

## Part three

On the exam, there are a lot of questions that revolve around data privacy. Mainly the questions were scenario based from my memory. There were a lot PAPA questions and the mass majority of it was on cyber security related issues that was mixed in with laws, The scenarios that was given to me were somewhat straightforward, but the answers were quite off, so again you will have to look for those key terms and phrases. And call on your judgment

I will provide an example and in bold or color, are some of key terms and phrases to look out for so you will have an idea of the direction for an answer

Here is an example

A mega IT company, TechGlobal, **experiences a cybersecurity breach** where **sensitive personal data of customers**, including names, email addresses, and payment information, **is leaked**. This **data includes the personal data of EU citizens**.

\*For this scenario here because it has to do with data of customers and the customers are EU citizens. If it's directed towards the law, I say the answer would be **general data protection regulation**. And if the answers are being directed towards a cyber security, I would say they were hacked by a **black hat hacker** or is it deal with **PAPA** answers I would say **privacy**. If this is directed towards CIA traid answer would be **confidently**.

For the **PAPA** model I will try to give a detailed explanation because the OA is tricky. There are a lot of PAPA questions some of the questions were scenario and some that I can remember on it just the definition but again every test is different.

# What is papa

The PAPA Model in ethics is a framework used to analyze ethical issues related to information management, especially in fields like information technology and data management. PAPA stands for Privacy, Accuracy, Property, and Accessibility, and it was developed by Richard Mason in 1986

## Privacy

**Privacy is about controlling who has access to your personal information. It involves deciding what personal data is collected, how it is stored, and who can use it.**

- Ethical Concern: Who has the right to access personal information? How is personal data collected, used, and protected?
- Example: When using social media platforms, users expect their personal data to be protected and not shared with third parties without their consent.

\*When you install a social media app, it may ask for access to your contacts, location, and photos.

The ethical question: Should the app have the right to collect and store such personal data?

Scenario: Suppose the app shares your location data with advertisers without your permission. This would be a violation of your privacy.

- What to think about:
- Who owns personal data?
- How can individuals protect their privacy in an increasingly digital world?
- What are the boundaries between useful data collection

## Accuracy

**Accuracy concerns whether the data collected is correct, complete, and up-to-date. If inaccurate data is used, it can lead to unfair outcomes.**

- Who is responsible for ensuring the correctness of information?

Scenario: you are applying for a loan for a car and the bank uses your credit score to decide. If the credit bureau has **incorrect** information about missed payments, your score may be negatively impacted and be lowered if incorrect.

- Issue: You might be denied the loan or get higher interest rates because of wrong data.

- Ethical Dilemma: **Who is responsible for ensuring data is accurate**—the person, the company collecting the data, or a third party? Ensuring data accuracy is essential to avoid unfair treatment.

What to think about?

How can we ensure **data accuracy**, especially when handling large volumes of information?

- Who should be held accountable when incorrect data leads to negative consequences?
- How can affected individuals correct inaccurate information?

## Property

- Ethical Concern: Who owns information and the rights to use it? How is intellectual property protected in the digital age?

- Explanation: **Property** deals with the ownership and distribution of information.

**Property** deals with who owns the data and who has the right to sell, share, or use it.

In the digital world, this concept also extends to intellectual property, like software or digital content.

Example: A software company that creates proprietary software faces challenges in protecting its **intellectual property from piracy or unauthorized access.**

Things to think about

**Who owns digital data (e.g., companies, users, governments)?**

- How should **intellectual property laws adapt** to new forms of digital information?

- What is the fair balance between **information being freely accessible** and **protecting the rights of creators**?

## Accessibility

Ethical Concern: **Who has the right or ability to access information, and how is it controlled?**

Accessibility is about the **right to obtain and use information**. Accessibility is also about ensuring equal access to information and technology for everyone, regardless of social or financial status.

**Example:** students in a rural community don't have access to the internet, while students in urban areas have high-speed connections.

- Issue: The rural students are at a disadvantage because they can't access the same learning resources.

## Things to think about

Who should have access to certain types of information?

- How can we ensure equitable access to information for marginalized groups?
- Should there be limitations on accessing certain information (e.g., in cases of national security or intellectual property)?

## Here is a breakdown

**Privacy** Who can access your personal information? Social media sharing, location, data, <- this is all data. Should companies collect and share user data without permission?

**Accuracy** is the data correct and reliable? Incorrect credit information can affect a loan approval Who is responsible for fixing inaccurate data?

