



Chapter 7

Privacy and Surveillance

Table of Contents

Privacy and Surveillance

Definition

Communication Technology and

Eavesdropping

Data Protection

Introduction to Privacy

Privacy refers to the ability of individuals or groups to control or keep confidential information about themselves, their personal lives, and their activities.

It is a fundamental human right that allows individuals to maintain autonomy, dignity, and security.



SURFACE WEB, DARK WEB, DEEP WEB

SURFACE WEB

Facebook
Google
Instagram
YouTube

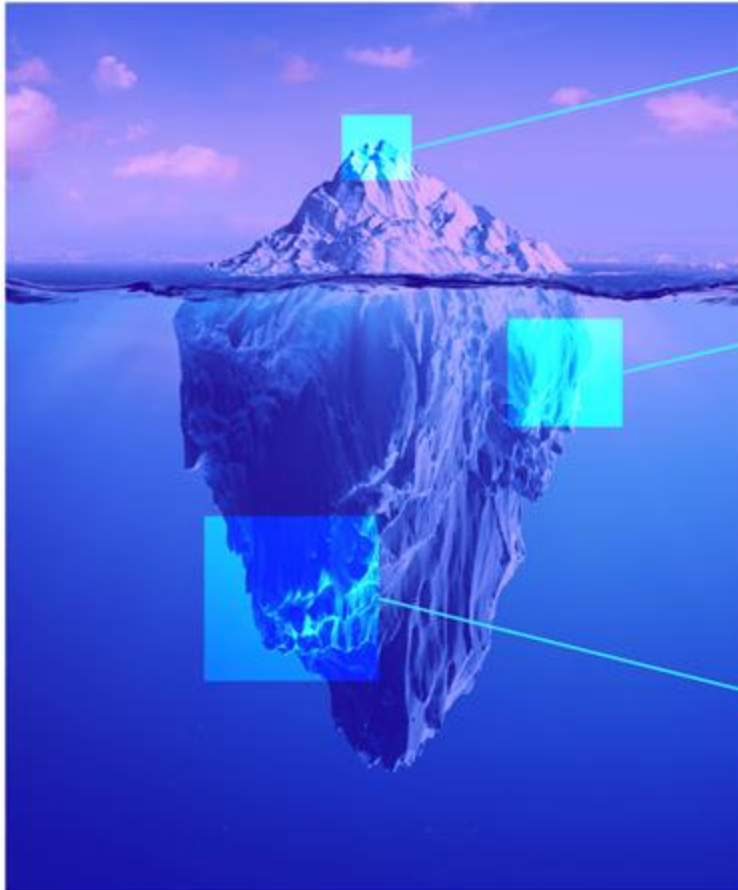
DEEP WEB

Medical Records
Legal Documents
Private Forums
Research Papers
Non Indexed Content

DARK WEB

Private Communication Forums
TOR Illegal Trade
Illegal Activities

The structure of internet content



World wide web (surface web)

Public websites available through search engines (e.g. Wikipedia)

Deep web (un-indexed web)

Protected websites, databases and intranets not accessible through search engines (email accounts, government resources, medical data, academic information, etc.)

Dark web (darknets)

Encrypted networks that offer full anonymity and require special software, configurations and permissions to access. Host of the underground economy teeming with illegal activities.

Types of Privacy

Personal Privacy: This refers to the protection of an individual's personal information, such as their name, address, contact details, financial data, health records, and other sensitive data.

Update Personal Information

Title: Mr.

Name (First, Middle/Initial, Last):

Hide Middle Name: ☐

E-mail Address:

Preferred Name:

Address:

City, State, Zip:

Country:

County:

Phone: (555) 555-5555 Ext:





































Birth Date: mm/dd/yyyy

Marital Status:

Gender:

Ethnicity:

Updates submitted are not immediate. They will be reviewed and you should be able to view them within a few days.

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	08/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 1	22.5\$	<input data-bbox="566 696 604 725" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	05/16	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 1	22.5\$	<input data-bbox="566 746 604 775" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	03/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 1	22.5\$	<input data-bbox="566 796 604 825" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	05/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 1	22.5\$	<input data-bbox="566 846 604 875" type="button" value="+"/>
<input type="checkbox"/>	480480	 VISA	CREDIT	CLASSIC	07/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 1	22.5\$	<input data-bbox="566 896 604 925" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	05/15	Yes	101	 United States, IN, Evansville, 47715		American Sanctions 1	22.5\$	<input data-bbox="566 946 604 975" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	03/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 2	22.5\$	<input data-bbox="566 996 604 1025" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	06/16	Yes	101	 United States, IN, Evansville, 47715		American Sanctions 2	22.5\$	<input data-bbox="566 1046 604 1075" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	05/15	Yes	101	 United States, IN, Evansville, 47715		American Sanctions 2	22.5\$	<input data-bbox="566 1096 604 1125" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	11/15	Yes	101	 United States, IN, Evansville, 47715		American Sanctions 2	22.5\$	<input data-bbox="566 1146 604 1175" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	03/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 2	22.5\$	<input data-bbox="566 1196 604 1225" type="button" value="+"/>
<input type="checkbox"/>	486185	 VISA	DEBIT	CLASSIC	08/15	Yes	101	 United States, IN, Evansville, 47712		American Sanctions 2	22.5\$	<input data-bbox="566 1246 604 1275" type="button" value="+"/>

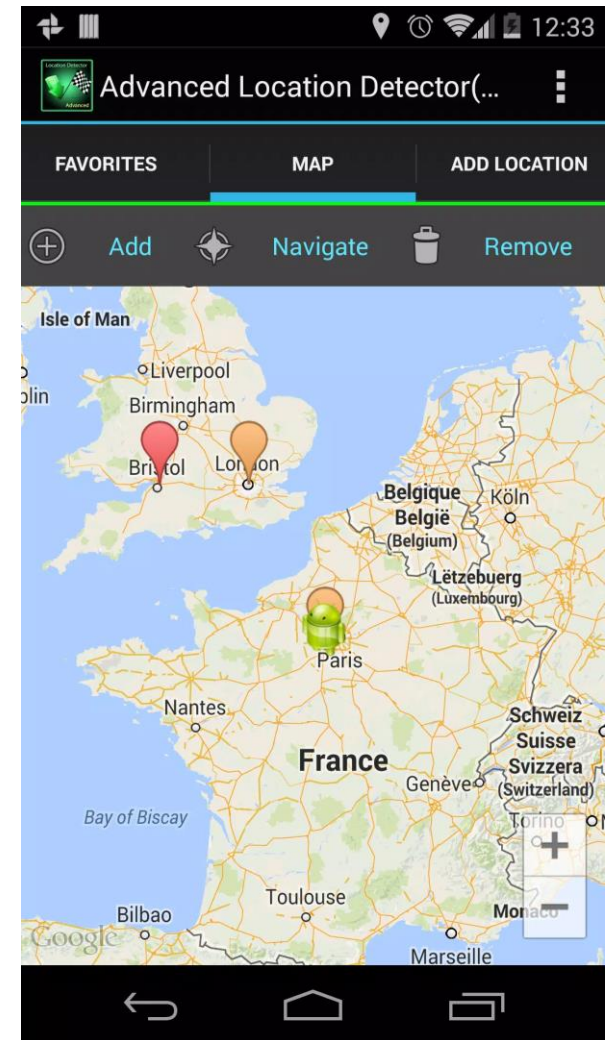
Types of Privacy



Communication Privacy: This involves safeguarding the confidentiality of one's communications, whether it be through traditional mail, phone calls, email, or online messaging services.

