After Mid 2

**Freedom of Expression on the Internet**

The internet gives people the freedom to share news, ideas, and information. It also lets people talk about different topics openly, sometimes without revealing their identity.

But with this freedom, people also have to use it carefully and respectfully. To help guide people, governments and companies have made rules to protect both users and their own interests.

In the U.S., the First Amendment protects the right to free speech. Some state and federal laws that tried to limit this right have been struck down because they went against this basic freedom.

Definition of Free Speech

Free speech means you can express your ideas and opinions in different ways. This includes speaking, writing, using gestures, signs, or symbols. It also means you can share your thoughts without revealing your identity (anonymously). Free speech protects all opinions, even those that most people might not agree with, so everyone has a chance to be heard.

**What’s Not Protected by the First Amendment:** Some types of speech are not protected because they can cause harm. These include:

* Lying under oath (perjury)
* Cheating or lying for personal gain (fraud)
* Damaging someone’s reputation with false claims (defamation)
* Extremely offensive or inappropriate speech (obscene speech)
* Creating unnecessary panic (incitement of panic)
* Encouraging illegal actions (incitement to crime)
* Words meant to provoke violence ("fighting words")
* Actions or speech that aim to overthrow the government (sedition)

**In IT, Obscene Speech and Defamation Matter:**

Online, issues like obscene speech and defamation are especially important, as they can spread quickly and cause harm.

**Obscene Speech** Obscene speech means using words or pictures that most people think are rude or inappropriate. It often includes indecent or adult content. This type of speech is not allowed because it can upset people and harm public values

**Defamation** Defamation happens when someone says or writes false things about you that hurt your reputation. For example, spreading lies about you online so others think badly of you. It’s a big problem because false information can spread fast and cause long-term harm.

**Freedom of Expression: Key Issues**

There are several important issues related to freedom of expression on the internet, such as:

* **Controlling access to information**: Managing what content is available online, especially to protect children from harmful material.
* **Anonymity online**: The ability to use the internet without revealing your identity.
* **Defamation and hate speech**: Making false statements that harm someone’s reputation or spreading harmful, discriminatory speech.
* **Corporate blogging**: Businesses using blogs to communicate with customers, share information, or promote products.
* **Pornography**

**Controlling Access to Information on the Internet**

It’s hard to manage freedom of speech on the internet because children can easily find harmful content.

To protect children, there are laws and software that block inappropriate material.

* Communications Decency Act (CDA) 1996: This law tried to protect children from pornography, but it was too unclear and was ruled unconstitutional in 1997.
* Child Online Protection Act (COPA) 1998: This law targeted websites that showed harmful content to kids, but it was also ruled unconstitutional in 2004.

**Internet Filtering**

**There are different ways to block bad content:**

* Software filters: These programs, installed with web browsers, block websites with harmful content.
* URL filtering: Blocks specific website addresses that are inappropriate.
* Keyword filtering: Blocks websites that contain certain words or phrases.
* Dynamic content filtering: Checks a website's content before showing it to make sure it’s safe.

**Popular Internet Filters**

Some well-known filters for home users include:

* NetNanny Parental Controls
* PureSight PC
* CYBERsitter
* SafeEyes
* CyberPatrol

**ICRA Rating System**

The ICRA system lets website owners rate their content through a questionnaire. This creates a content label that browsers can use to help users decide what’s okay to view.

**ISP Blocking**

Internet Service Providers (ISPs) can block certain websites directly from their servers. Tools like ClearSail/Family.NET can stop users from accessing these websites, and the blocked sites list is updated regularly.

**Children’s Internet Protection Act (CIPA)**

CIPA requires schools and libraries that get federal funding to block access to:

* Obscene material
* Pornography
* Anything harmful to minors

To get internet discounts, schools and libraries must:

* Use filters to block obscene or harmful pictures
* Monitor what minors do online
* Limit minors’ access to harmful material

CIPA doesn’t require schools or libraries to track how minors or adults use the internet.

An **acceptable use policy** is important, and everyone involved (students, parents, employees) must sign it.

It’s harder for libraries to follow CIPA because they serve people of all ages, including adults who have First Amendment rights.