**Property** Who owns and controls the data? Streaming services controlling digital content, Should customers have full control over purchased content?

**Accessibility** Can everyone access the information equally? Lack of internet in rural areas, unauthorized access

Here is a few more examples

## Privacy

Scenario: A healthcare company collects personal health information through its app. After **a data breach**, sensitive **patient data is leaked online**.

This action here, raises **privacy** concerns because information was leaked

## Accuracy

Scenario: An brokerage at a bank uses an online platform algorithm system to recommend products based on user credit. However, a glitch causes the system to **misinterpret data, suggesting misleading products** to some customers.

This actually here would be an **accuracy** issue because there was a glitch that misinterpreted the data that was given and sent out misleading data.

## Property

Scenario: A software company develops a popular application and later discovers that a **competitor has copied its code without permission**.

This action here would be property because a company develop the application Since they develop the application, **(they own the application)** and another entity, which is the competitor copied the application **(the competitor does not own the application and no rights were stated)**, without any consent or permission.

## Accessibility

Scenario: A cloud service provider **experiences an outage, preventing** customers from **accessing** their data for several days.

This action, right here would be accessibility because the outage prevented the customers from accessing their data.

CIA Traid it is definitely on the test for this section. It was mostly scenario based questions. The CIA model is easy for me because of previous classes. The section of cypress security questions. I did really good in. I excel it, but just in case you may have issues in this area, I will explain this model the best I can

# What is the CIA?

The CIA Triad is a foundational model in information security that stands for **Confidentiality, Integrity, and Availability**. Each component is essential for protecting information and ensuring that systems function properly.

## Confidentiality

**Confidentiality** ensures that sensitive **information is accessed only by authorized individuals**. This is often achieved through encryption, access controls, and authentication measures.

**Example:** A healthcare provider stores patient records in an **electronic health record (EHR)** system. To maintain **confidentiality**, the provider **implements strong access controls that restrict access to patient information to only authorized medical personnel**. They also use **encryption** to protect data both in transit and at rest.

If a **hacker gains unauthorized access to the EHR system and steals patient data**, it could lead to identity theft and breaches of patient privacy, violating regulations like **HIPAA**. The healthcare provider could face significant penalties and reputational damage.

## Integrity

Integrity involves **ensuring that information is accurate and reliable**. It means that **data cannot be altered or deleted by unauthorized individuals**, and there are measures in place to detect any unauthorized changes.

**Example:** A financial institution maintains transaction records for its clients. To ensure data integrity, the institution implements **checksums** and **hash** functions to verify that transaction records remain unchanged. They also maintain **audit logs** that track who accessed or modified the data.

If an employee attempts to **alter** transaction records to cover up fraudulent activities, this goes against **integrity**.

## Availability

**Availability** ensures that **information and systems are accessible** when needed by authorized users. This includes having robust systems in place to prevent downtime and **mitigate** the effects of disasters.

Example: An e-commerce website experiences a **Distributed Denial of Service (DDoS) attack**, causing the site to become **unavailable** to customers. To ensure availability, the company implements DDoS protection solutions and has a **disaster recovery plan** that includes backup servers.

A financial company faced a **distributed, denial of service attack DDoS, and a ransomware** attack hacker also wants a payment for the code to be released to access the website this attack made their platform to be **in accessible** and now customers can't access their accounts.

**CIA for end user:** security education for employees, and contract worker they should understand security and follow policies. user authentication methods should be used for all users. Installation, of antivirus software to scan for virus signature. There should be data encryption protection.

**CIA for applications:** single factor authentication should be required for everyone. Second factor authentication requires a second credentials of something you know something you have or something you are. User accounts and rules users can perform their duties and no more. Use data encryption to protect sensitive data from unauthorized access.

**Multifactor authentication(MFA)** is a security process that requires you to provide two or more different types of information to verify your identity when accessing an account or system

**Something you know:** like a password or a pin

**Something you have:** like a smart phone, laptop, or tablet.

**Something you are:** fingerprint facial and voice recognition



Note: also pay attention to bold it and study it because those terms are also on the test with their own set of scenario questions .

For the above scenario, for **confidentiality** , the protection laws are **copyright patent and trademark**. Also understand what intellectual property is.

**Copyright** protects original works of authorship, such as books, music, art, and films. It gives the creator exclusive rights to use, reproduce, and distribute their work for a certain period of time. Copyright does not protect ideas, only the expression of those ideas.