Types of Privacy

Location Privacy: This relates to an individual's right to keep their physical whereabouts and movements private. It includes concerns about surveillance technologies, location tracking, and the collection of geolocation data.



Types of Privacy

Data Privacy: This pertains to the protection of personal data collected by organizations, such as websites, apps, or government agencies. It involves ensuring that data is collected and used transparently, with the individual's consent, and that appropriate security measures are in place to prevent unauthorized access or misuse.

Base64*

Decode Base64 to Image

Preview Image | Toggle Background Color



File Info

- Resolution: 150x200
- MIME type: Image/jpeg
- Extension: jpg
- Size: 5.1 KB
- Download: [image.jpg](#)
- Channels: 3
- Bit depth: 8

Malaysia Stung by Massive Data Breach Affecting Millions

Mobile Phone Records Appear on Dark Web, Both for Sale and for Free

Jeremy Kirk (@Jeremy_kirk) · November 2, 2017

Name	Date modified	Type	Size
ALTEL.zip	27/10/2017 18:02	Compressed (zipp...	7,850 KB
CELCOM.zip	28/10/2017 11:14	Compressed (zipp...	698,332 KB
DIGI.zip	28/10/2017 09:19	Compressed (zipp...	727,845 KB
ENABLINGASIA.zip	27/10/2017 17:54	Compressed (zipp...	3,733 KB
FRIENDIMOBILE.zip	28/10/2017 09:19	Compressed (zipp...	80,036 KB
jobstreet.zip	29/10/2017 13:25	Compressed (zipp...	2,042,094 ...
MAXIS.zip	28/10/2017 12:09	Compressed (zipp...	1,332,640 ...
MerchantTradeAsia.zip	28/10/2017 08:49	Compressed (zipp...	36,462 KB
Part 1.zip	27/10/2017 17:49	Compressed (zipp...	3,928 KB
Part 3.zip	27/10/2017 18:02	Compressed (zipp...	8,746 KB
PLDT.zip	28/10/2017 07:38	Compressed (zipp...	6,944 KB
REDTONE.zip	28/10/2017 07:38	Compressed (zipp...	12,557 KB
TUNETALK.zip	28/10/2017 10:01	Compressed (zipp...	16,439 KB
UMOBILE.zip	28/10/2017 10:30	Compressed (zipp...	233,909 KB
XOX.zip	28/10/2017 07:38	Compressed (zipp...	4,228 KB

Data breach expert Troy Hunt's screenshot of a file directory containing leaked data, found freely available on a Tor hidden service.

id	permanent_address	pic	race	religion	status
1	49 L C 1	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
2	NO 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
3	LOT 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
4	52C	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
5	NO 7	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
6	9 JALU	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
7	NO 2	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
8	NO 9	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
9	1507	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
10	LOT 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
11	NO 1	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
12	243 /	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
13	66 JF	src="data:image/png;base64, /j/AA	CINA	BUDDHA	Aktif
14	NO 6	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
15	NO 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
16	NO 8	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
17	NO 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
18	204 A-1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
19	56 1749	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
20	LOT 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
21	NO 2	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
22	NO 7	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
23	NO 5	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
24	KAMP	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
25	NO 3	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
26	NO 1	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
27	NO 2	src="data:image/png;base64, /j/AA	MELAYU	ISLAM	Aktif
28	NO 3	src="data:image/png;base64, /j/AA	INDIA M.	ISLAM	Aktif

Types of Privacy

Privacy in Public Spaces: This involves the expectation of privacy even when individuals are in public areas. It includes limitations on surveillance activities, facial recognition technologies, and the ability to be free from intrusive monitoring.



Types of Privacy

Privacy of Personal Relationships: This relates to the right to keep intimate or personal relationships private, free from unwanted intrusion or surveillance.



Harms and Benefits of Privacy

Benefits of Privacy

- ✓ Individual autonomy
- ✓ Personal security
- ✓ Emotional well-being
- ✓ Freedom of expression
- ✓ Stronger personal and professional relationships
- ✓ Encouragement of innovation and creativity
- ✓ Facilitation of social and political participation
- ✓ Trust in institutions and systems

Harms and Benefits of Privacy

Harms of Privacy

- ✓ Invasion of personal space
- ✓ Unauthorized access to personal information
- ✓ Identity theft and fraud
- ✓ Stalking and harassment
- ✓ Discrimination and bias based on personal data
- ✓ Loss of control over personal information
- ✓ Surveillance and monitoring
- ✓ Data breaches and leaks
- ✓ Targeted advertising and manipulation
- ✓ Reputation damage or online shaming

Introduction to Surveillance



Surveillance refers to the systematic monitoring, observation, or collection of information about individuals, groups, or activities.

It involves the use of various techniques, technologies, or methods to gather data, track behavior, or monitor specific targets.

Surveillance can be conducted by governments, organizations, or individuals for different purposes, such as security, law enforcement, intelligence gathering, or commercial interests.

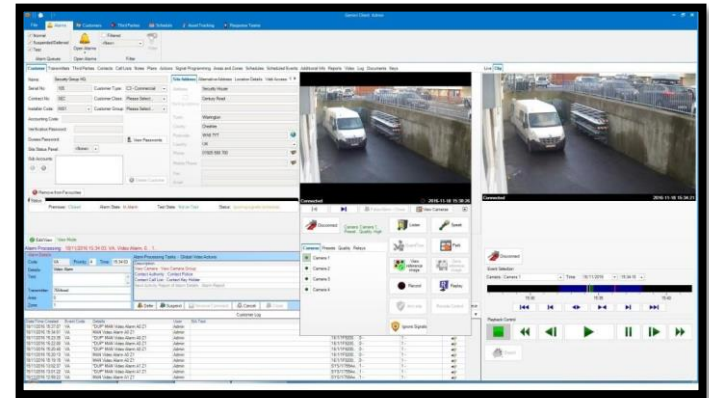
Types of surveillance can include:

Physical Surveillance: This involves the direct observation of individuals or activities by human agents, typically through visual or auditory means. It can include monitoring public spaces, using closed-circuit television (CCTV) cameras, or employing undercover agents.