**Anonymity on the Internet**

Anonymity means sharing opinions online without showing your identity. It helps people express their views without being afraid of punishment, which is an important right in free societies.

In countries where free speech is not allowed, being anonymous is even more important. It has also been important in U.S. history, like during the American Revolution.

But, anonymity can be misused for illegal or harmful actions.

**History of Anonymity**

During the American Revolution, people who did not agree with British rule used anonymous pamphlets to share their opinions. In England, there were laws that punished people for secretly sharing political ideas.

A famous case in 1735 was about a printer named John Zenger. He was charged for printing anonymous writings that criticized the governor of New York. However, the jury did not punish him. This became an important moment for the freedom of the press.

**Legal Cases About Anonymity**

It took nearly 200 years for the U.S. Supreme Court to rule on anonymity as part of the Bill of Rights. In 1958, the Court decided in **NAACP v. Alabama** that the NAACP didn't have to share its membership list because it could lead to threats.

**Anonymity on the Internet Today**

Being anonymous online helps people:

* Get help in online support groups
* Report problems with products
* Take part in sensitive discussions

But some people argue against anonymity because it can be used for:

* Defamation (hurting someone's reputation)
* Fraud (lying for personal gain)
* Libel (spreading false information)
* Exploiting children

**Anonymous Remailer Service**

An anonymous remailer is a tool that hides the sender’s email address and sends the message to the recipient without revealing who sent it. This keeps the sender’s identity secret. What the sender says, whether it’s good or bad, is their choice.

**Blocking Remailer Services**

Companies can block their employees from using anonymous remailers by setting up special firewalls. They can also send warnings if an employee tries to use one.

**John Doe Lawsuit**

If someone shares harmful information or secrets online without showing their name, it can hurt a company’s reputation. Because it’s hard to know who did it, the company can file a John Doe lawsuit to find out who the person is.

The court can send legal orders, called subpoenas, to websites or internet service providers (ISPs) to help identify the person.

**John Doe Lawsuit in Action**

In 1999, Raytheon, a company, sued 21 anonymous people who shared private company information online. The court gave Raytheon permission to get information from Yahoo! and internet providers to find out who the people were. All 21 were identified—some chose to leave the company, and others were warned not to share private details again.

Big companies like America Online and Verizon get over 1,000 legal requests (subpoenas) each year to reveal the identities of anonymous users. Some people think a person’s identity should only be revealed if they are proven guilty of something, like spreading lies (libel).

However, anonymity can be misused by people who try to manipulate stock prices or harm a company’s reputation.

**Pre-Paid Legal Case**

In the Pre-Paid Legal case, the company wanted the names of anonymous users who criticized them on a Yahoo! message board. They asked for this information to check if the users were breaking rules by sharing secret company information

**EFF Defends Anonymity**

The **Electronic Frontier Foundation (EFF)** defended the anonymous users. They said the users were just giving their opinion and not revealing secrets. The EFF warned that exposing them could punish free speech.

**When Can Identities Be Revealed?**

A court will only reveal someone's identity if:

1. The request is for a good reason.
2. The information is important to the case.
3. There is no other way to get the information.
4. The information is directly related to the case.

In **2001**, a judge ruled that Yahoo! didn’t have to reveal the identities of the users in this case.

**Defamation and Hate Speech**

**Hate Speech That Can Be Prosecuted**(Prosecuted means being taken to court because someone believes you broke the law. If you are prosecuted, legal action is taken against you, and a court decides if you are guilty or not)

* Threatening or scaring specific people online
* Sending private threats through email or messages
* Posting online about hurting someone
* False statements that damage someone’s reputation (libel)

Annoying or offensive speech is usually allowed by law. But if the speech includes threats or bullying, legal action can be taken. Internet companies can also remove harmful content if it breaks their rules.

**ISPs and Content Removal**

* Internet companies (ISPs) can remove harmful content if it breaks their rules, and this doesn't go against free speech laws. They have to keep an eye on what people post and take action if the rules are violated.

**Public vs. Private Institutions**

* Public schools and universities must follow the law about free speech.
* Private schools and companies can stop people from posting offensive content.

