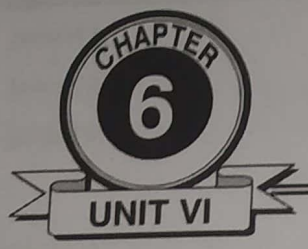



# Confidentiality and Cyber Forensic

**Syllabus :**

At the end of this unit, you should be able to understand and comprehend the following syllabus topics :

- Introduction to Personally Identifiable Information (PII)
- PII impact levels with examples
- PII Confidentiality Safeguards
- Cybercrime
- Information Protection Law - Indian Perspective
- Cyber Stalking

## 6.1 Privacy on Web

- Security and Privacy are related but not the same. Whereas security is concerned with protecting CIA of digital information, Privacy is geared towards protecting personal data of individuals (people).
- Generally Accepted Privacy Principles Framework or GAPP Framework defines Privacy as,

✍ ***Definition :*** *Privacy encompasses the rights and obligations of individuals and organisations with respect to the collection, use, retention, disclosure, and disposal of personal information.*

- Personal information such as Name, Gender, Age, Date of birth, Citizenship, IP Address, what you buy online, where you eat, which location you go, all these are various forms of private information that relates to you and requires privacy protection.
- Your personal data can be used to sell items to you or modify your behaviour. Also, your personal data is subject to exposure and there could be sensitive personal information e.g. diseases that you might have or your most called numbers.

## 6.2 Introduction to Personally Identifiable Information (PII)

**Q. Explain personally identifiable information PII.** **SPPU – May 19**

**(May 19, 4 Marks)**

- Before you understand more about privacy, you should have a clear understanding of what type of data does privacy principles and practices refer to. So, let me ask you a question – what is a private or personal information?
- As per the Article 4 of European Union General Data Protection Regulation (GDPR),

***Definition :*** *Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

- PII is the information (or combination of information) that is sufficient to trace you as an individual. It could be several elements such as
  1. Name
  2. IDs such as Aadhar, Passport, Email ID, PAN, Bank Account, Phone Number, etc.
  3. Address – Physical or Digital (IP Address)
  4. Demography details such as location, caste, gender, age, income group, etc.
- Here the personal information itself may not always be unique enough to identity someone. For example, Narendra itself could just be the name of any individual and may not be unique enough to identify someone without further details about him. But, if you say, "Prime minister of India in 2018", it could certainly be referring to Shri. Narendra Modi. The single attribute is strong enough to identify the person uniquely.
- So, when we talk about privacy, we are talking about protecting the information that could be used to uniquely identify someone and possibly track him or her. Just a scary fact, if someone just knows your name, your date of birth and your postal code, there is more than 75% chance to pinpoint you!

### 6.2.1 Privacy Principles

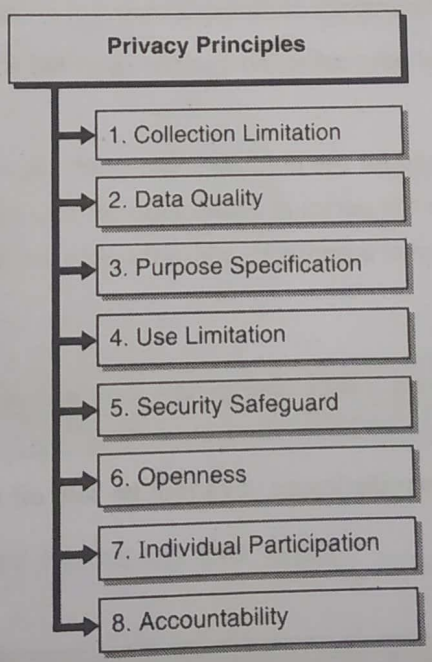



**Fig. 6.2.1**

- Now that you have a general understanding of what privacy is, let's dive deeper and understand the tenets of Privacy. The Organisation for Economic Co-operation and Development (OECD) has defined several Privacy Principles.
- Any organisation that collects personal or private data should consider following the recommended privacy principles. In some countries there are strict laws around privacy and very steep penalty if an organisation is found to be non-compliant with the privacy laws.

- You will learn about one such privacy law later but for now understand the broader and recommended privacy principles that any organisation collecting personal information should consider following and abiding by.