**Patent** protects inventions and processes. It gives the inventor exclusive rights to make, use, and sell their invention for a limited time (usually 20 years from the filing date).

**Trademark** protects symbols, names, and slogans used to identify goods or services. It helps consumers distinguish between different brands and prevents confusion in the marketplace. Trademarks can last a really long time if they are in use and protected.

**Software copyright protection** is a legal mechanism that safeguards the original code and expression of a software program, preventing unauthorized copying, distribution, or modification of the software by others.

Patent infringement

**Risk Assessment** and **security policies** should be studied just terms.

Know the term: **BYOD Bring Your Own Device** policy - When employees bring their personal devices to connect to an organizations network and access to perform their job.

Now I'm again, will explain the above copyright pattern and trademark so there's a better understanding because it revolves around what intellectual properties are

**Intellectual property (IP)** refers to **creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce.** It gives creators exclusive rights to use and profit from their creations.



Copyright: Protects **original works of authorship, like music, books, and movies.**

Example: Your favorite musician writes a song. They **own the copyright to that song**, meaning **others cannot legally copy, perform, or sell it without permission.** If a movie studio uses that song in a film without getting permission, they could be sued for **copyright infringement.**

Trademark: Protects **brands, slogans, and logo designs that distinguish goods or services.**

Example :Think about Nikes logo. If another company tries to sell shoes using a similar logo, consumers might confuse it with Nike. Nike can take legal action for trademark infringement to protect their brand identity.

Patent: Protects **inventions and gives the inventor exclusive rights to their creation.**

Example : an engineer invents a new type of solar panel that is more efficient than existing ones. They can apply for a patent, which would prevent others from making, using, or selling the panel without their consent for a certain period of time (usually 20 years).

Trade secret: Protects **confidential business information that provides a competitive edge.**

A restaurant might have a secret recipe for a special sauce that is a major draw for customers. As long as the recipe is kept secret and not publicly disclosed, the restaurant can protect it as a trade secret. If an employee shares the recipe with a competitor, that could lead to legal action.

This sums up **intellectual property** both terms and simplified

## More terms

**Acceptable Use Policy (AUP)** is a set of rules that outline how to use an organization's digital resources, such as a website, network, or software. AUPs are a key part of an organization's information security policies and are designed to protect assets, ensure security, and maintain a productive work environment.



**Software piracy** is when there is an unauthorized, distribution or reproduction of software So just copying software with the permission, downloading part versions from the Internet are using a single license to install software on multiple computers software is illegal and violates copyright laws which protects the rights to software developers and companies

The **Fair Use Doctrine** is a legal principle in U.S. copyright law that allows limited use of copyrighted material without needing permission from the copyright owner. It is designed to balance the interests of copyright holders with the public's interest in the dissemination of information and creative expression.

**Example:** A popular example of fair use occurred in the case of *Campbell v. Acuff-Rose Music, Inc.* (1994). The rap group 2 Live Crew created a parody of Roy Orbison's song "Oh, Pretty Woman." The Supreme Court ruled that the parody constituted **fair use**, emphasizing that it was transformative and did not harm the market for the original song.

The **Fair Use Doctrine** allows for flexibility in the use of copyrighted materials, fostering creativity and the free exchange of ideas.

The **General Agreement on Tariffs and Trade (GATT)** is a global trade framework established in 1947 to promote international trade by reducing barriers like tariffs, quotas, and subsidies.

**GATT** was a set of rules that helped countries trade goods more easily by cutting taxes and trade restrictions, leading to smoother global trade.

The **World Intellectual Property Organization (WIPO) Copyright Treaty (WCT)** is an international agreement that protects the rights of authors and their works in the digital environment. The WCT was adopted in 1996 and went into effect in 2002. It provides additional protections for copyrights in response to the advances in information technology since the creation of previous copyright treaties.

The **Digital Millennium Copyright Act (DMCA)** is a U.S. law enacted in 1998 that aims to protect copyright in the digital age.

**Copyright Protection:** The DMCA strengthens copyright protections for digital content, making

it illegal to bypass copyright protections, such as digital rights management (DRM).

2. **Safe Harbor Provision:** It provides immunity to online service providers (like websites and platforms) from liability for user-uploaded content, as long as they follow specific procedures, such as removing infringing content when notified.

3. **Notice-and-Takedown System:** Copyright owners can send a DMCA takedown notice to platforms to request the removal of infringing material. Platforms must act quickly to avoid penalties.

4. **Anti-Circumvention:** The act prohibits the unauthorized circumvention of copyright protection technologies, such as software or tools used to access restricted content.

