley Act (GLBA) is a law that allows financial institutions, such as banks and insurance companies, to share information with each other while also protecting consumers' personal financial information. It requires these institutions to explain their information-sharing practices to customers and to let them opt-out of having their information shared in certain cases. The main goal of this act is to enhance consumer privacy and security while promoting competition among financial services.

Example A:

A ***Bank*** wants to **offer** Mia an ***investment products*** in partnership with a ***Brokerage Firm.*** Before they can do this, ***they must first inform Sarah about their practices regarding information sharing.*** Then provide her with a ***privacy notice detailing what information they plan to share with Brokerage Firm*** —such as her account balance and transaction history—and ***how it will be used to help her access potentially beneficial investment opportunities.***

Note these are key terms that could lead to an answer if this was a question

The sections highlighted in pink represent something that is financial and something that is being offered

The blue represents with whom a product or service has been offered to or with

The red terms provide details of what being shared/offered and what it represents, which is something financial

The **Right to Financial Privacy** protects your personal financial information from being shared without your permission. It ensures that banks and other financial institutions cannot give your financial records to the government unless:

1. You give consent
2. A legal process is followed, such as a subpoena or warrant

This right is mainly established through the Right to Financial Privacy Act (**RFPA**), which **limits how federal agencies can access your financial data**. It's designed to strike a balance between your privacy and the government's need for information during investigations.

Example B

Is it **justifiable** for the ***government to access*** an ***individual's financial records without their consent during an investigation***, even if no formal charges have been filed yet?

This question, we can automatically assume that the answer would be the right to financial privacy because without consent or warrant private financial information cannot be accessed

For this question, I highlighted key words in terms to look for if this was a real exam, one in bold justifiable means the question is asking can you justify an action. Second in blue, the terms government was trying to access something of who an **individuals and their financial information.** In pink is giving their actions and in red shows the nature of their actions.

The **Privacy Act** is a law in the United States designed to protect the privacy of individuals by regulating how federal agencies collect, use, and share personal information. It establishes certain rights for individuals regarding their personal data held by government agencies. Agencies must inform individuals when they collect their information and provide a privacy notice explaining how it will be used.Federal agencies are restricted from disclosing personal information without the individual's consent, except in certain circumstances (like law enforcement needs).

Example

You run into situation where a person named John is applying for a job with the government . During the process, the federal agency **collects personal information about him,** including his educational background and work history. Under the Privacy Act, John has the right to ask the agency for copies of the records they have about him. If he finds that there's incorrect information, like a misreported job title, he can request that the agency correct it.

Additionally, **the agency cannot share John's information with any other entity** (like a background check company) **without his consent unless it falls under specific exceptions,** such as for national security reasons. This ensures John's personal information is kept confidential and only used for its intended purpose.

The Foreign Intelligence Surveillance Act (FISA) is a U.S. law that allows the government to collect intelligence about foreign powers or agents. It involves monitoring communications, such as phone calls and emails, if they involve foreign interests that may pose a threat to national security. Amended to surveillance act.

FISA sets up a special court, called the Foreign Intelligence Surveillance Court (FISC), which reviews requests for surveillance to ensure they're justified and lawful. The act aims to protect both national security and the privacy rights of individuals. So, in **simple terms, it's a law that lets the government spy on foreign threats while trying to respect citizens' privacy.** FISA gives the government the ability to conduct surveillance on foreign intelligence targets without a traditional warrant.

Example C:

The the **US government allows** for the collection of **electronic communications** from **foreign targets** to protect national security. However, during surveillance, incidental data from U.S. citizens may also be collected

What act only allows for foreign data and communication to be collected without a warrant ?

*******FISA foreign intelligent surveillance act *********

FOIA freedom of information act

CALE communication assistance for law-enforcement

ECPA electronic communication privacy act

FISA allows, search an interception without a warrant on foreign surveillance.

For this act here, I really didn't see it on the exam but again every test is different. I simplified it the best I could because the given material was too much for me to try to comprehend.

Executive Order 12333, titled "United States **Intelligence Activities**," was signed by President Ronald Reagan on December 4, 1981. This order outlines the roles and responsibilities of U.S. intelligence agencies in conducting operations to protect national security and gather intelligence, both domestically and internationally.