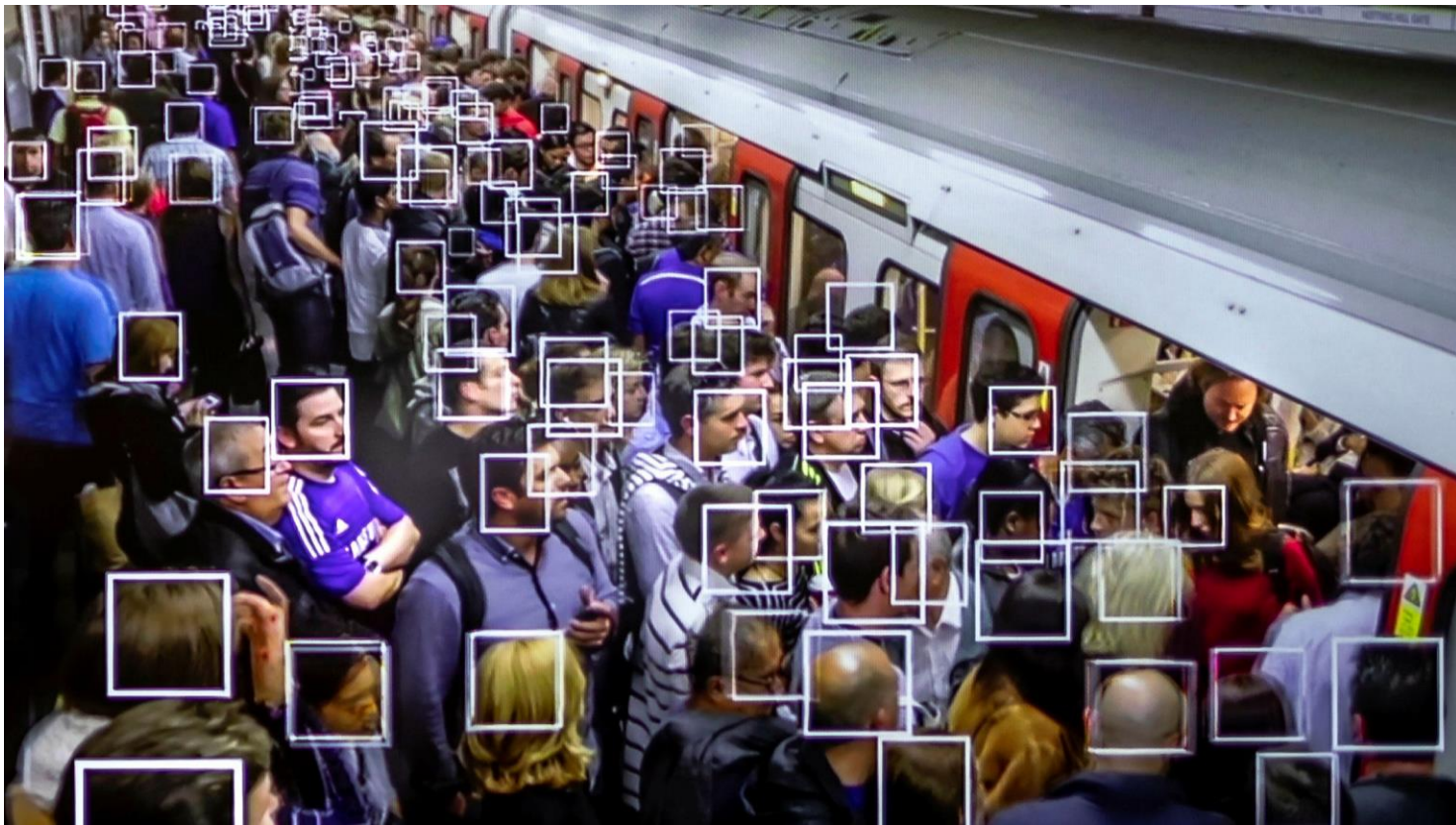
Types of surveillance can include:

Digital Surveillance: Digital surveillance involves the monitoring of online activities and communication. It includes tracking internet usage, collecting metadata, intercepting emails or instant messages, monitoring social media posts, or using surveillance software or technologies.



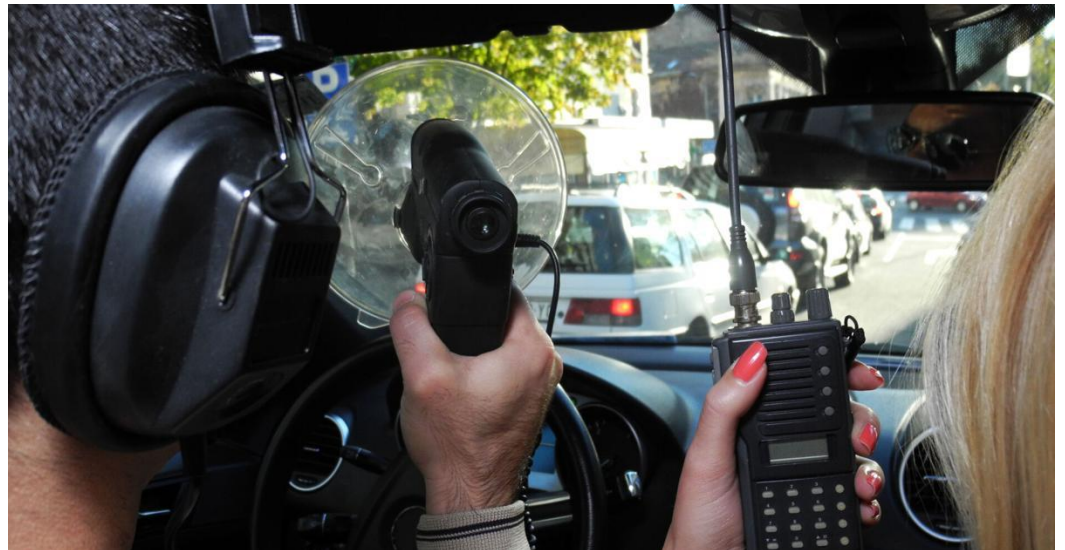
Types of surveillance can include:

Mass Surveillance: Mass surveillance refers to the widespread, indiscriminate monitoring of a large population or a broad range of activities. It often involves the collection of vast amounts of data, which can be analyzed, stored, and accessed for various purposes.



