

# Module CS5052NI

## Professional Issues, Ethics and Computer Law

2023

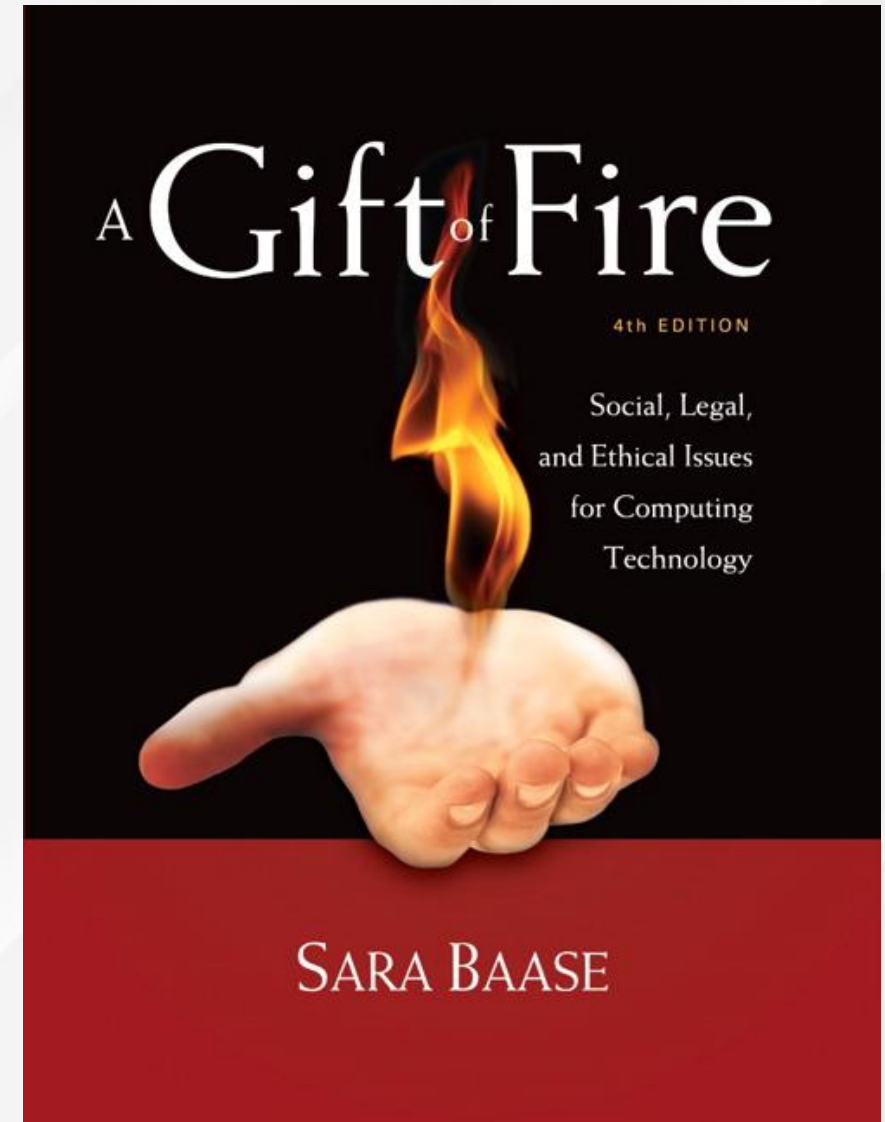
# A Gift of Fire

Fifth edition

**Sara Baase**

Chapter 2:

Privacy



# Agenda

---

- Privacy Risks and Principles
- The Fourth Amendment, Expectation of Privacy, and Surveillance Technologies
- The Business and Social Sectors
- Government Systems
- Protecting Privacy: Technology, Markets, Rights, and Laws
- Communications



# Long history of technology and internet



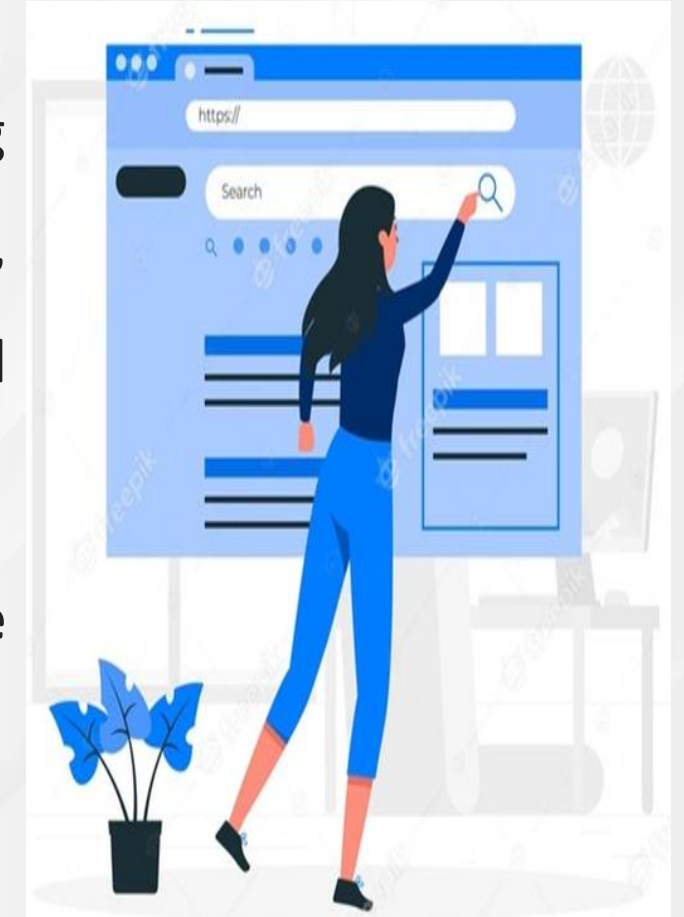
- Considered as something special, available only to tech-wizards and geeks for specific purposes such as launching NASA rockets, space study and more.