**Example: Hate Speech in the U.S.**

* A student was sent to prison for sending racist death threats to Asian American students.
* **Hate Speech in Other Countries**In some countries, like Germany, hate speech is against the law, such as promoting Nazi ideas or denying the Holocaust. In 2009, people who posted hateful messages about a man in Australia were in legal trouble.
* **Hate Speech Across Borders**If someone in the U.S. posts something online that is illegal in another country, they can still be charged there. But in the U.S., speech that is allowed by U.S. laws is protected, even if it breaks laws in other countries.

**Blogging** is when anyone writes and shares posts online about any topic, like personal experiences, hobbies, or interests.

**Corporate Blogging** is when employees or companies write blogs to talk about their business, share updates, connect with customers, and improve the company’s image. It’s more focused on work-related topics.

**Corporate Blogging**

Some companies allow their employees to have personal blogs to:

* Connect with customers, partners, and coworkers
* Improve the company’s image
* Talk about work-related topics
* Share ideas or get feedback

Blogs let employees share their honest thoughts, including criticism of company policies.

**Risks of Corporate Blogging**

But, employees might:

* Share company secrets
* Break rules about security

**Guidelines for Safe Blogging:**

* Don’t share confidential company information
* Make your posts interesting
* Be real and authentic

**Example of a Corporate Blogging Issue**

Mark Jen worked at Google and started a blog to share about his job. He wrote about his first day, meetings, and even Google’s future plans. His blog became very popular, with thousands of readers.

After a week, Mark’s blog was removed because he shared too much private information about Google. He was fired, and this caused rumors that hurt Google’s image. After this, many companies made their own rules about blogging.

## **Why is Privacy Protection Important?**

* **Systems and Data**:
  + Businesses collect and store data during interactions with customers.
  + Data helps make better decisions, such as approving loans or hiring candidates.
* **Global Competition:**

To stay competitive, companies need to understand customer habits, like what they buy and their financial situations. This information helps companies target their marketing more effectively, reaching the right people with the right products or services

### **Example:**

A credit card company tracks spending patterns to identify customers likely to need a loan, sending personalized offers to them.

## **Challenges with Data Collection**

**Concerns:**Many people are worried about how governments and businesses collect their personal data. Internet users fear their privacy might be violated, and some people avoid using the Internet because of these concerns.

**Need for Balance:**While businesses and governments need data to work, there must be limits to protect privacy. A balanced approach is needed, which includes:

* **New laws**
* **Technical solutions**
* **Clear and honest privacy policies**

## **Historical Perspective: The Right to Privacy**

**Constitutional Questions:**In the past, people worried if a strong government would invade their privacy.

**Fourth Amendment:**The Fourth Amendment protects people from unfair searches. It also says that people have a "reasonable expectation of privacy," meaning you should expect privacy unless you're in a situation where it’s not expected.

**Key Concept:**If you don’t expect privacy in a situation, the law doesn’t protect it.

## **Privacy and Private Industry**

Few laws protect individuals from how private companies use their data. Companies mainly follow their own privacy policies and industry rules.  
*Example*: An online retailer may promise to use customer data only for shipping and ads, but legal checks are limited.

**Definition of Privacy**Privacy is the right to be left alone, a key part of a free society.

**Components of Information Privacy**

1. **Communications Privacy**: Protects private conversations.  
   *Example*: Using secure messaging apps.
2. **Data Privacy**: Controls who can access your personal info.  
   *Example*: Choosing who can view your social media profile.

## **Privacy Laws, Applications, and Court Rulings**

**Legislative Overview**Over the past 40 years, privacy laws have mainly aimed to prevent government intrusion.

**Gaps in Protection**

* No laws completely stop companies from misusing personal data.
* No national policy or organization exists to guide businesses on privacy rules.

### **Financial Data**

* People share financial data to use services like credit cards, bank accounts, and loans. The risk is losing privacy or having money stolen if sensitive information, like PINs or account numbers, is not handled properly. Consumers are concerned about how safely companies manage their financial data.