I also saw this come up if few times in the exam the term safe Harbor it's really not mentioned in their guides and I don't remember reading it but here is an explanation

A "**safe harbor**" refers to a **legal provision that protects companies from liability**

under certain conditions. It allows organizations to operate with some assurance that they won't face penalties for specific actions, as long as they meet predetermined guidelines or standards.

Explanation:
You work at a company that handles customer data. If the company follows a specific privacy practices outlined by laws (like **GDPR or CCPA)**, they can avoid penalties even if there's a data breach. These practices create a "**safe harbor**," giving them a level of protection as long as they comply with the rules.

The **Communication Decency Act (CDA)**, enacted in 1996, was designed to regulate online content, particularly to protect minors from harmful materials. It includes provisions that provide immunity to internet service providers and platforms from liability for content posted by users.

Example D

Consider a social media platform that you may use. If a user posts offensive or defamatory content, Section 230 of the CDA protects Facebook from being sued for that post. Instead, the responsibility lies with the individual who made the post. This legal framework encourages platforms to allow free expression while still having the option to remove harmful content.

The CDA act and sometimes be confused with COPA act.

The **Child Online Protection Act (COPA)**, enacted in 1998, aimed to **protect minors from harmful material on the internet by imposing restrictions on websites that contain inappropriate content**. It sought to make it illegal to knowingly transmit harmful content to minors.

COPA was designed to limit children's access to obscene or harmful content online. Websites could face penalties for failing to restrict access to inappropriate material for users under 17.

Example E

a website that hosts user-generated videos. (**Websites or you create Contant in terms)** Under COPA, this site would need to **implement measures,** such as **age verification** or **content filtering, to prevent** minors from **accessing videos deemed inappropriate**. If the site fails to do this and a minor views harmful content, the website could potentially face legal consequences.

The bolded word are terms or something you could think about, if you are asked a question such a scenario based ,always remember to look for terms that could lead or produce an answer.

So both laws aim to address online content and its impact on minors, the CDA emphasizes platform protection and content moderation, whereas COPA focuses on restricting minors' access to harmful material.

Children's Online Privacy Protection Act (COPPA)

- Enacted in 1998, **COPPA focuses on protecting the privacy of children under 13 when they use websites and online services.**
- Requires websites to obtain verifiable parental consent before collecting personal information from children.
- Mandates that websites provide clear privacy policies and guidelines for data collection.
- Focuses on Protecting children's personal information online.

Internet filter is a software that can be used to block access to certain websites that contain materials that are considered to be inappropriate or offensive a strong Internet filter uses a combination of URL, keywords, and other dynamic content filtering. Sometimes the Internet filters can be aggressive and block, legitimate sites, some Internet service

providers.

The **Children's Internet Protection Act (CIPA)**, enacted in 2000, aims to protect children from harmful online content **in schools and libraries.** It requires these institutions to implement certain safety measures when using federal funds for internet access or technology.

CIPA aims to create a safer online environment for children in educational settings while balancing the need for access to information.

Example

There is local public library that receives federal funding for internet access. Under CIPA, the library must:

- Implement a filtering system to block access to websites containing explicit material or inappropriate content.
- Establish an internet safety policy outlining how they will protect children using their computers.
- Educate library staff on these policies to ensure they can assist young patrons safely.

If a parent finds that their child accessed inappropriate content on a library computer, they could raise concerns, prompting the library to review and potentially strengthen its filtering and safety measures.

Bribery, is an act offering, giving receiving or soliciting something of value such as money gifts or favors with the intentions of influencing actions of an individual in a position of authority. This is considered an unethical practice and is often used to gain an unfair advantage, bribery is considered illegal in many jurisdiction/ Countries and can have serious consequence.

The Foreign Corrupt Practices Act (FCPA) is a U.S. law that makes it illegal for American companies and individuals to bribe foreign officials to gain or keep business. It aims to promote fair competition and prevent corruption in international business dealings.

The act also requires companies to maintain accurate financial records and have controls in place to prevent bribery. In short, it's about ensuring that companies play fair when doing business overseas.

Example
When someone pays(bribes) foreign officials to win a contract, influence the procurement process, avoid contract termination, or obtain exceptions to regulations in return for favor. This is illegal todo

The **Digital Millennium Copyright Act (DMCA)**, enacted in 1998, is a U.S. law that aims to protect copyright holders in the digital age. It addresses issues related to online copyright infringement and establishes procedures for handling copyright violations.