### 1. Collection Limitation

✍ ***Definition :*** *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

- Any unauthorised data collection and collecting information beyond actual use is prohibited. You cannot just go on collecting personal data indefinitely.
- Additionally, the user must provide her consent (approval) before you can collect the personal data. The user should be aware of what is being collected and how it would be used by the organisation.

### 2. Data Quality

✍ ***Definition :*** *Personal data should be relevant to the purposes for which they are to be used and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

The collected personal data should meet the data quality requirements. It should be accurate and kept up-to-date wherever possible.

### 3. Purpose Specification

✍ ***Definition :*** *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

- The specific purpose of personal data collection must be specified at the time of collection and not later on or in the future.
- Personal data should only be used for the purpose it was originally specified to be collected for. So, for example, if you claimed that you will use the personal data for cancer research, you cannot then use the data for selling goods and services. Every additional purpose for which the data would be used must be consented by the user.

### 4. Use Limitation

✍ ***Definition :*** *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.*

Personal data should be protected from disclosure. It cannot be sold off to third-party or be used for purposes other than those approved by the user.

### 5. Security Safeguards

✍ ***Definition :*** *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

- This is where Security and Privacy overlap. This privacy principle states that the CIA of privacy data should be protected.
- Security controls ensure that the private data is adequately protected and is not disclosed. The data could be encrypted, anonymised or protected via regular security mechanisms such as access control.

6. **Openness**

***Definition :*** *There should be a general policy of openness about developments, practices and policies with respect to personal data.*

Organizations should adequately disclose its policies regarding handling of privacy data. Policies around data protection, encryption, processing, deletion, etc. should be publicly available.

7. **Individual Participation**

***Definition :*** *An individual should have the right : (a) to obtain her data (b) to receive information regarding data (c) to challenge data relating to him.*

The user should have the complete authority over her data. She should be able to obtain a copy of it, ask questions about its use or get it erased from the system and restrict further use.

8. **Accountability**

***Definition :*** *A data controller should be accountable for complying with measures which give effect to the principles stated above.*

- The organisation collecting personal data should be totally responsible for following all the privacy principles.
- There could be penalties levied on the organisation for non-complying with the privacy laws or it could be loss of reputation and goodwill if the poor practices around are personal data collection and use are leaked or exposed.
- Fig. 6.2.2 summarizes how security and privacy are connected. The overlap is around protection of personal data. The various security measures that you would learn in this book can be used to effectively protect personal data.

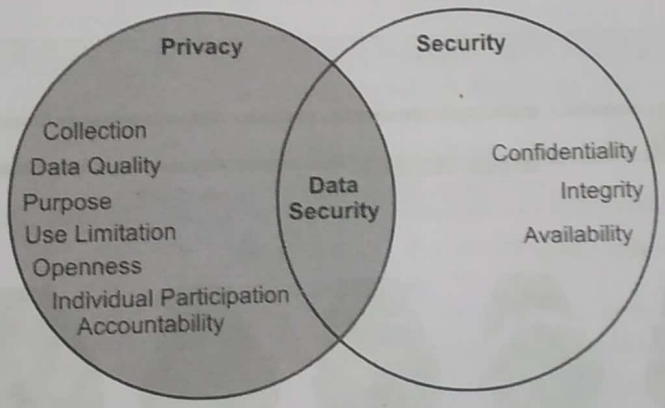



Fig. 6.2.2

## 6.3 Concept Building - Privacy Risks on the Web

- Lot of companies and organisations track and watch out what you do online. Most of the websites have trackers built in them which capture your browsing habits, navigation, products that you have looked at, videos that you have seen, what you have searched for, which websites you visit and various other online activities and behaviours.
- Let's understand some of the mechanisms and technologies using which your online privacy could be breached.