Internet Live Stats **3.5 billion of the world's population** now use the internet in their daily lives, with more than **1 billion sites on the web.**

- **90 %** of households with access to internet have **at least one device** that is **available online at any given time.**
- Rise during weekdays, **75 %** of all the **internet traffic** comes from video streaming of TV shows, movies, according to the **Cisco's Annual Internet Report of the global analysis on assessing the digital transformation**

# Why technology?

- We require technology, whether internet, laptops, or something else, for half the work we do. **From searching for the topic, conducting surveys, having discussions with the client, all require the use of the internet in some way or another.**
- If we hear a **new word** or know about a **new place**; what do we do?
- Our first thought would be **to search about it on the internet.**



# Technology

---

- The moment we go online, we start sharing our **(Internet Protocol) IP address**, which can be used as a **source to pinpoint our country and location**.
- Other information such as your **Operating System, whether we're a user of Firefox, Explorer, or Chrome for browsing** can also be tracked.
- Information like showing the **battery level** of our device at any particular point in time, or is it a **phone, a tablet, or a laptop** we are online from can also be tracked.
- This is where **privacy** is needed.

# Privacy

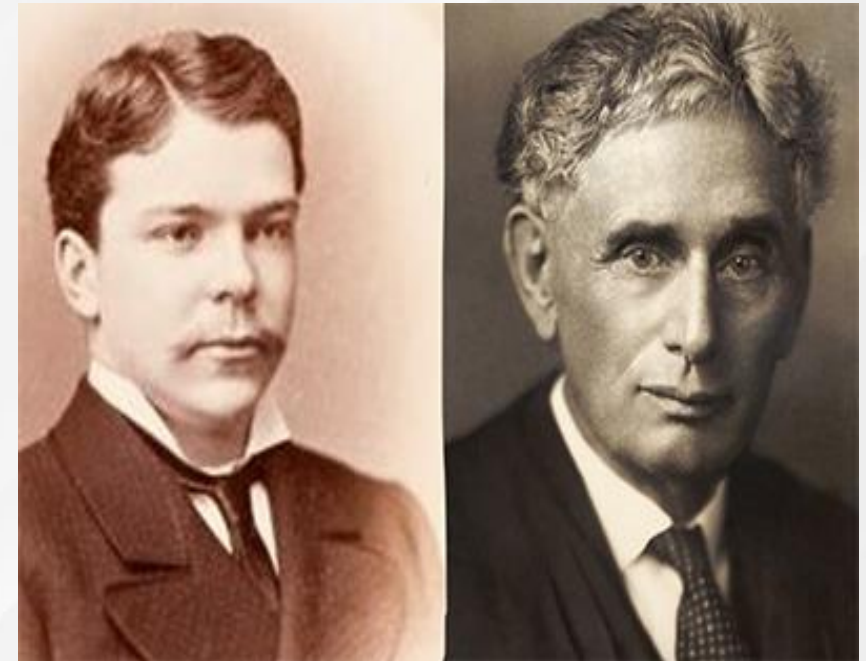
- Ability of an individual or group to seclude (isolate) themselves, or Information about themselves, and thereby express themselves selectively.
- Generated from Greek work which means division between the “polis,” or the **public**, and the “oikos,” or **private**
  - **Oikos** means an **individual’s “goods or property”**
  - This very distinction between the “**household**” and the “**public**” introduced the term **privacy**





# Modern notion of privacy

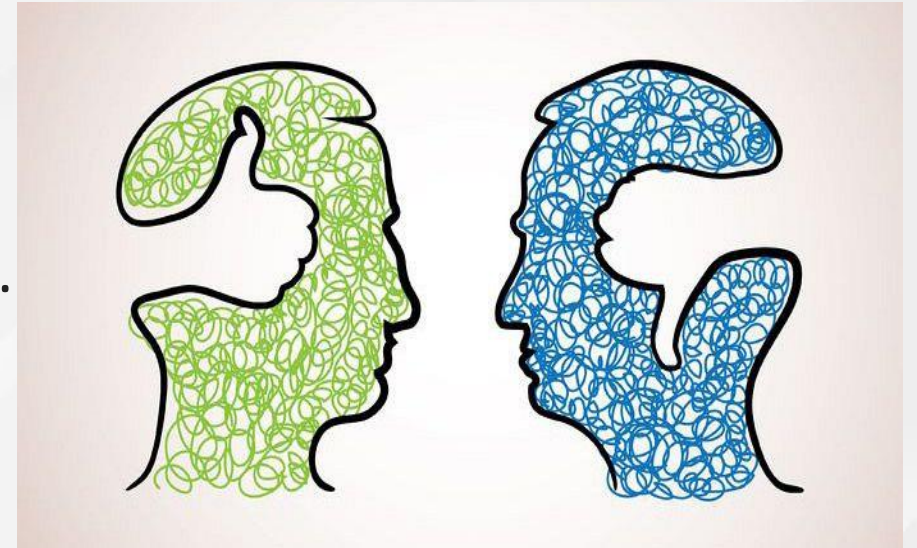
- Appeared in the famous study written by **Louis Brandeis** and **Samuel Warren** in **1890**, called “**The Right to Privacy**”.
- In their paper, they defined **privacy** as “**the right to be left alone**”. Since then, this right has become widely known and has evolved as a **fundamental human right** in our societies.