The act provides a "**safe harbor**" for online service providers (OSPs), protecting them from liability for user-uploaded content as long as they comply with specific requirements, such as promptly removing infringing content when notified.

The **USA PATRIOT Act**, enacted on October 26, 2001, is a legislative response to the September 11 terrorist attacks. The act aimed to enhance national security and strengthen law enforcement's ability to prevent, detect, and respond to terrorism. The acronym "PATRIOT" stands for "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

This act allowed law enforcement to use "roving wiretaps," which permit monitoring of multiple communication devices used by a suspect.
the **USA PATRIOT Act** was a crucial legislative tool in fighting terrorism post-9/11.

The **SLAPP Act, or "Strategic Lawsuit Against Public Participation" Act,** refers to

legislation aimed at **preventing abusive lawsuits that are intended to silence or intimidate individuals or organizations from exercising their rights to free speech and public participation**.

These lawsuits often **target those who speak out on matters of public interest, such as activism, journalism, or community engagement,** with the goal of stifling dissent or discouraging others from expressing their views.

Wiretap Act

The **Wiretap Act**, part of the **Omnibus Crime Control and Safe Streets Act of 1968,** regulates the interception of wire and oral communications. **It makes it illegal to intentionally intercept or disclose the contents of any wire, oral, or electronic communication without consent.**

Here are some Key Points:

- Consent Requirement: Generally requires consent from at least one party involved in the communication to legally intercept it.
- **Law enforcement must obtain a court order to wiretap communications for criminal investigations.**
- Penalties: Violating the act can lead to criminal and civil penalties.

Communications Assistance for Law Enforcement Act (CALEA)

Enacted in 1994, **CALEA** requires telecommunications carriers and manufacturers to ensure their equipment is capable of enabling law enforcement to conduct lawful surveillance. Mandates that telecom providers design their systems to allow for easy law enforcement access. CALEA focuses on making sure the technology used for communication can support

wiretaps when authorized by law enforcement.
the **Wiretap Act governs** the legalities of intercepting communications, while **CALEA** ensures that telecommunications systems can support such law enforcement activities when legally warranted.

I noticed that these two laws can be mixed and mistaken for the other so here is a breakdown of what they mean. on the OA exam, especially the way some of the scenario questions are asked to be a bit tricky with these two laws.

- Wiretap Act: Primarily regulates the act of intercepting communications.
- CALEA: Ensures telecommunications systems are equipped for law enforcement surveillance.
- Wiretap Act: Focuses on legal requirements for interception and disclosure.
- CALEA: Addresses technical capabilities of communication service providers.
- Wiretap Act: Requires law enforcement to obtain a court order for surveillance.
- CALEA: Provides the framework for how telecom companies must comply with existing law enforcement requests.

The **General Data Protection Regulation (GDPR)** is a comprehensive data privacy law enacted by the European Union (EU) in May 2018. Its primary aim is to enhance the protection of personal data for individuals within the EU and the European Economic Area (**EEA**), as well as to address the export of personal data outside these regions. The **GDPR** represents a landmark shift in data privacy regulation, emphasizing the importance of protecting individual rights and ensuring responsible data handling practices.

The **Freedom of Information Act (FOIA)** is a law that gives people the right to access information from the federal government. It allows you to request records and documents held by government agencies. The goal of the FOIA is to promote transparency and keep the public informed about government activities.

E-Discovery, short for electronic discovery, refers to the process of identifying, collecting, and producing electronically stored information (ESI) in response to a request in legal investigations .ESI can include emails, documents, databases, social media, text messages, and any other digital data relevant to the case.
E-Discovery is a critical aspect of litigation, regulatory investigations, and government inquiries, as it helps parties involved in legal disputes gather evidence and assess facts.

Example
a large corporation, XYZA Corp, is involved in a legal dispute with a former employee who claims wrongful termination and discrimination. The former employee files a lawsuit seeking justice and compensatory damages.
So how does this work……..

1. During the discovery phase of the lawsuit, the employee's legal team submits a request for documents related to the employee's termination and any relevant communications within the company.
2. XYZA Corp's legal team must identify all potential sources of ESI that could be relevant to the lawsuit. This includes emails, internal chat logs, employee records, and documents stored on their servers or in cloud storage.
3. To avoid spoliation (the destruction of evidence), XYZ Corp places a legal hold on all potentially relevant electronic records. This means that employees are notified not to delete or alter any communications or documents that may pertain to the case.
4. The company's IT department works with the legal team to collect relevant data .Once collected, all the data goes through a review process where attorneys analyze the information for relevance and privilege.