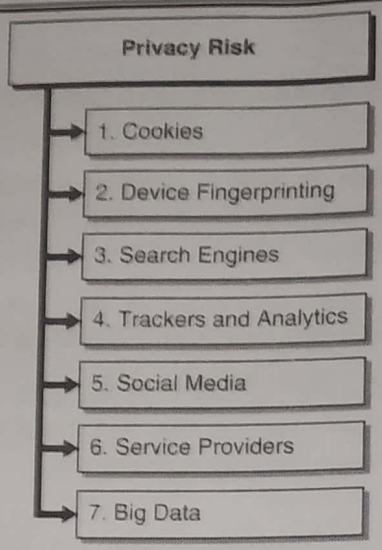
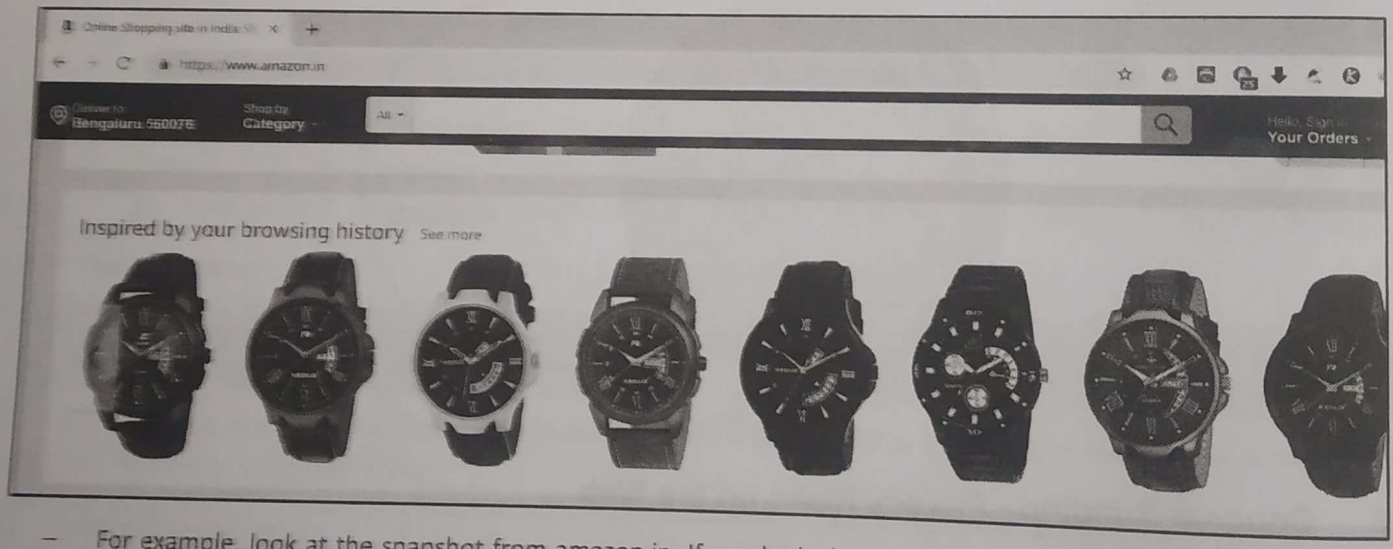



**Fig. 6.3.1**

## 1. Cookies

- As you learnt earlier, webservers can place cookies on the client side to save information that they care about. Cookies can not only be used for saving authentication and authorisation states, but cookies can also save a lot of other useful information that can be used later to shape the webserver behaviour and what is shown on a web page.
- Ever wondered that without even logging into the website, how does the website know the products that you last checked out?




- For example, look at the snapshot from amazon.in. If you look closely, I am not logged in into the website. I am still presented this page when I go to the website.
- It even says that "Inspired by your browsing history". How does it know what products I looked at on my previous visits to the website? That's the power of cookies.
- Websites keep storing the browsing history and your other browsing habits as you go to various sites.
- Cookies can breach you privacy by sharing your information with advertising, analytics, tracking, marketing and campaigning companies.

- That is precisely how you start seeing ads on various websites that carry forward the products that you looked on some website from your browsing history.
- Sometimes, your personal data, such as browsing habits, is sold to third-parties or companies who make product and marketing decisions based on your data and can offer you some attractive deals via ads to push you for purchasing the product you saw.