#### **Key Laws for Financial Privacy:**

1. **Fair Credit Reporting Act (1970):** Regulates credit-reporting companies.
2. **Fair and Accurate Credit Transactions Act (2003):** Gives people free credit reports once a year.
3. **Right to Financial Privacy Act (1978):** Protects customer financial records from unauthorized government checks.
4. **Gramm-Leach-Bliley Act (1999):** Sets rules for financial privacy:

* **Financial Privacy Rule:** Companies must inform customers about their privacy policies and choices for sharing data.
* **Safeguards Rule:** Companies must show how they protect customer data.
* **Pretexting Rule:** Stops people from accessing personal data without permission.

### **Health Information**

* Widespread use of electronic medical records raises concerns about privacy breaches.
* Risks include misuse of health data by employers, insurers, or marketers.

#### **Key Laws for Health Privacy:**

**Health Insurance Portability and Accountability Act (HIPAA) (1996):**

* Makes it easier to move health insurance between jobs.
* Reduces fraud and abuse in health care.
* Simplifies the way health insurance is managed.

**American Recovery and Reinvestment Act (2009):**

* Strengthens privacy protection for electronic health records.
* Provides extra protection for people affected by data breaches.

### **State Laws on Security Breach Notifications**

* Over 40 states require organizations to disclose security breaches.
* Some states have strict rules on reporting breaches to affected individuals.

### **Children’s Personal Data**

**Children’s Online Privacy Protection Act (COPPA) (1998):**Websites for kids must:

* Have clear privacy rules.
* Tell parents how they collect data.
* Get parents' permission before collecting data from kids under 13.

**Family Education Rights and Privacy Act (FERPA) (1974):**Parents have the right to see their child’s education records. When the child turns 18, these rights go to the student.

**Electronic Surveillance**Electronic surveillance includes laws about the government monitoring things like phone calls, emails, and other types of communication. These laws were updated because of concerns about terrorism and advances in technology.

* **Communications Act of 1934**The Communications Act of 1934 created the Federal Communications Commission (FCC) and controls how radio, TV, and communication between states are used.
* **Wiretap Act of 1968**The Wiretap Act of 1968 regulates how phone calls and conversations can be listened to, and over time, it was updated to cover new technologies.
* **Foreign Intelligence Surveillance Act (FISA) of 1978**The Foreign Intelligence Surveillance Act (FISA) of 1978 explains how to collect information about foreign governments and focuses on international communications.
* **Electronic Communications Privacy Act (ECPA) of 1986**The Electronic Communications Privacy Act (ECPA) of 1986 protects messages like emails and texts while they are being sent or stored and stops the collection of phone numbers without a warrant.
* **Communications Assistance for Law Enforcement Act (CALEA) of 1994**The Communications Assistance for Law Enforcement Act (CALEA) of 1994 requires phone and internet companies to help law enforcement monitor communications, including newer tech like wireless internet and email through radio signals.
* **USA PATRIOT Act (2001)**The USA PATRIOT Act (2001) gives law enforcement more power to access phone, email, financial, and medical records but has been criticized for reducing privacy protections and allowing sensitive data to be collected without a warrant.

## **Export of Personal Data**

When personal data is shared between countries, there are rules to protect how it’s stored and used.

### **Key Guidelines and Rules**

The Fair Information Practices (1980) were made by the OECD. They include 8 rules to help use people's data fairly and safely.

The European Union Data Protection Directive says businesses in the EU must follow strict rules for using personal data. It also makes sure data sent outside the EU stays safe. But, some worry that the U.S. government could use the USA PATRIOT Act to access data from Europe stored in the U.S.

## 

## 

## **Access to Government Records**

1. **Government’s Data Capacity**Governments collect and store a lot of data about people and how the government works. This includes personal records and other important information.
2. **Freedom of Information Act (FOIA)**The FOIA lets people see certain government records. It helps make the government more open and accountable.
3. **Privacy Act of 1974**The Privacy Act stops government agencies from keeping personal data systems hidden. It sets 12 rules for how government agencies must handle people’s records.

**Exceptions** This law does not apply to the CIA, law enforcement agencies, or private companies

## **Local Scenario: Pakistan**

**Privacy in Pakistan**

In Pakistan, **Article 14(1) of the Constitution** protects privacy and dignity, while the **Electronic Transaction Ordinance (2002)** highlights data privacy. However, strong rules are missing. The **Prevention of Electronic Crimes Act (2016)** requires storing user data for 90 days but lacks strong safeguards. Pakistan has no **Privacy Commission**, and a proposed data protection law is still under review. This shows privacy is recognized but not well-protected.