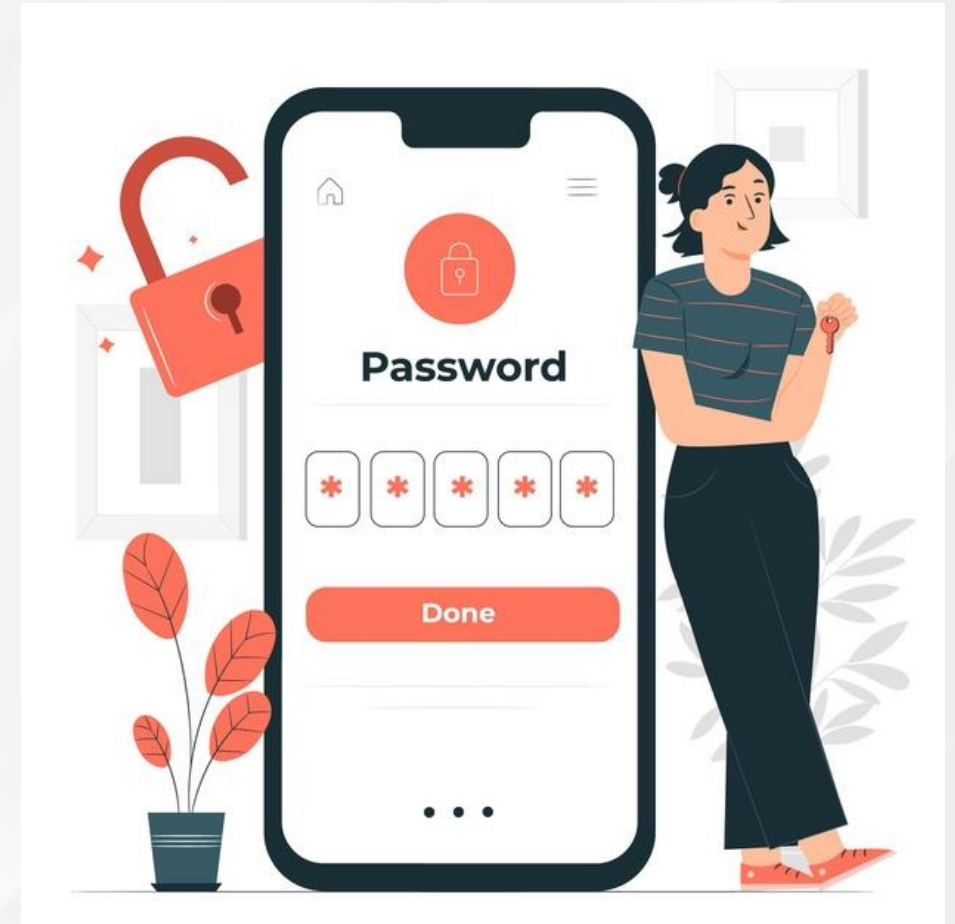
# Modern notion of privacy

- There are two types of people in the world, good and bad.
- **Bad people:** plot terrorist attacks or engage in violent criminality so have to **care about** their **privacy**.
- But, good people are responsible, who go to work, come back home, raise their family, and watch television. They have nothing to hide and no reason to fear from anyone.
- **One might argue, if you're not a bad person, and if you're doing nothing wrong, then you have nothing to hide. Right?**



# Modern notion of privacy

- Are you willing to share your browser history to the public?
- Are you willing to share all the information in phone to your parents?
- Or even the passwords of your social media account?



# Key aspects of privacy

1. **Accessibility Privacy:** This type of privacy is also known as **Freedom from Intrusion**, which is the right of any individual to be left alone.