### 2. Device Fingerprinting

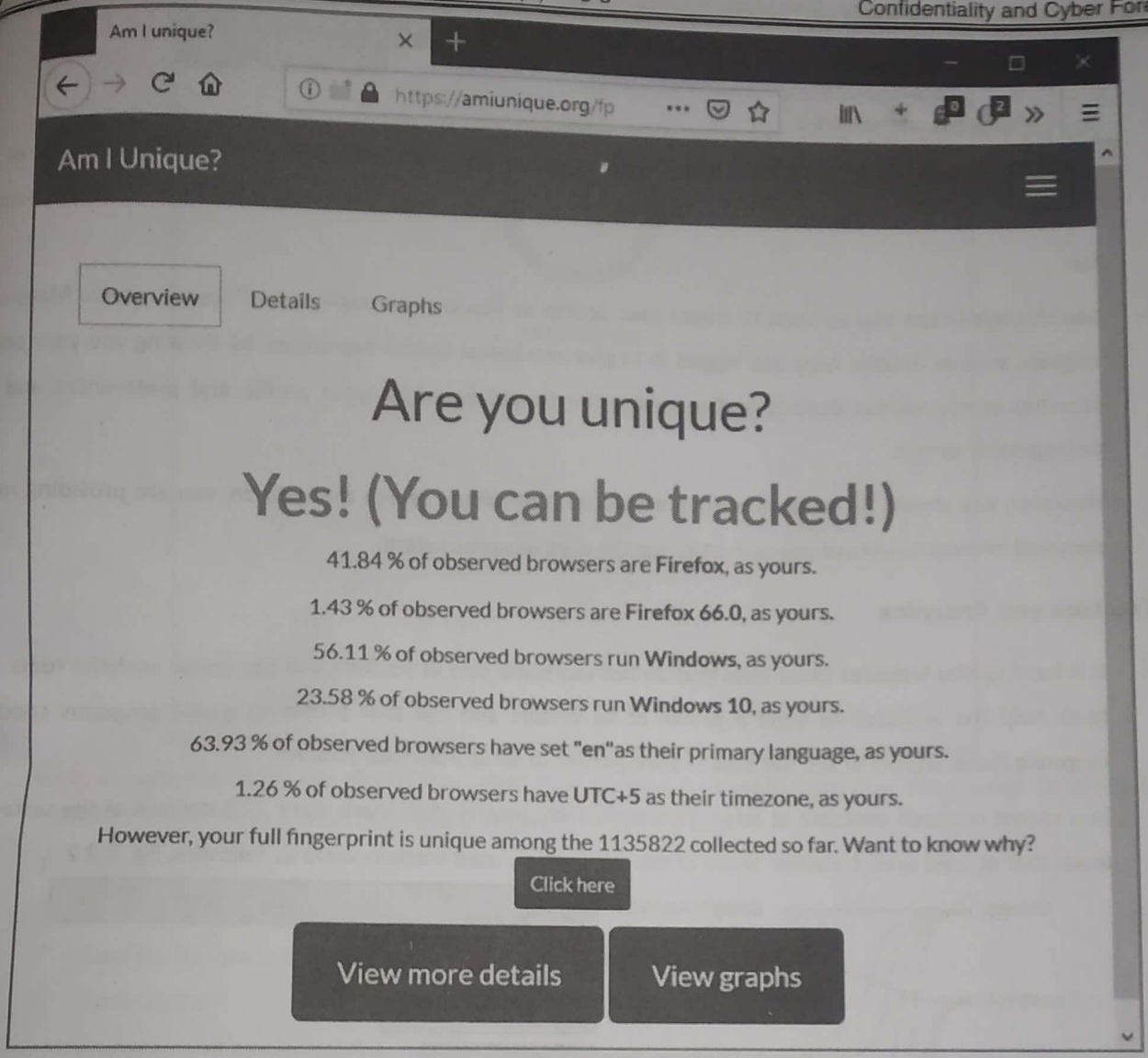
- Device fingerprinting or browser fingerprinting is one of the latest techniques used to correlate a device with the user identity and behaviour.
- When you visit a website, the website can uniquely identify you from its other visitors, even if you are not logged in, from your device characteristics.
- Various websites can just look into various device characteristics that could be unique to identify you as the client. The websites may not be looking to find your name or email id but more specifically what kind of person you could be and your general whereabouts such as locations, tastes and preferences.
- Table 6.3.1 shows some of the various device characteristics that could be used for fingerprinting the device and uniquely identity it.