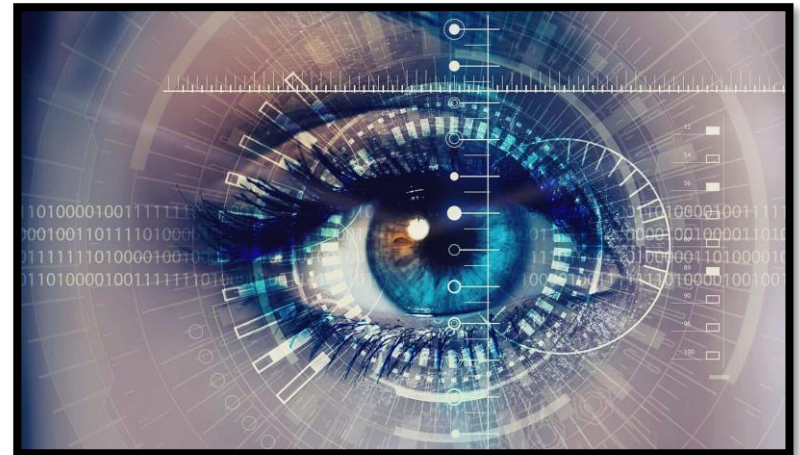
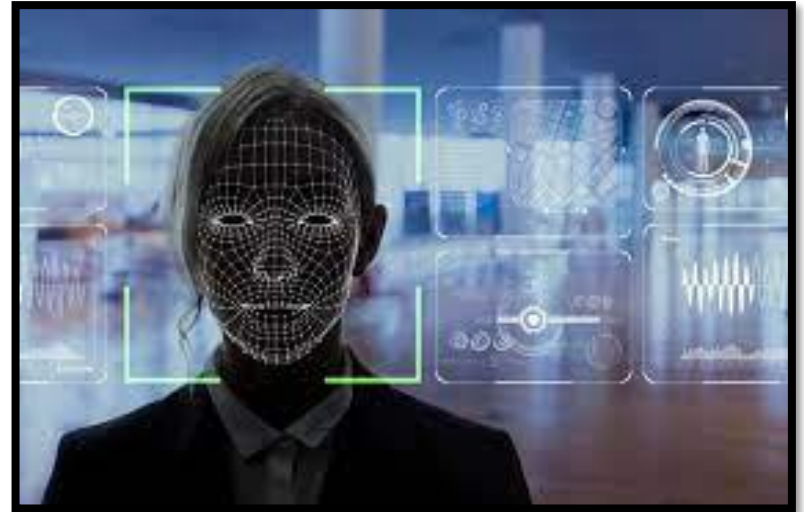
Types of surveillance can include:

Electronic Surveillance: This includes the interception or monitoring of electronic communications, such as phone calls, text messages, emails, or other forms of electronic data transmission. It may involve the use of wiretapping, data interception, or surveillance tools.



Types of surveillance can include:

Biometric Surveillance: Biometric surveillance relies on the use of biometric data, such as fingerprints, facial recognition, iris scans, or DNA, to identify and track individuals. It is often used in security systems, border control, or law enforcement.



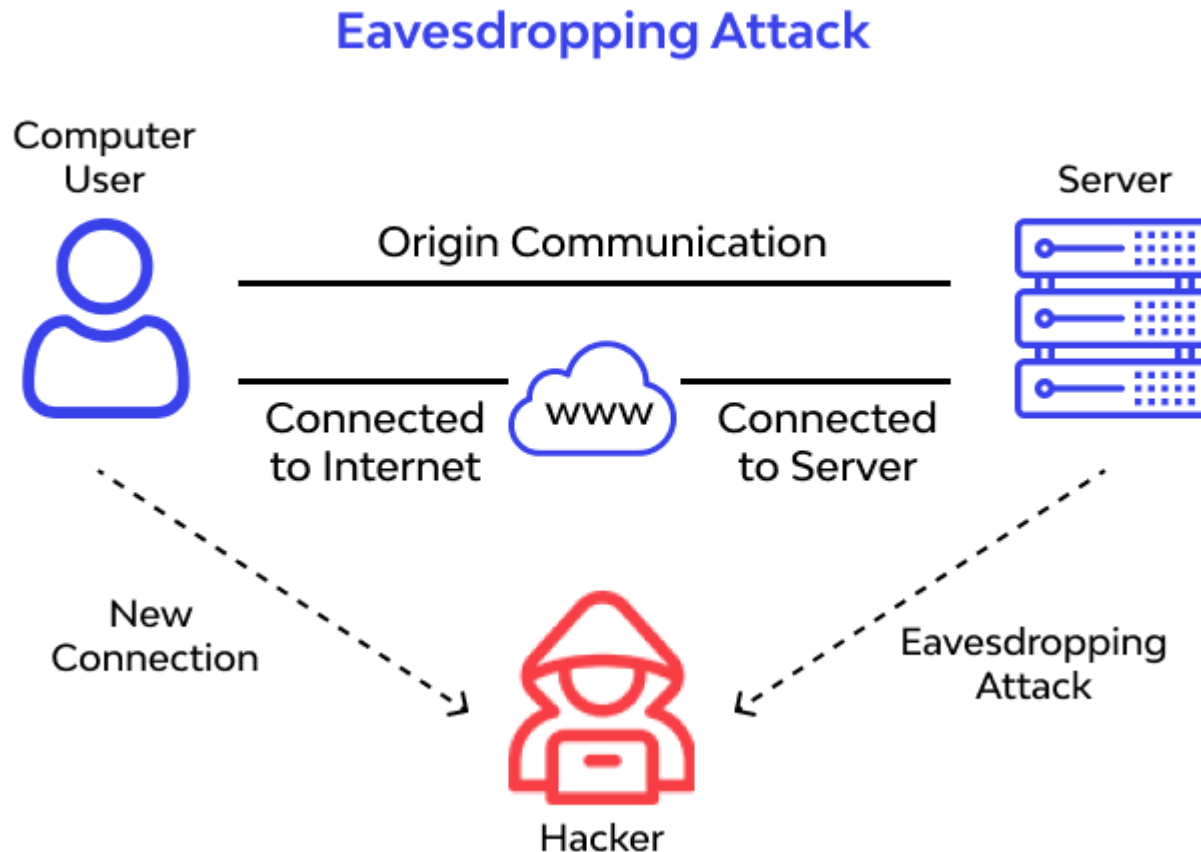
Communication Technology and Eavesdropping

Communication technology has provided both opportunities and challenges when it comes to eavesdropping.

While these technologies have greatly enhanced communication and connectivity, they have also created potential vulnerabilities that can be exploited for eavesdropping purposes.



Eavesdropping Attack



Identity of Eavesdropper

- Two types of eavesdropper: governmental and non-governmental
- Governmental eavesdropping:
 - Regulated and legal
- Non-governmental:
 - Restricted or completely banned in most countries
 - Exception: employers monitoring the employee's use of Internet communication methods.
 - Example: in the United Kingdom, employers can monitor their employees' e-mail provided they tell their employees quite clearly that such monitoring is happening (they may not, however, monitor telephone use).

Eavesdropping ways: Wiretapping

Wiretapping involves intercepting and monitoring telephone or internet communication.

In the past, physical access to telephone wires was required, but with the digitalization of communication, it can now involve the interception of digital signals or data packets transmitted over networks.