## **International Scenario: United Kingdom**

The **New Data Protection Bill** replaces the old 1998 law and introduces stricter rules for protecting personal data. It requires companies to report any data breaches to the **UK Information Commissioner’s Office** within **72 hours**. Companies that fail to follow these rules face stricter penalties.

# **Key Privacy and Anonymity Issues**

### **Main Concerns**

1. **Identity Theft**
2. **Electronic Discovery** (searching electronic data for legal use)
3. **Consumer Profiling** (tracking customers’ habits and preferences)
4. **Responsible Handling of Customer Data**
5. **Workplace Monitoring**
6. **Advanced Surveillance Technology**

## 

## **Identity Theft**

Identity theft happens when someone steals your personal information to pretend to be you.

* What Information Thieves Steal

Information thieves target personal details such as your **name, address, and date of birth**. They also steal sensitive data like your **Social Security Number, passport number, and driver’s license number.** In some cases, they may use details like your **mother’s maiden name** to access accounts or verify your identity.

### **What Thieves Do With Your Identity:**

* Open new credit cards or bank accounts.
* Rent apartments.
* Set up phone or utility services.
* Register for college courses.

### **Fast Facts:**

* Identity theft is the **fastest-growing fraud** in the U.S. To fight it, consumers and organizations are using tools like **credit monitoring services**, learning to **recognize phishing attempts**, and adopting **better security systems and practices**.

### **How Identity Thieves Operate:**

1. **Data Breaches:** Stealing information from large organizations.
2. **Buying Personal Data:** Personal data is sold illegally, such as:
   * Credit card numbers: $0.40 each.
   * Bank account login details: $10.
   * Full identity information: $1–$15.
3. **Phishing:** Tricking users into entering details on fake websites.
4. **Spyware:**
   * Software secretly installed to log keystrokes.
   * Captures usernames, passwords, and credit card numbers.

### **Protecting Yourself Against Identity Theft**

1. Destroy old digital data completely.
2. Shred important paper documents(To **shred** means to cut something into small, thin pieces)
3. Ask retailers to verify your identity (e.g., show photo ID).
4. Be cautious of “shoulder surfing” (people watching you enter passwords).
5. Avoid putting too much personal information on checks.
6. Minimize the time mail sits in your mailbox.
7. Avoid using debit cards for online shopping.
8. Use strong, hard-to-guess passwords and PINs.

### **Data Breaches** (A breach means a violation or breaking of something, such as a law, rule, or security. In the context of data breaches, it refers to unauthorized access to or theft of private information, like personal or financial data)

Thieves often target large databases to steal personal data. The causes of data breaches include **hacking** and **poor security practices** by organizations.

**California’s Notification Law (2002)** requires companies to inform people about data breaches as quickly as possible. This law was passed after a major payroll database was breached, and victims were not informed for **six weeks**.

**Phishing and Spyware**

**Phishing:**Phishing is when fake emails or websites trick you into giving away personal information, like your password or credit card number.

**Types of Phishing:**

1. **Email Phishing:** Fake emails that look real, asking you for personal info.
2. **Spear Phishing:** Fake messages made to look personal, using details about you.
3. **Vishing:** Fake phone calls asking for your personal info.
4. **Smishing:** Fake text messages asking for your details.

**Spyware:**Spyware is software that secretly watches what you do on your computer and steals your passwords and personal info. It works even if you're not online.

**Example:**In 2007, the FBI used spyware to track a 15-year-old who made bomb threats. It helped find him, and he was punished with detention and a fine.

# **Consumer Profiling**

### **What Is Consumer Profiling?**

Consumer profiling is the process where companies collect and analyze personal information about internet users to understand their preferences and habits.

### **How Companies Collect Data:**

1. **Cookies:**Cookies are small files that websites put on your device. They help websites remember you and track what you do on the site.
2. **Tracking Software:**Tracking software watches what you do online, like the websites you visit and the products you look at. It helps websites give you better suggestions or ads.