**Table 6.3.1 : Various device characteristics**

| Sr. No. | Device Characteristics | What it could reveal |
|---|---|---|
| 1. | The User agent header | HTTP header sent to the server that contains information regarding your browser and operating system. |
| 2. | The Accept header | HTTP header sent to the server that contains information regarding the type of media that are acceptable for the response. |
| 3. | The Connection header | HTTP header sent to the server that contains specific options that are desired for that particular connection. |
| 4. | The Encoding header | HTTP header sent to the server that lists the compression methods supported by the browser. |
| 5. | The Language header | HTTP header sent to the server that indicates the preferred languages for the response. |
| 6. | The list of plugins | Browser-populated JavaScript attribute that gives the list of activated plugins in the browser. |
| 7. | The platform | Browser-populated JavaScript attribute that indicates the platform the browser is running on. |
| 8. | The cookies preferences | Browser-populated JavaScript attribute that indicates if the browser accepts cookies or not. |
| 9. | The Do Not Track preferences | Browser-populated JavaScript attribute that indicates your Do Not Track setting. |
| 10. | The timezone | Timezone offset of your browser obtainable through JavaScript. |

| Sr. No. | Device Characteristics | What it could reveal |
|---|---|---|
| 11. | The screen resolution and its colour depth | Browser-populated JavaScript attributes that indicate the resolution of the device's screen. |
| 12. | The use of local storage | JavaScript test to find out if local storage is supported. |
| 13. | The use of session storage | JavaScript test to find out if session storage is supported. |
| 14. | A picture rendered with the HTML Canvas element | Rendering of a specific picture with the HTML5 Canvas element following a fixed set of instructions. The picture presents some slight noticeable variations depending on the OS and the browser used. |
| 15. | A picture rendered with WebGL | Rendering of specific 3D forms following a fixed set of instructions. The picture presents some slight noticeable variations depending on the device of the user. |
| 16. | The presence of AdBlock | Test to find out if the AdBlock extension is installed. |
| 17. | The list of fonts | Flash attribute that gives the entire list of fonts installed on the operating system. |
| 18. | Cookies | Which cookies are present on the system identifying the websites opened on the device. |
| 19. | IP Address | The IP address of your device. It is very likely that you would be using the same IP address the next time you visit the website or at least the same service provider. |

- Scary, isn't it? Any website can know so much and plenty of other parameters which could help your device to be uniquely identified.
- To check if your device can be likely fingerprinted, you could probably go to https://amiunique.org/fp.
- For example, look at the results for my browser.
- The fingerprint is revealing my device unique stats and not necessarily my personal details. My device could be used by my family members, friends or office colleagues. Device fingerprinting does not uniquely identity the users in all the cases until and unless the device fingerprint is somehow linked to a user identity.
- For example, if amazon.in wants to fingerprint my device and wants to associate it with my user details, then it can because I use it for authenticating my details and making online purchases.
- It can then potentially sell my data to other partner companies and inform them that hey if you find this device fingerprint, it would be likely Pravin Goyal. Here are his details that you can use to offer him deals!




### 3. Search Engines

- Your normal day might involve several online searches –
  - Search for restaurants
  - Search for locations
  - Search for a particular syllabus topic
  - Search for other exciting things
- You would agree that what you search for has some sort of linkage to your demographic details such as
  - Your age
  - Your location
  - Your mood
  - Your money spending power
  - Your profession
  - Your likes

- Your requirements
- Your plans and activities

– All such information about you is private. Search engines can track and save your searches and can sell your search data to various companies who could then offer you products and services based on what you searched for.

– Search engines can also be used to create your profile as you click through various search results. Many search engines, such as Google, keep you logged in to give you better search experience by showing you your previous searches across various devices or fine tuning the results based on your profile and preferences and other demographic details.

– However, you should be cautious of such a practice. With every search that you do, you are providing massive personal information about yourself which can be used in various ways.

## 4. Trackers and Analytics

– It is hard to find websites these days that do not use some sort of trackers and site visitor analytics tools. These tools help the websites to build a profile of its visitors and use that profile to create programs specifically targeting those visitors or sell the data to third parties to serve malicious motives.

– In a recent research available at https://www.ghostery.com/study/, there were 77.4 percent of the tested page loads that at least used 1 tracker. Some of the most widely used trackers were as following Fig. 6.3.2.