The **DMCA** helps **protect copyright holders in the digital environment while providing a framework for online platforms to handle copyright issues**, balancing the interests of creators and users.

**The Leahy-Smith America Invents Act** enacted in 2011, is a significant reform of the U.S. patent system.

Here is a breakdown

**First-Inventor-to-File:** The AIA changed the patent system from “first to invent” to “first inventor to file.” This means that the first person to file a **patent application for an invention is granted the patent, regardless of when the invention was actually created.**

**International Patent Cooperation:** The AIA aligns U.S. patent laws more closely with international standards, making it easier for inventors to seek protection in multiple countries.

**Example:** an inventor, named Jane, who creates a new type of solar panel, which is created Under the old system. Now with the new system if another inventor, Tom, invents a similar solar panel but files for a patent first, he could claim the patent even if Jane invented it earlier.

Under the AIA, if Jane files her patent application first, she is granted the patent, regardless of Tom’s invention date. This change encourages inventors to file for patents sooner and provides clarity in patent ownership.

## Trade Secret

A **trade secret** is any information that a company keeps confidential to maintain an advantage over competitors. This can include formulas, practices, processes, designs, instruments, or customer lists that are not publicly known.

## Trade Secret Law

**Trade secret law** protects this confidential information from being disclosed or used without permission. In the U.S., trade secrets are protected under both state laws (like the **Uniform Trade Secrets Act**) and federal law (the **Defend Trade Secrets Act**).

Trade secrets are crucial for businesses, and trade secret laws protect these valuable assets from unauthorized use and disclosure, helping companies maintain their competitive edge.

**Example:** Trade secrets are crucial for businesses, and trade secret laws protect these valuable assets from unauthorized use and disclosure, helping companies maintain their competitive edge.

**\*\*Also know the term uniform trade secret act \*\***

The word **espionage** and the terms that follow were mentioned in the OA too.

Know and Study



**Economic Espionage Act (EEA)** ←

The **Economic Espionage Act (EEA)** is a U.S. law enacted in 1996 to **address the theft of trade secrets and economic espionage**. It makes it a **federal crime to steal, misappropriate, or knowingly receive trade secrets for commercial advantage**.

1. **Criminal Offense:** The act criminalizes the theft of trade secrets and provides severe penalties, including fines and imprisonment.

2. **Protects Businesses:** It aims to protect U.S. companies from foreign and domestic espionage that harms their competitive position.

3. **Federal Jurisdiction:** The EEA allows federal authorities to prosecute cases involving trade secret theft, even if the theft occurs in a foreign country.

The **Economic Espionage Act** serves to **deter and punish the theft of trade secrets**, protecting the economic interests of U.S. companies and maintaining fair competition in the marketplace.


For more on laws, it is helpful to use the **courses chapter 6 PowerPoint**, which would help you with all the terms. They're pretty simple. I only took the terms that were a challenge on the exam. For the rest, which is just the basic cyber security, you can use the **chapter 3 PowerPoint** in the course. I will break down in a few more terms that can be challenging on the exam.



## Cyber Espionage:

**Cyber espionage** involves the **covert theft of sensitive information**, often for political, military, or commercial advantage. It typically targets government or corporate data.

- Motivation: Primarily driven by the desire to gain intelligence or competitive edge.
- Tactics: Involves hacking, phishing, and other means to infiltrate systems without detection.

**Example:** A nation-state hacks into another country's defense contractor to steal plans for advanced weapon systems. 

## Cyber Terrorism:


**Cyber terrorism** involves **using the internet to conduct violent acts or threaten public safety, aiming to intimidate or coerce societies or governments.**

- Motivation: Driven by ideological, political, or religious goals, often intending to instill fear or disrupt critical infrastructure.
- Tactics: Can include hacking into critical systems (like power grids) to cause physical harm or instigate panic.

**Example:** A terrorist group takes control of a city's water supply system, contaminating the water to cause harm and instill fear among the population.

**cyber espionage seeks to gain information**, while **cyber terrorism aims to instill fear and cause harm.**

**Vulnerability** is a weakness in a system or software that can be exploited by attackers. Vulnerabilities allows hackers to steal information disrupt services and or cause harm other.

Read on the sections of EXPLOITS this section is easy also use the chapter 3 PowerPoint very helpful. 

The different types of cyber attacks are also a very easy section if you have taken previous classes on it, but even if you haven't, they're very easy to remember that one section that I pass On the OA.