5. After reviewing, the relevant documents and communications are produced to the former employee's legal team. Then court

E-discovery is a crucial aspect of modern litigation that ensures that all relevant electronic information can be accessed and reviewed in a legal context.

There are a few more laws that you should research, the chapter 4 PowerPoint for this course is also very helpful and shows all of the laws that may be on your test. The ones I showed were some of the ones that were on my test and was a bit confusing , but the rest of the set laws are pretty much easy. You just have to read the terms.

From my knowledge, there was also a few HIPAA related questions that were somewhat direct And some of the European policy laws. Easy laws to remember.

Also, no, what the **first and fourth amendments** are those two were on my exam.
Example a question that was asked that I can remember was **what type of speech is not protected under the first amendment** now I do remember that there was scenario along with the question. There was another regarding the fourth amendment. I don't remember the exact details, but it was scenario that was more ethical and involved around IT. So just try to remember key terms and phrases.

There was a direct question about the **John Doe act**- which means a lawsuit that organizations may file against anonymous person to gain a subpoena power to learn their identity of who tried to harm the organization and when a lawsuit is filed, it's a is issued for the defendant to appear in court, and the plaintiff can seek permission from the court third-party to get the identity of the defendant.

There was a scenario base question that was very direct regarding the foreign intelligence surveillance act I had to deal with a US citizen who had a warrant from what I can remember, but I do remember the answers being completely off and semi not related to the question.
They were questions that were related to **doxing, anonymity** and one question that was pretty much direct about **Can-Spam Act.**

Also study on the fair and accurate credit transaction act and fair credit act. Pay close attention to those questions.

There were many questions that were scenario based on these two act right here is good to study them

Computer Fraud and Abuse Act (CFAA)

The **Computer Fraud and Abuse Act (CFAA)**, enacted in 1986, is a U.S. federal law that **criminalizes unauthorized access to computers and networks, as well as activities involving data theft or damage.** Originally aimed at combating hacking and computer-related espionage, the CFAA has evolved to cover broader computer-related misconduct.

Example

An employee, Mia who works for a brokerage company, accesses a restricted part of the company's database using credentials she has but wasn't authorized to use for that specific area. She downloads sensitive client information to sell to a competitor.

She is in violation this unethical and illegal : This is considered exceeding authorized access under CFAA, as she was authorized to access certain parts of the system but not the section containing sensitive client information.

Stored Communications Act (SCA) - Part of the Electronic Communications Privacy Act (ECPA)

The **Stored Communications Act (SCA)** is a section of the **Electronic Communications Privacy Act (ECPA),** enacted in 1986. **It regulates the access to and disclosure of stored electronic communications and transactional records by service providers. It aims to protect users' privacy in electronic communications that are stored on servers**, such as emails, texts, or cloud data.

Example

John hacks into a friend's email account, hoping to find personal photos or sensitive information. Even though he only looks at the inbox without deleting or modifying any emails, his actions violate

the SCA.

he's in Violation: This constitutes unauthorized access to stored communications, even if no damage is done, because John accessed private emails stored on the email server without authorization.

CFAA focuses on unauthorized access to computer systems and the misuse of data from those systems (whether the systems belong to a private company or government).

- SCA deals specifically with the privacy and access rules for stored electronic communications, such as emails or data held by communication service providers.

The **False Claims Act (FCA)** is a U.S. federal law designed to prevent people or businesses from defrauding the government. Essentially, it punishes those who submit false or fraudulent claims to get money from the government.

- If someone lies or cheats to get paid by the government (or to avoid paying what they owe), they can be held accountable under the FCA.
- The law allows whistleblowers (people who report the fraud) to sue on behalf of the government and earn a reward if the case succeeds.

Example: A construction company gets a government contract to build a school but secretly uses cheaper, substandard materials while still billing the government for high-quality ones.

- Violation: The company committed fraud by billing the government for something it didn't deliver as promised.

the **FCA** targets anyone trying to cheat the government and rewards those who help catch the cheaters!(**whistleblowers**)