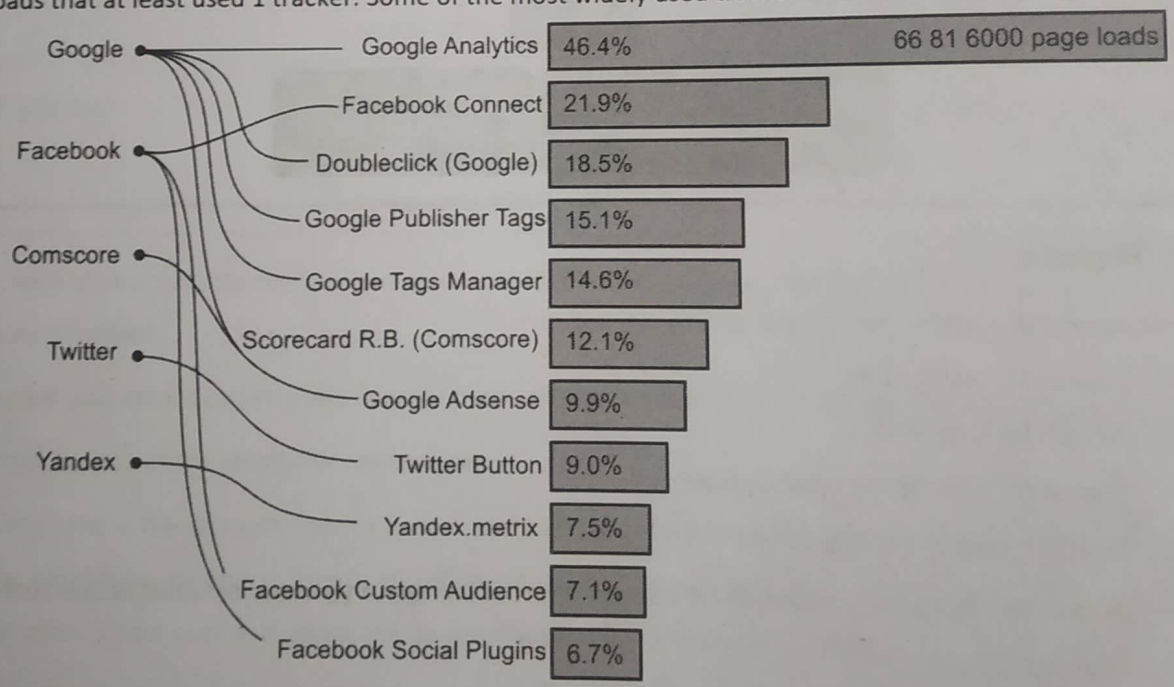
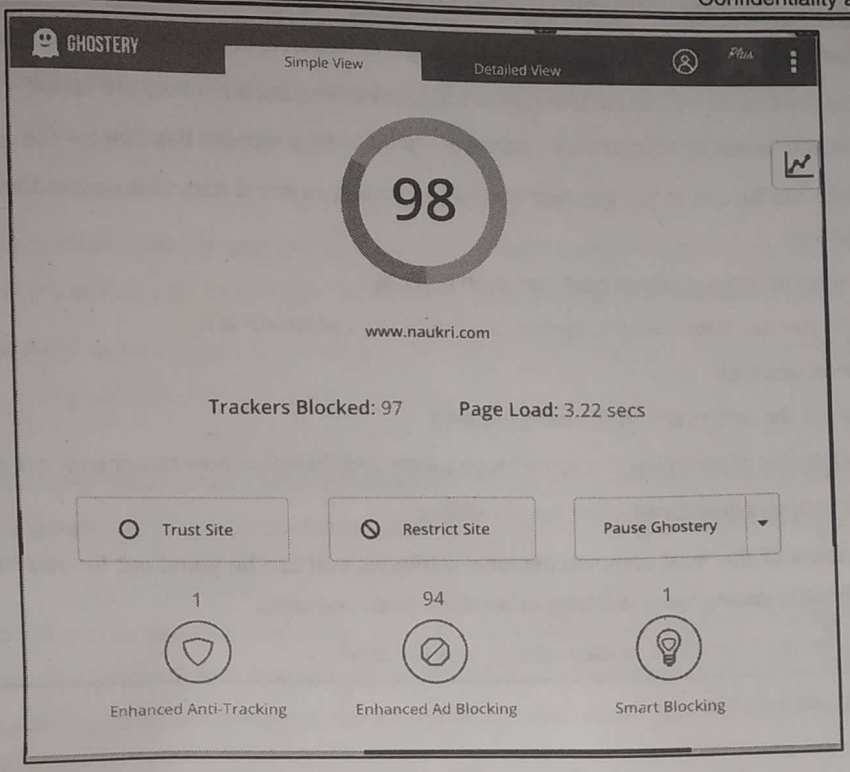