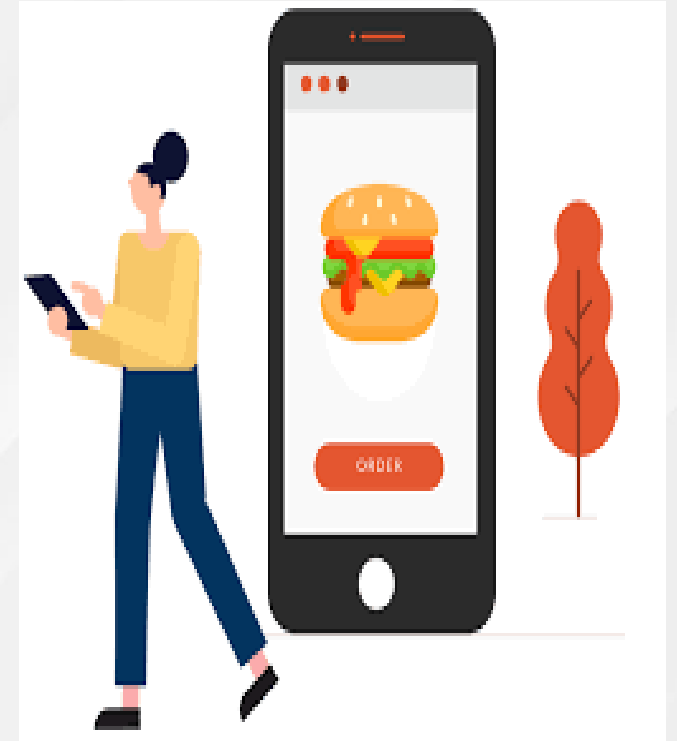
- It is also ability to be private or by yourself in some location that others are prevented from entering.
- You may have locked yourself inside your room to give you private time, if you have done so, **you are practicing accessibility privacy by not letting others enter your room.**



# Key aspects of privacy

**2. Decisional Privacy:** having freedom to make your own decisions however you please. Includes **freedom from external influence** in one's personal **choices, plans, or decisions**.

- If you have visited a restaurant with your friends but insisted on ordering your own dish instead of sharing what your friends ordered, you seem to practice **decisional privacy**.
- **Freedom from Surveillance:** Right of the individual from not being tracked, followed or watched also falls under decisional privacy.



# Key aspects of privacy

3. **Informational Privacy:** Refers to all the data about a person, including everything about the individual's data and controlling who gets to know what, and who doesn't.

- Includes **Controlling the Information** about oneself.
  - You do not share your social media accounts passwords with your teachers or friends even if you fully trust them, right?





# Threats come in several categories:

- Intentional or institutional uses of personal information
- Unauthorized use or release by “insiders”
- Theft of information
- Inadvertent leakage of information
- Our own actions





# Why privacy in technology?

- Tablets, laptops, smartphones and other wearable technologies has greatly affected our behavior. When we should wake up, how much distance should be run, can now be tracked and controlled by mobiles and watches.
- **What price are we paying for our trust and are we willing to face the consequences?**



# The price we pay...

---

- Browsing through internet, we leave behind **digital traces, or footprints**, that can be used to keep track of our activities that can be used as a source to **identify us**.
- Data like our **location, device we're using, advertisements we've clicked on**, and many more.
- No matter **how strong the privacy settings of our browser is**, certain information might be **inevitably revealed to the sites we visit**.
- Data is **collected, stored**, and may be **shared with others, with or without our consent**.

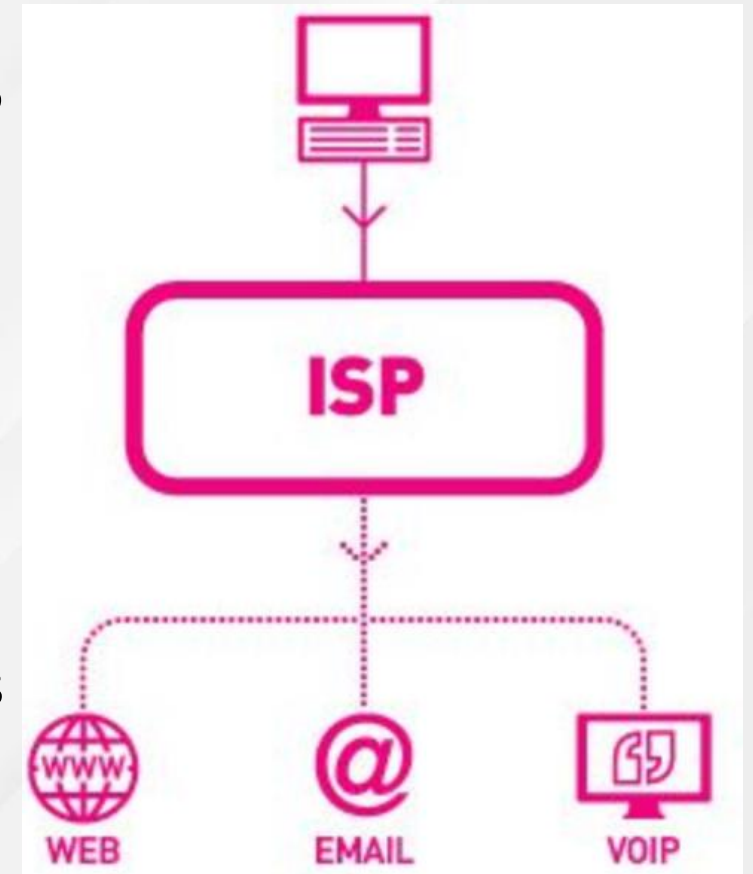
# Who collects information?