### **Ways to Limit or Stop Cookies:**

1. **Browser Settings:** Adjust the browser to block or limit cookies.
2. **Manual Deletion:** Remove cookies directly from your device.
3. **Cookie-Management Programs:** Use tools that manage or delete cookies.
4. **Anonymous Browsing:** Use private browsing modes or software that doesn’t accept cookies.

**Personalization Software in Consumer Profiling**Personalization software helps show ads and recommendations based on what you do online.

**Techniques Used:**

1. **Rules-Based Personalization:**Shows ads based on what you like or do online.  
   Example: After booking a flight, you might see ads for rental cars.
2. **Collaborative Filtering:**Suggests things based on what others like.  
   Example: If you buy a book, you might see suggestions for books by similar authors.
3. **Demographic Filtering:**Uses information like age, gender, or location to show personalized ads.  
   Example: Microsoft shows different ads to men and women.
4. **Contextual Commerce:**Shows products based on what you’re looking at.  
   Example: If you read an article on rafting, you might see ads for rafting gear.

### **Privacy Concerns in Consumer Profiling**

1. **Consumer Data Privacy:**
   * A major issue, as consumers expect their data to be protected.
   * Companies that fail to protect data risk losing customer trust and facing legal action.
2. **DoubleClick Case Study:**
   * People were upset when DoubleClick, an ad company, wanted to mix data about what people do online with their personal details from another company, Abacus Direct. This would have connected online actions with real names. Because of complaints and lawsuits, the company stopped the plan.

**Opposition to Consumer Profiling**

Critics raise concerns about:

* **Who is collecting the data:** Lack of transparency around which companies are using consumer data.
* **How the data is used:** Fear of misuse, such as intrusive advertising or unauthorized sharing of information.

### **Key Takeaway:**

While consumer profiling helps companies create personalized experiences, it raises significant privacy concerns. Users can take steps to protect their data, and companies must ensure ethical and transparent practices to maintain trust.

**Treating Consumer Data Responsibly**

### **Why Is It Important?**

Strong measures are needed to handle consumer data properly and avoid damaging customer trust.

### **What Companies Should Do:**

**Adopt Fair Information Practices**:

* Protect and share data responsibly.
* Let consumers review their personal data.
* Notify and allow opt-out if data is used for research.

**Establish a Corporate Data Policy**:

* Clearly outline how customer data will be handled and protected.

### **Role of Chief Privacy Officer (CPO):**

A Chief Privacy Officer (CPO) ensures a company’s data practices are ethical and compliant with laws.

**Key Responsibilities of a Chief Privacy Officer (CPO):**

* Train employees on data privacy.
* Create and enforce privacy policies.
* Find and fix privacy risks.
* Follow government regulations.

**Why a CPO Is Necessary:**Acting early on privacy issues saves money and prevents problems.  
*Example*: U.S. Bancorp paid $3 million to settle a lawsuit for selling customer data. They hired a CPO to avoid such issues in the future.

**Workplace Monitoring:**Employers monitor employees to ensure productivity and legal compliance. Private employees have fewer privacy rights than public ones because private companies don’t follow the Fourth Amendment. Privacy groups want stronger laws to protect workplace privacy.

**What is Surveillance?**Surveillance means watching people, activities, or places to gather information. It is used by governments, companies, or individuals for security or other purposes.

**What is Advanced Surveillance Technology?**It includes modern tools to monitor and collect data, such as:

* **CCTV cameras**: Track movements or faces.
* **Drones**: Watch from above.
* **GPS chips**: Track locations in phones or cars.
* **Biometric systems**: Use fingerprints or eye scans for ID.

**Examples:**

* **Camera Surveillance**: Cities use cameras to monitor public areas, but some worry about misuse.
* **GPS Chips**: Track locations and offer location-based services.

**Summary**Laws and technology help balance business needs with consumer rights.  
Key points:

* Identity theft is growing fast.
* E-discovery can be costly and reveal private information.
* Websites collect personal data for marketing.
* There are rules to help businesses use data fairly.
* Employers monitor workers to improve productivity.
* New technology, like cameras and GPS, gives more ways to track people, but this affects privacy.