**Fig. 6.3.2**

– Let me give you an example. I use a tracker blocking extension on my browser. If I go to https://www.naukri.com/, the extension program shows that it has blocked 98 trackers!




- *Now, imagine a website like Naukri that might have thousands of visitors per day. The specific targeting for the category for job-seekers could be possibly around*
  - CV services
  - Consulting services
  - Courses for quick job placement
  - Online jobs
  - Lotteries and games if falling short of cash
  - Other ways of making money
- These trackers could belong to different categories. Various types of trackers are purposed at analysing different aspects of the sites and its visitors. Some common tracker categories are site analytics, social media, audio/video players, adult advertising, etc.

### 5. Social Media

- It is hard to find people actively using the internet but not hooked into some or the other forms of social media – Facebook, WhatsApp, Instagram, Reddit, LinkedIn, Twitter, and perhaps several more, are the most common platforms we all use today. You might be sharing your personal details such as phone number, age, location etc. or simply hundreds of photos every day.
  - Do you care about your privacy at all?
  - Do you care who sees your photos?
  - Do you care who can see your posts?
  - Do you care who can see your updates and figure out when you are not at home and can rob your house?

- Have you heard about online stalking (tracking and following people)?
- Have you constantly looked at someone's account to find out what they are up to?
- Have you looked at what privacy settings are present for a website that you use?

– Social media can be one of the greatest tools when finding personal data that people themselves share without any restrictions.

- It is easy to find out where have you been recently
- Which movies, books, actors, groups or websites you associate with
- How do you look
- Who are the others whom you hang out with
- Which brand of clothes and accessories you wear and therefore how rich or poor are you
- When are you online and when are you offline

– These are some of the most common personal attributes that can be found out for you from your social media profile without spending too much time or technical brain and skills.

– By the way, do your Facebook privacy settings look like this?

**Privacy Settings and Tools**

| | | | |
|---|---|---|---|
| **Your Activity** | Who can see your future posts? | Public | Edit |
| | Review all your posts and things you're tagged in | | Use Activity Log |
| | Limit the audience for posts you've shared with friends of friends or Public? | | Limit Past Posts |
| **How People Find and Contact You** | Who can send you friend requests? | Friends of friends | Edit |
| | Who can see your friends list? | Friends | Edit |
| | Who can look you up using the email address you provided? | Friends | Edit |
| | Who can look you up using the phone number you provided? | Friends | Edit |
| | Do you want search engines outside of Facebook to link to your profile? | No | Edit |

– What is wrong with it?

## 6. Service Providers

– You might be using various online services. Also, your internet service provider has clear visibility into which websites you visit, how long you stay there and your other online activities. These providers are not generally malicious but could sometime have malicious intent to collect and use your data for malicious motives.

– Irrespective of whether the service providers are malicious or not, your online data is at their mercy. If they fail to keep your online activities safe, your privacy could breached.

- For example, in 2015, AT&T, one of the largest telecom service providers in the world, suffered a data breach and exposed about 2,80,000 U.S. customers' names and full or partial Social Security numbers.
- The breaches occurred at call centres used by AT&T in Mexico, Colombia, and the Philippines when employees accessed sensitive customer data without adequate authorisation.
- Those employees took payment from third-parties who were apparently interested in customer names and Social Security numbers so that they could unlock stolen cell phones for sale on secondary markets.
- You could be victim of such incidents as well and your privacy data could be breached or exposed.