---

- **Web browsers :First party trackers.** Reveals information like if you are using web browsers on a public computers or someone's system.
  - Can save data such as **browsing history, cookies and passwords**
- **Websites:** Data collected includes the **forms, email addresses, and credit card information.** Information, like **IP addresses, user interactions** are also collected.
- **Cookies : Data packet** sent by a **server** with a **small piece of data.**
  - Used for **authenticating, session tracking and maintaining specific information** for advertising purposes

# Who collects information?

- **Internet Service Providers (ISP)** : always know your IP Address and the IP Address to which you are communicating.
- **Unique IP address** track what user does and determine our **location and track us**
- ISPs can observe unencrypted data passing between you and the Internet, but not properly encrypted data. ISPs are usually prevented to do so, due to social pressure and law



# By Email

---

- An email message can be stored at multiple locations, including on the:
  - Sender's computer, Server of your email or Internet Service Provider or Company's email (SMTP) server or Receiver's computer
- Emails may be inappropriately spread by the original receiver.
- Unlike paper documentation, the digital nature of email messages and attachments allows to be archived for long periods of time.
- Emails may be legally viewed or disclosed by services providers or authorities





# By Official Use

---

## ■ Court Records

- When you file a lawsuit for divorce or are a party to a civil lawsuit or criminal case, court records are accessible to the Public

## ■ Government

- The government may want your personal information for law enforcement purposes as well as for foreign intelligence investigations. Various laws govern these procedures.





# By Cybercrime

- **Spyware** takes advantage of security holes by attacking the browser and forcing it to be downloaded and installed and gather your information without your knowledge
- **Phishing** occurs when criminal lure the victim into providing financial data.
- **Pharming** occurs when criminals plant programs in the victim's computer which redirect the victim from legitimate Web sites to scam look alike sites.



# Apple vs FBI

---

After the 2016 terrorist attacks in the US city of San Bernardino the FBI asked Apple for the information stored on the iPhone of one of the suspects.

- However Apple's operating system is encrypted and only accessible through a pin code.
- The FBI asked Apple to modify the system to let them in.
- Apple refused opening a lively debate on the right to privacy versus security needs. The case was almost taken to court.
- But the FBI later found a vulnerability to crack the phone in privacy terms, which was a legal setback.

# US Privacy Law - Example

---

- Facebook being questioned for **illegal monopolization and privacy issues**
  - **US regulators** have reportedly voted to fine Facebook for **data breach** and **sharing users' personal information** with **Cambridge Analytica**.
- It was said that **Cambridge Analytica**, a political data firm, gained **access to information** on **50 million Facebook users**. They used this information to identify the personalities of American voters and influence their behavior to vote.
- This firm was also believed to be responsible for Brexit and many other political issues.

# UK Privacy Law - Example

---

- The Supreme court filed a lawsuit against Google for Data Privacy Fines and Damages for a £3 billion pounds lawsuit.
- The case was related to the "**safari workaround**". What had happened was, the iPhone users who used the safari web browser had tracking cookies planted in their devices secretly, without their consent.

**Why do you think these cases are happening?**

# Privacy Policy

---

- A Privacy Policy is **statement or a legal document** that states how a company or website collects, handles and processes data of its customers and visitors.
- It clearly describes whether that information is kept confidential or is shared with or sold to third parties.
- Personal information about an individual may include the following: Name, Address, Email, Phone number, Age, Sex ,Race etc.

# Terms and Conditions

## 1. When you give it to us or give us permission to obtain it

When you sign up for or use Pinterest, you give us certain information voluntarily. This includes your name, email address, phone number, profile photo, Pins, comments, and any other information you give us. You can also choose to share with us location data or photos. If you buy something on Pinterest, we collect payment information, contact information (address and phone number) and details of what you bought. If you buy something for someone else on Pinterest, we collect their delivery details and contact information.

If you link your Facebook or Google account or accounts from other third party services to Pinterest, we also get information from those accounts (such as your friends or contacts). The information we get from those services depends on your settings and their privacy policies, so please check what those are.

## Privacy Policy Sample Clauses

Google: "Log information – When you access Google services, our servers automatically record information that your browser sends whenever you visit a website. These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser. Also, in order to protect you from fraud, phishing, and other misconduct, we may collect information about your interaction with our services. Any such information we collect will only be used to detect and prevent fraud or other misconduct."



# User Consent

---

- The process where a user is asked to confirm the release of the scopes and claims that a client requests, i.e. Handing over ownership, personal information
- This is a once only kind of requirement required only once when you create a user account. In other cases, you are required to click an **‘Accept’** or **‘I Accept’** option every time you perform the task.
- This is generally common for downloading software updates as a way of checkbox.

# What do they do with the information?

---

- To **gain insights**, to **provide a personalized online experience**, and to help advertisers monetize by showing targeted advertisements to the users'.
- Privacy of some information can be **important to safety and security as well**. Examples include travel plans, financial data, and for some people, simply a home address.
- Simply to make your browsing experience **faster and more convenient**
- But is it always used for these purposes? The answer to this question is NO.
- Most of our data is mostly used by marketers or advertisers to track our browsing activities across multiple sites and serve us tailored ads.