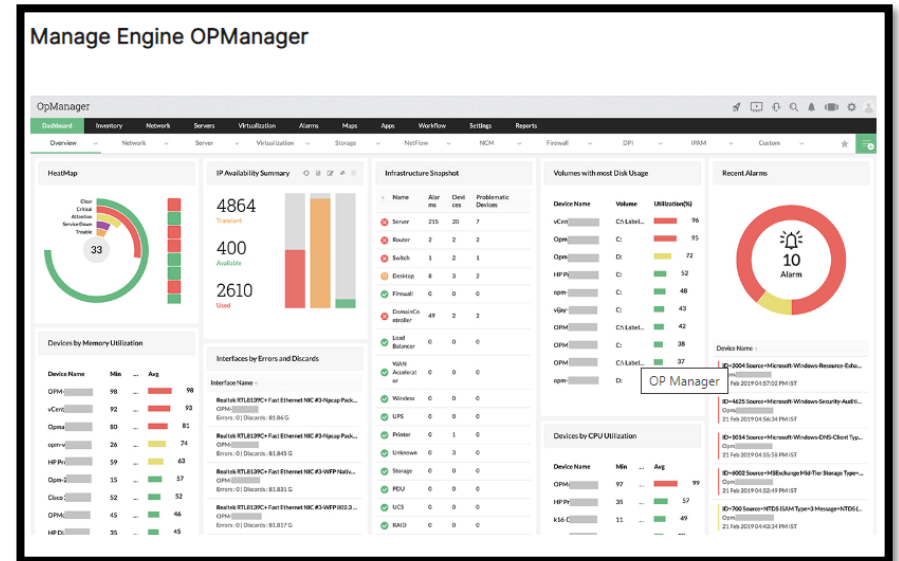


Eavesdropping ways: Network Monitoring

Internet Service Providers (ISPs), government agencies, or malicious actors can monitor network traffic to intercept and analyze communication data. This can include email content, instant messages, voice calls, or browsing activities.

What are the best network monitoring tools for 2023? Here you have a list of 5 useful cloud solution for network management:

Manage Engine OPManger
PRTG (Paid Network Monitoring Solutions)
Tanaza
EventSentry
SpiceWorks



Eavesdropping ways: Wi-Fi Eavesdropping



In public or unsecured Wi-Fi networks, eavesdroppers can intercept and capture data packets transmitted between devices on the network. This can expose sensitive information such as login credentials, personal messages, or financial transactions.

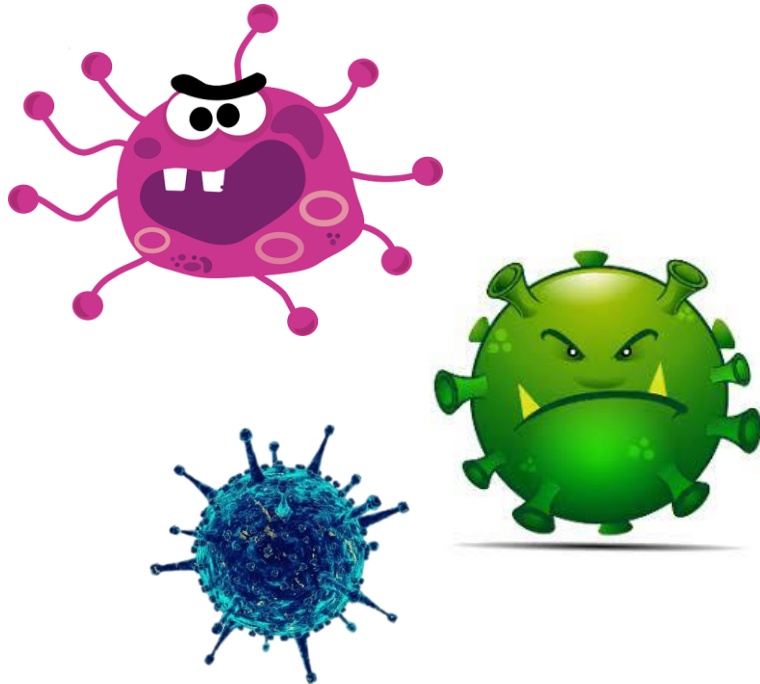
7 MOST COMMON WI-FI THREATS



- 1 **Configuration Problems:** Misconfigurations, incomplete configurations.
- 2 **Denial of Service:** Sending large amounts of traffic (or viruses) over the network with the intent of hijacking resources or introducing backdoors.
- 3 **Passive Capturing:** Eavesdropping within range of an access point to capture sensitive information.
- 4 **Rogue (or Unauthorized/Ad-Hoc) Access Points:** Fool devices into connecting with a false access point.
- 5 **Evil Twin Attacks:** Impersonating legit access points with a stronger signal to entice authorized users to sign on.
- 6 **Hacking of Lost or Stolen Wireless Devices:** Bypassing the password to gain access.
- 7 **Freeloading:** Piggybacking on a connection or intercepting file sharing.

Eavesdropping ways: Malware and Spyware

Malicious software or spyware can be used to secretly monitor communication on infected devices. This can include keylogging, screen capturing, or accessing microphone and camera functionalities without the user's knowledge.



DIFFERENT TYPES OF MALWARE PROGRAMS:



VIRUSES

These bugs normally are attached to an email.



RANSOMWARE

Encrypts your files, and then demands a ransom to return the data to the user.



SCAREWARE

The user would be taken to a page to purchase a fake program.



SPYWARE

It can monitor all forms of communication and interaction on a device



TROJANS

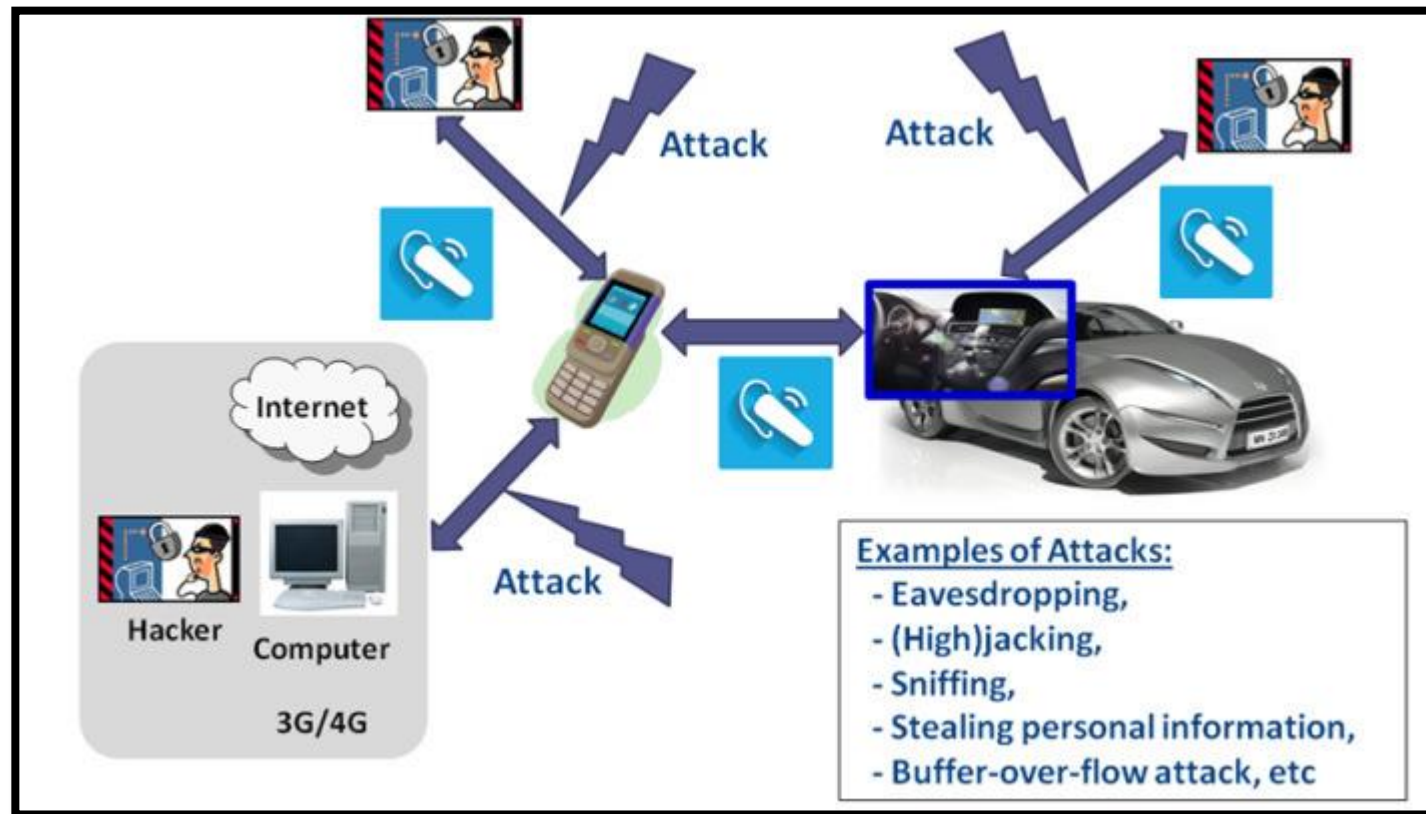
This application is actually stealing personal data, spying, or even crashing your computer.



ADWARE

Will pepper the user with unwanted ads to attempt to get them to part with their money.

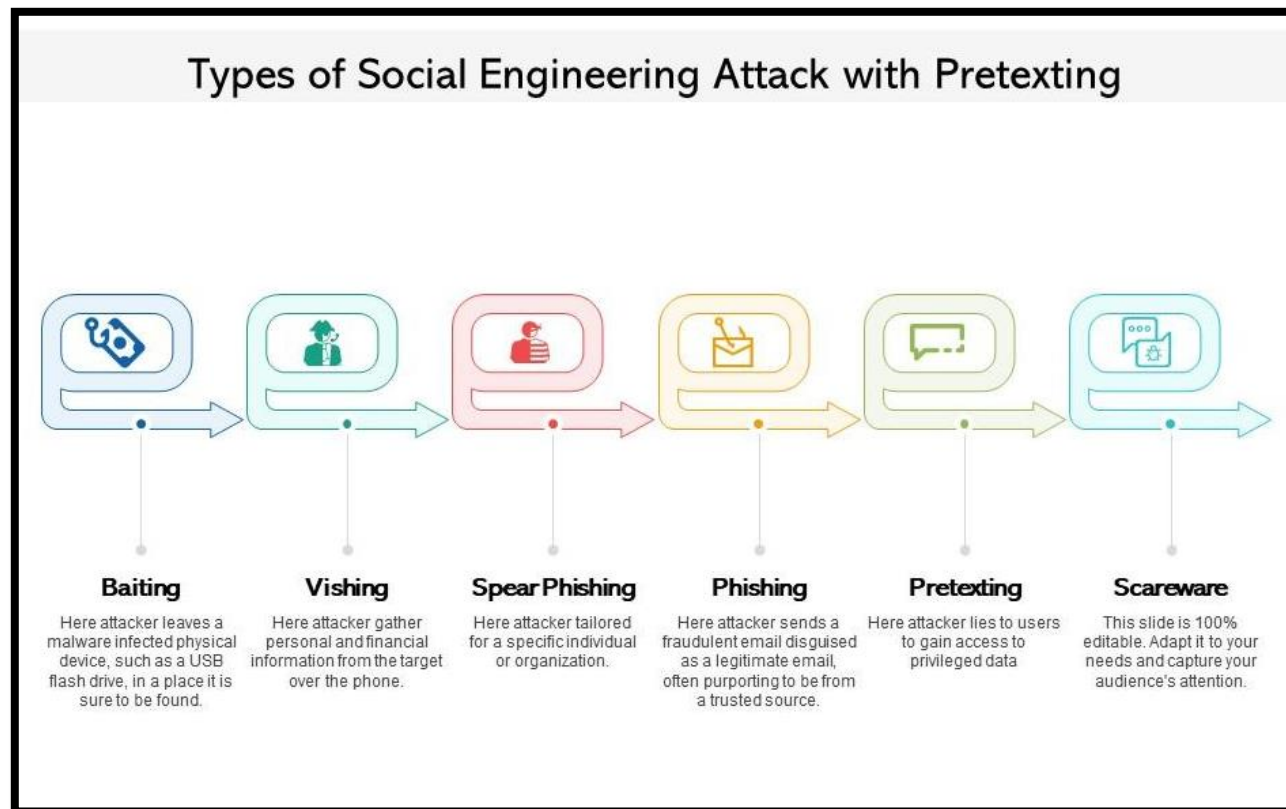
Eavesdropping ways: Bluetooth Eavesdropping



Bluetooth-enabled devices can be vulnerable to eavesdropping attacks if they have weak security settings or are not properly protected. Eavesdroppers can intercept and capture Bluetooth signals to listen in on conversations or access data being transmitted between devices.

Eavesdropping ways: Social Engineering

Eavesdroppers can employ social engineering techniques to manipulate individuals into revealing sensitive information or granting unauthorized access to their communication devices or accounts. This can involve impersonation, phishing, or pretexting.