# Solution?

---

- ~~Insulate yourself from the Internet~~
- The Only Two Absolute Choices
  - Raise awareness of Privacy
  - Learn to safeguard your privacy with a minimum sacrifice of convenience

# Platform for Privacy Preference

---

- Developed by the **World Wide Web Consortium (W3C)**,
- **Platform for Privacy Preference (P3P)** is a protocol allowing websites to declare their **intended use of information** they collect about browsing users and **allow users to configure their browsers or other software tools** in such a way that they are **notified whether web site privacy policies match** their preset preferences

# Privacy Risks and Principles

---

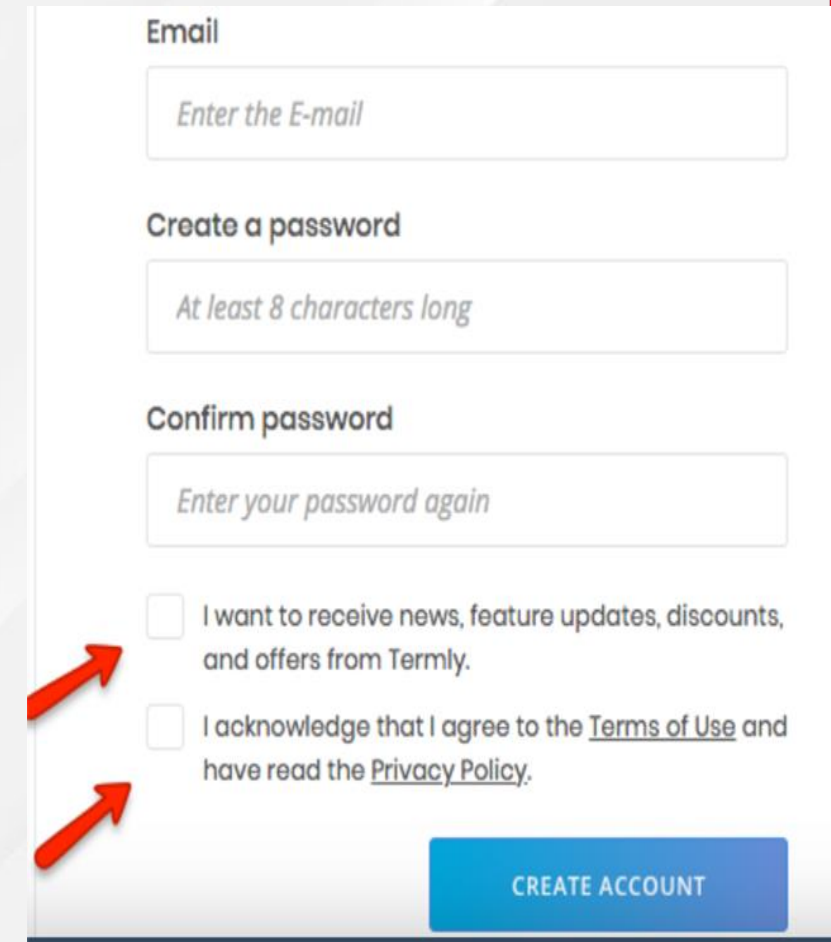
## New Technology, New Risks – Summary of Risks:

- Anything we do in cyberspace is recorded.
- Huge amounts of data are stored.
- People are not aware of collection of data.
- Software is complex.
- Leaks happen.
- Data collected for one purpose will find other uses.
- Government can request sensitive personal data held by businesses or organizations.
- We cannot directly protect information about ourselves. We depend upon businesses and organizations to protect it.

# Privacy Risks and Principles

Two common forms for providing informed consent are *opt in* and *opt out*:

- **Opting in** means that a user will take a **confirmatory action** to **offer their consent**.
- The most common way we see opt-in methods implemented is through checkboxes. When presented with a checkbox, the user must take action to check the box – which denotes their consent.



The screenshot shows a registration form with the following fields and options:

- Email**: A text input field with placeholder text "Enter the E-mail".
- Create a password**: A text input field with placeholder text "At least 8 characters long".
- Confirm password**: A text input field with placeholder text "Enter your password again".
- ☐ I want to receive news, feature updates, discounts, and offers from Termly.
- ☐ I acknowledge that I agree to the [Terms of Use](#) and have read the [Privacy Policy](#).
- CREATE ACCOUNT**: A blue button at the bottom right.

Two red arrows point to the checkboxes, highlighting the opt-in mechanism.



# Fair Information Principles

---

1. Inform people when you collect information.
2. Collect only the data needed.
3. Offer a way for people to opt out.
4. Keep data only as long as needed.
5. Maintain accuracy of data.
6. Protect security of data.
7. Develop policies for responding to law enforcement requests for data.

# Universal Declaration of Human Rights, Article 12 – United Nations

---

- “No one should be subjected to arbitrary interference with his / her privacy, family, home or correspondence, not to attacks upon his /her honour or reputation. Everyone has the right to the protection of the law against such interference or attacks” – mid 20th century.
- This simply means no one has the **right to interfere or intervene, or even violate others’ information, property, papers, or even houses as they desire**. No one is allowed to bully or **degrade others’ reputation and honor either**. But if found doing so, the victim is protected under the country’s law and can also take serious legal actions.

# The constitution of Nepal, 2021

---

- Nepalese constitution includes a total of 31 fundamental rights, which includes **freedom to live with dignity, freedom of speech and expression, religious and cultural freedom, right against untouchability and discrimination.**
- The parliament of Nepal passed the Act in July, 2007 AD called the **right to information** (RTI), which allows the people's fundamental right **to seek and receive** information on any matters of **public importance, held by public agencies**
- This act falls under our fundamental right, **the freedom of speech and expression.**

# The constitution of Nepal

---

- **Privacy Relating to Document**

- **Every person shall have the right to privacy of the personal document related to him or her.** No person is allowed to publish, or distribute personal documents of anyone unless consent of the concerned person is given.

- **Privacy relating to data**

- To have privacy of data, personal data or details of any person must be kept confidential. Data collected may only be used for the purpose for which such data have been collected, unless it is for national security or peace and order.

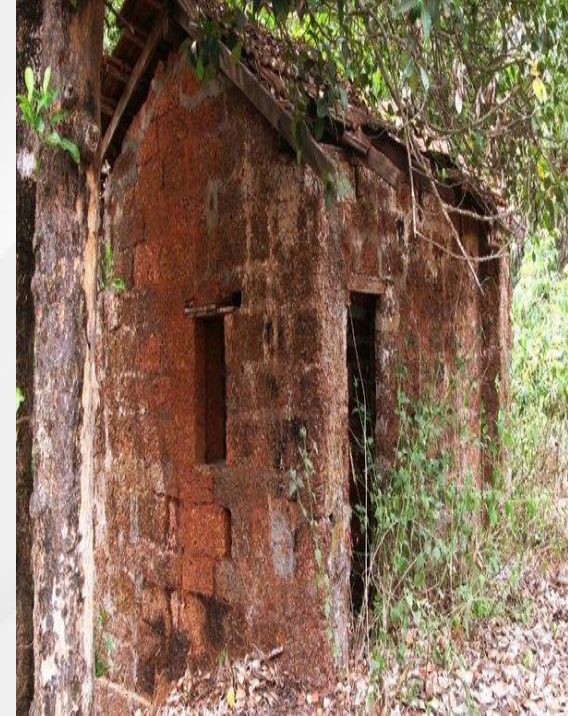
# The constitution of Nepal

- **Collection and Protection of Personal Information.**
  - No one except the official authorized under law or the person permitted by such official shall collect, store, protect, analyze, process or publish the personal information of any person. Information provided must be collected after obtaining consent for the purpose of conducting any study, research or collection of public opinion.
  - The public body must make appropriate arrangements against unauthorized access likely to occur against the possible risk of unauthorized use, change, disclosure, publication or transmission of such information.
- **Application may be made to correct information:**
  - If any person thinks that any information related to him or her which has remained under the responsibility, protection or control of any public body is wrong or is not based on the fact, he or she may, at any time, make an application to correct such information.

# William Pitt - Prime Minister of Great Britain

## 1766 – 1768 – 18<sup>th</sup> Century

- “The poorest man may in his cottage bid defiance to all forces of the Crown. It may be frail, its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King on England cannot enter.....”
- This means that even the poorest man has the right to privacy. He has the right to decide who can enter his home and who cannot. With the exception of natural calamities, like rain, wind and storm, even the king himself cannot enter the cottage without its owner's permission.





# The Fourth Amendment – 18<sup>th</sup> Century

---

- The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

— 4<sup>th</sup> Amendment, U.S. Constitution
- This amendment is triggered when there is **search or seizure by the police or government authority**.
- Which means, the authority does not have the right to intrude on a person's houses, papers, or belongings, whenever or wherever they want when the person is expected to maintain privacy, like their homes, restaurants, offices, and more.

# The Fourth Amendment

---

- Two key problems arise from new technologies:
  - Much of our **personal information is no longer** safe in our homes; it resides in huge **databases outside our control**.
  - New technologies allow the government to search our homes **without entering them** and search our persons from a distance without our knowledge.

# Olmstead v. United States (1928)

---

- In 1928, there was a Washington state resident called **Roy Olmstead** who was a suspected **bootlegger**, a person who makes, distributes, or sells goods illegally. At the time in the US, attempt to **smuggle and sell alcohol** was considered a **violation**.
- After years of suspecting Olmstead, the government gathered evidence by wiretapping his office phones without warrant.
- Supreme Court allowed the use of wiretaps on telephone lines without a court order.
- Court ruled against Olmstead interpreting the Fourth Amendment to apply only to physical intrusion and only to the search or seizure of material things, not conversations.

# Katz v United States (1967)

---

- In 1967, Charles Katz was convicted for transmitting **gambling information over the phone to clients in other states**, from Los Angeles to Boston and Miami. Federal agents attached an eavesdropping device to the outside of a public phone booth, for gathering information.
- Supreme Court reversed its position and ruled that the Fourth Amendment does apply to conversations.
- Court said that the Fourth Amendment **protects people, not places**. To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order.

# Kyllo v United States (2001)

- Danny Kyllo was suspected of growing marijuana in his triplex. So, the Department of the Interior agent made use of a thermal-imaging device to scan his property.
- The imaging was used to determine the amount of heat emitting from the home that was consistent with the high-intensity lamps typically used for indoor marijuana growth.
- The imaging found relatively hot areas existed within the premises, compared to the rest of the home.





# Kyllo v United States (2001)

---

- Based on the informants, the utility bills, and the thermal imaging result, a warrant was issued to search Kyllo's home, which indicted Kyllo with a federal drug charge.
  - Supreme Court ruled that police could not use thermal-imaging devices to search a home from the outside without a search warrant.
  - Court stated that where “government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, **the surveillance is a ‘search.’**”



# Video Surveillance and Face Recognition

---

- Security Cameras
  - Increased Security
  - Decreased Privacy
- Example: Police in Tampa, Florida, scanned the faces of all 100,000 fans and employees who entered the 2001 Super Bowl (causing some reporters to dub it Snooper Bowl) to search for criminals. People were not told that their faces were scanned.