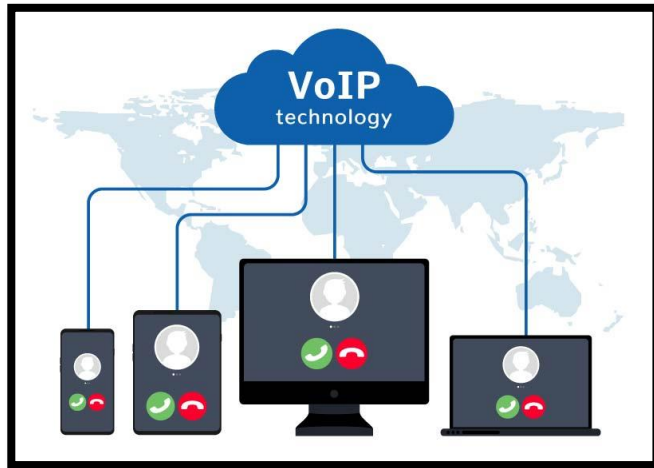


Eavesdropping ways: Voice over IP (VoIP)

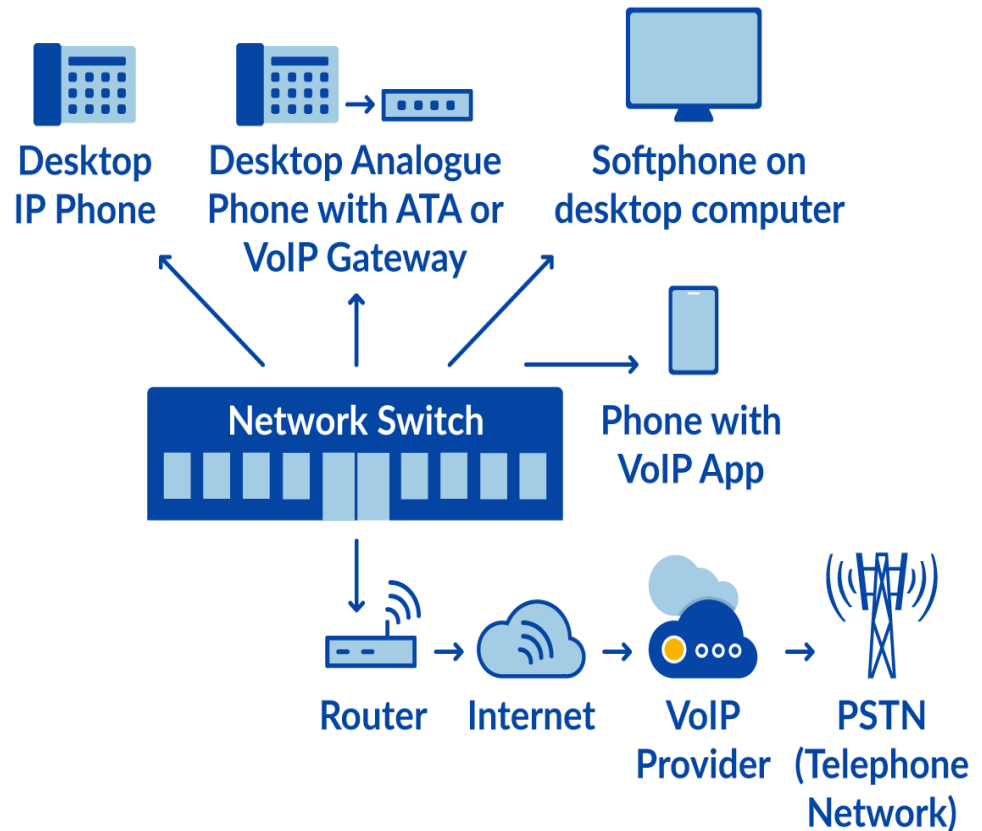
Voice over IP (VoIP)

Eavesdropping: VoIP technology, which allows voice communication over the internet, can be subject to eavesdropping if not properly secured.

Eavesdroppers can intercept and listen in on VoIP calls, potentially accessing private conversations or sensitive information.



Hosted VoIP Network Infrastructure



Data Protection

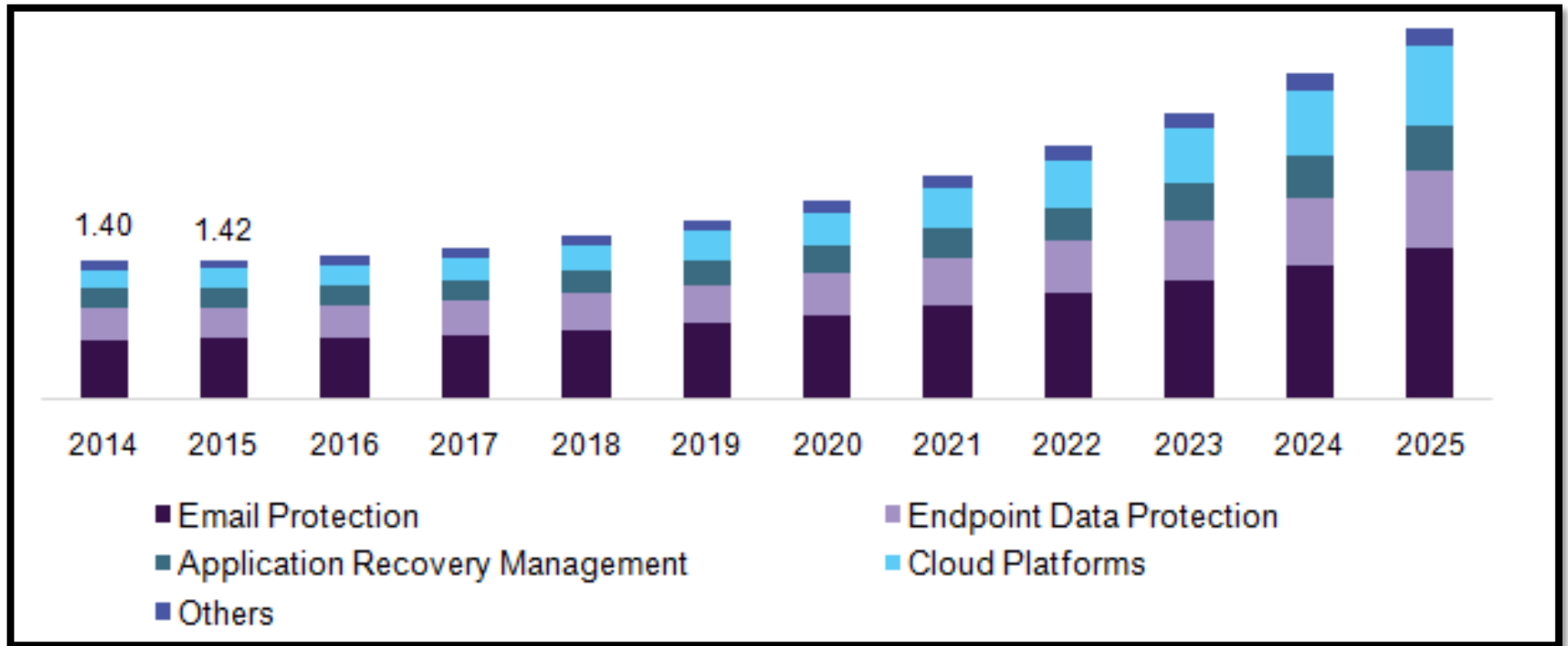


Data protection refers to the set of practices, policies, and measures implemented to safeguard personal and sensitive information from unauthorized access, use, disclosure, alteration, or destruction.