# Marketing and Personalization

---

- Also known as one-to-one marketing is a marketing strategy by which companies leverage data analysis and digital technology to deliver individualized messages and product offerings to current or prospective customers
- Data Mining, Targeted ads
- Privacy maintained by
- Informed Consent
- “Do Not Track” button in browsers
- Paying for consumer information: Some businesses offer discounts to shoppers who use cards that enable tracking of their purchase.

# Location Tracking

- Global Positioning Systems (GPS) – computer or communication services that know exactly where a person is at a particular time
- Cell phones and other devices are used for location tracking
- GPS tracking via cell phones or Radio frequency identification tags (RFID)
- RFID tags are small devices – contain an electronic chip and an antenna – can transmit data to a base station and receive data from a base station. Can be hidden in children's clothes / bags
- Both can tell exactly where the person carrying the device is located at any given time, if the device is switched on.

# A Right to Be Forgotten

---

- Legislators and privacy advocates in Europe and the US are promoting a legal right to demand that websites remove information about oneself or their material removed. This right is known as the right to be forgotten
- The right to have material removed.
  - Negative Right (a liberty)
  - Positive Right (a claim right)
- They fall under negative as well as positive rights. This is because the right to be forgotten is the concept where individuals request for their personal information to be removed from the Internet.
- However, this consequently hampers our right to information.

# Government Systems

---

## Public Records: Access vs. Privacy:

- Public Records – records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)
- Identity theft can arise when public records are accessed
- How should we control access to sensitive public records?
- Opponents of national ID systems argue that they are profound threats to freedom and privacy. “Your papers, please” is a demand associated with police states and dictatorships.

# National ID Systems

---

- Social Security Numbers (US), National Insurance Numbers (UK): Too widely used, Easy to falsify
- Various new proposals would require citizenship, employment, health, tax, financial, or other data, as well as biometric information. In many proposals, the cards would also access a variety of databases for additional information.
- A new national ID system - Pros
  - would require the card
  - harder to forge
  - must carry only one card



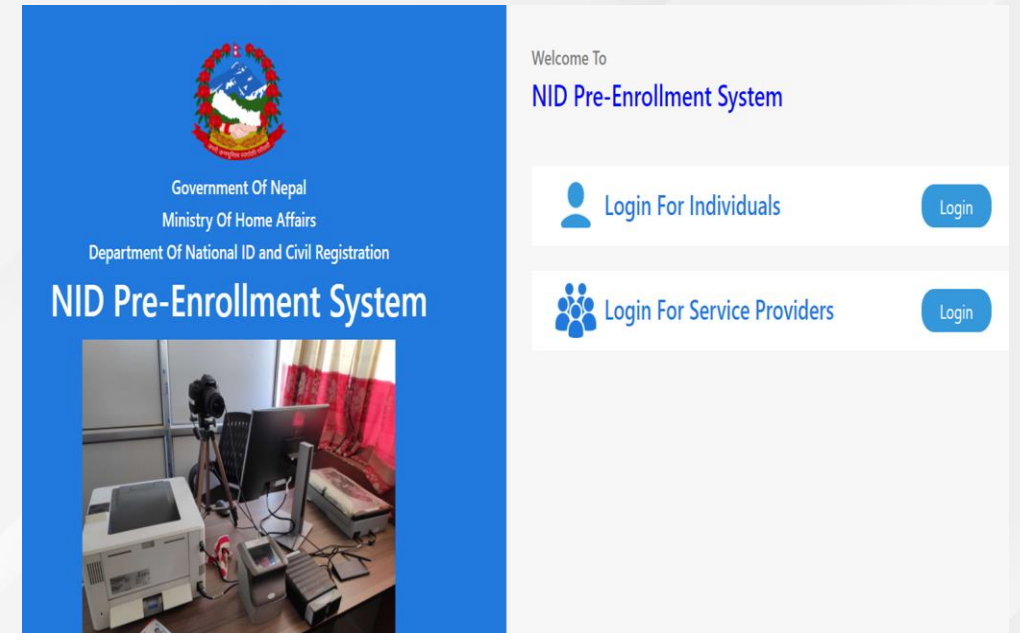
# National ID in Nepal

- Two main types of identity cards issued by the government they are **Foundation ID** and **Functional ID**.
- **Foundation ID**: Establishes the identity of the individual, is identified within the state for a number of service facilities and purposes. Example **Citizenship ID**.
- **Functional ID**: Are given only for a specific purpose. Example, Driving license, PAN card, voter ID card.



# National ID Systems

- New National Identity Card is based on information technology and will contain information like the demographic details of the person in citizenship, biographical details of the person including face (photo), fingerprints of ten fingers, iris of two eyes as well as e-signature in the form of electronic signature will be kept.
- Any body can verify the identity of a person both online and offline and is designed to gradually eliminate the hassle of using other functional IDs for different purpose.



# Rights and Law

---

- Rights – is the constitutional sense – are not created by laws. They exist independently, and the laws are there to protect them, not to establish them.
- Transactions
- Ownership of personal data
- A basic legal framework: Enforcement of agreements and contracts Regulation

# Any questions?

---



designed by  freepik