It involves ensuring that data is collected, processed, stored, and shared in a manner that respects the privacy and rights of individuals.

Data protection measures include implementing security protocols, encryption, access controls, and regular backups to prevent data breaches, unauthorized disclosure, or loss.

Technology and Markets



Data Protection and Privacy



What is GDPR?

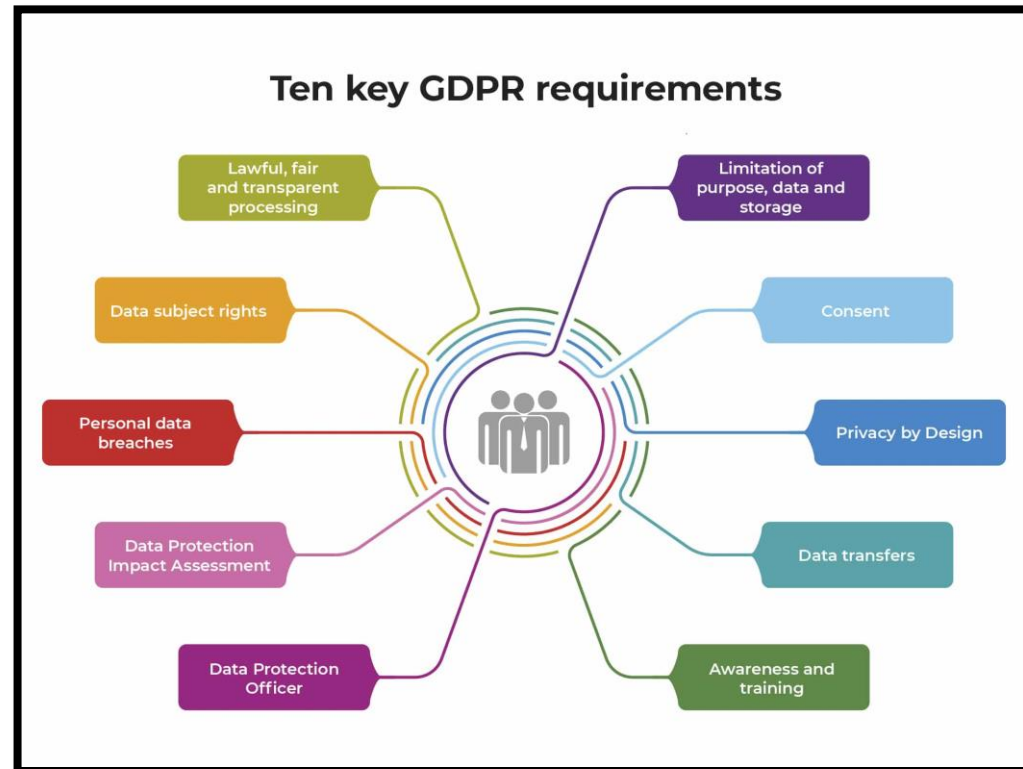
The General Data Protection Regulation (GDPR) is a comprehensive data protection law enacted in the European Union (EU) to safeguard the privacy and rights of individuals regarding the processing of their personal data.

It establishes a set of rules and principles that organizations must adhere to when handling personal data, regardless of their location.

The GDPR grants individuals greater control over their data, empowering them with rights such as access, rectification, erasure, and the ability to object to processing.

Non-compliance with the GDPR can result in substantial fines and penalties.

The GDPR's impact extends beyond the EU, as many organizations worldwide have adopted its principles as a benchmark for ensuring robust data protection practices.



Malaysian Law:

Personal Data Protection Act 2010

7 Principles of Personal Data Protection under the PDPA

1. General Principle

Person whose data is to be processed must consent.

2. Notice and Choice Principle

Person must be notified his personal data will be processed and how. He must also be given the choice to limit the right to process.

3. Disclosure Principle

Personal data cannot be used except for purpose stated, and cannot be disclosed except to disclosed third parties.

4. Security Principle

Companies must have sufficient steps and procedures to protect personal data from loss, misuse, modification, unauthorised access or disclosure, alteration or destruction.

Principles of Personal Data Protection (2)

5. Retention Principle

Personal data cannot be kept longer than necessary, and must be destroyed or permanently deleted if no longer required.

6. Data Integrity Principle



Companies must take reasonable steps to ensure personal data is accurate, complete, not misleading and kept updated.

And finally,

7. Access Principle

Any person must be permitted access to his own personal data and be entitled to correct any inaccurate, incomplete or misleading information of himself.

Comparison between GDPR vs PDPA

 GDPR PRINCIPLES Lawfulness, fairness and transparency Purpose Limitation Data minimisation Accuracy Storage limitation Integrity and confidentiality (security) Accountability	 MALAYSIA PRINCIPLES General Principle Notice & Choice Principle Data Integrity Principle Security Principle Retention Principle Disclosure Principle Access Principle
---	--

Other example of Data Protection Laws

Korea

Data Protection Act 2011

- Data Protection Principles
- Rights of Data Subjects
- Organization to designate someone to take charge
- Special entity to enforce the Act (Data Protection Commission/DPC)
- Mandatory reporting of significant breach to DPC
- Data breach notification (to the Data Subject)
- Mediation to resolve dispute.
- Differentiate personal data & sensitive data
- PIAs are encouraged

Malaysia

Personal Data Protection Act 2010

- Data Protection Principles
- Rights of Data Subjects
- Special entity to enforce the Act (Data Protection Commissioner)
- No mandatory data breach notification.
- Differentiate personal data & sensitive data.
- Does not apply to Federal and States Governments

Taiwan

Personal Data Protection Act 2010

- Data Protection Principles
- Rights of Data Subjects
- Mandatory data Breach Notification (to the Data Subject)
- Enforcement by Ministries responsible for each industry sector

Other laws in Malaysia that have provisions related to data protection or privacy.

Communications and Multimedia Act 1998 (CMA): The CMA regulates the communications and multimedia industry in Malaysia. It includes provisions related to the protection of personal data, confidentiality of communications, and the obligations of licensees to protect customer information.

Computer Crimes Act 1997: This act addresses various computer-related offenses, including unauthorized access, unauthorized modification, and unauthorized interception of computer data. It includes provisions related to the protection of data stored or transmitted electronically.

Penal Code: The Malaysian Penal Code includes provisions that relate to privacy and data protection, such as those pertaining to unauthorized access to a computer or the publication of private information without consent.

Official Secrets Act 1972: The Official Secrets Act is aimed at protecting sensitive government information from unauthorized access, use, or disclosure. It establishes offenses related to the unauthorized communication, retention, or obtaining of official secrets.

Financial Services Act 2013 and Islamic Financial Services Act 2013: These acts regulate the financial services industry in Malaysia. They contain provisions related to the confidentiality and protection of customer financial information, as well as obligations for financial institutions to have data protection policies and procedures in place.

End