**7. Big Data**

- Big data is the latest trend in the industry focusing on various aspects of consumer behaviour, diseases, choices, demographic details, etc to predict the future patterns or find solutions to long standing problems such as cancer cure.
- Various aspects of your personal information are collected in bulk for this purpose. The big data companies claim to anonymise your personal data so that it cannot be traced back to you but nevertheless they hold and process a lot of personal data. Any data breach at these companies could indeed reveal a huge load of personal data and can potentially expose you.

## 6.4 PII Impact Levels

SPPU – May 19

**Q.** Describe PII impact levels with examples. **(May 19, 4 Marks)**

✍ ***Definition :*** *The PII confidentiality impact level indicates the potential harm that could result to the subject individuals and/or the organisation if PII was inappropriately accessed, used, or disclosed.*

There are three impact levels :

**1. Low**

The potential impact is Low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might

a. cause a degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.

b. result in minor damage to organisational assets

c. result in minor financial loss

d. result in minor harm to individuals

2. **Moderate**

- The potential impact is Moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals.
- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might
  a. cause a significant degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
  b. result in significant damage to organisational assets
  c. result in significant financial loss
  d. result in significant harm to individuals that does not involve loss of life or serious life threatening injuries

3. **High**

The potential impact is High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might

a. cause a severe degradation in or loss of mission capability to an extent and duration that the organisation is not able to perform one or more of its primary functions
b. result in major damage to organisational assets
c. result in major financial loss
d. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

### Factors for determining PII confidentiality impact levels

The following factors determine the impact levels of PII. These factors should be considered together and not individually to determine the impact level correctly.

1. **Identifiability :** Identifiability is the extent of personal identification possible using the PII. For example, Name, Fingerprints, Aadhar card, etc. can directly identify individuals.
2. **Quantity of PII :** The quantity of PII the organisation holds directly affects the impact that is likely possible in case of a privacy data breach. Typically, the higher the quantity, the higher is the possible impact.
3. **Data field sensitivity :** The organisation should consider the sensitivity of each data field and also all of them together. Certain fields such as postal code may not be considered sensitive of its own but when combined with date of birth and name could identify an individual correctly with 75% probability.
4. **Context of use :** Not all PII, even if containing the same type of data, might be equally sensitive. For example, a direct phone number of a national undercover agent may be more sensitive than the number of a regular citizen.
5. **Obligations to protect confidentiality :** Privacy laws around the world have direct impact on how PII is handled within the organisation. Privacy laws, such as GDPR, impose severe fine for any privacy breach. Any organisation, that is required to adhere to such laws, would likely be more watchful and attentive to PII protection.
6. **Access and Location of PII :**The location where PII is stored and the entities that have access to PII could directly impact the confidentiality of PII. You should carefully evaluate that the PII is continuously protected and is accessed only by authorised entities.

## 6.5 PII Confidentiality Safeguards

SPPU – May 19

Q. Discuss PII confidentiality safeguards. (May 19, 8 Marks)

**Your privacy is like your money :** protecting it online is your responsibility. Following are some of the considerations that might help you to protect your privacy on the web.

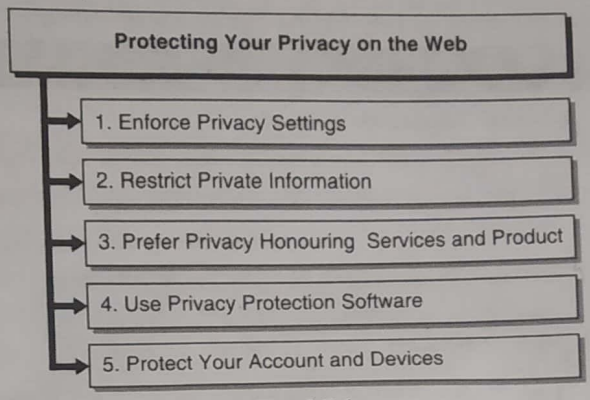



**Fig. 6.5.1**

### 1. Enforce Privacy Settings

Mostly any device, software or service that you use today come with a host of privacy enhancement settings. The default privacy settings might not be optimum, and you must carefully review the privacy settings of each device, software or service that you use to ensure that your private data is potentially protected. It might be a little time consuming to periodically check them all, but it can go a long way to ensure that your online privacy is adequately protected. Let's examine a few examples of privacy settings and what it could mean.

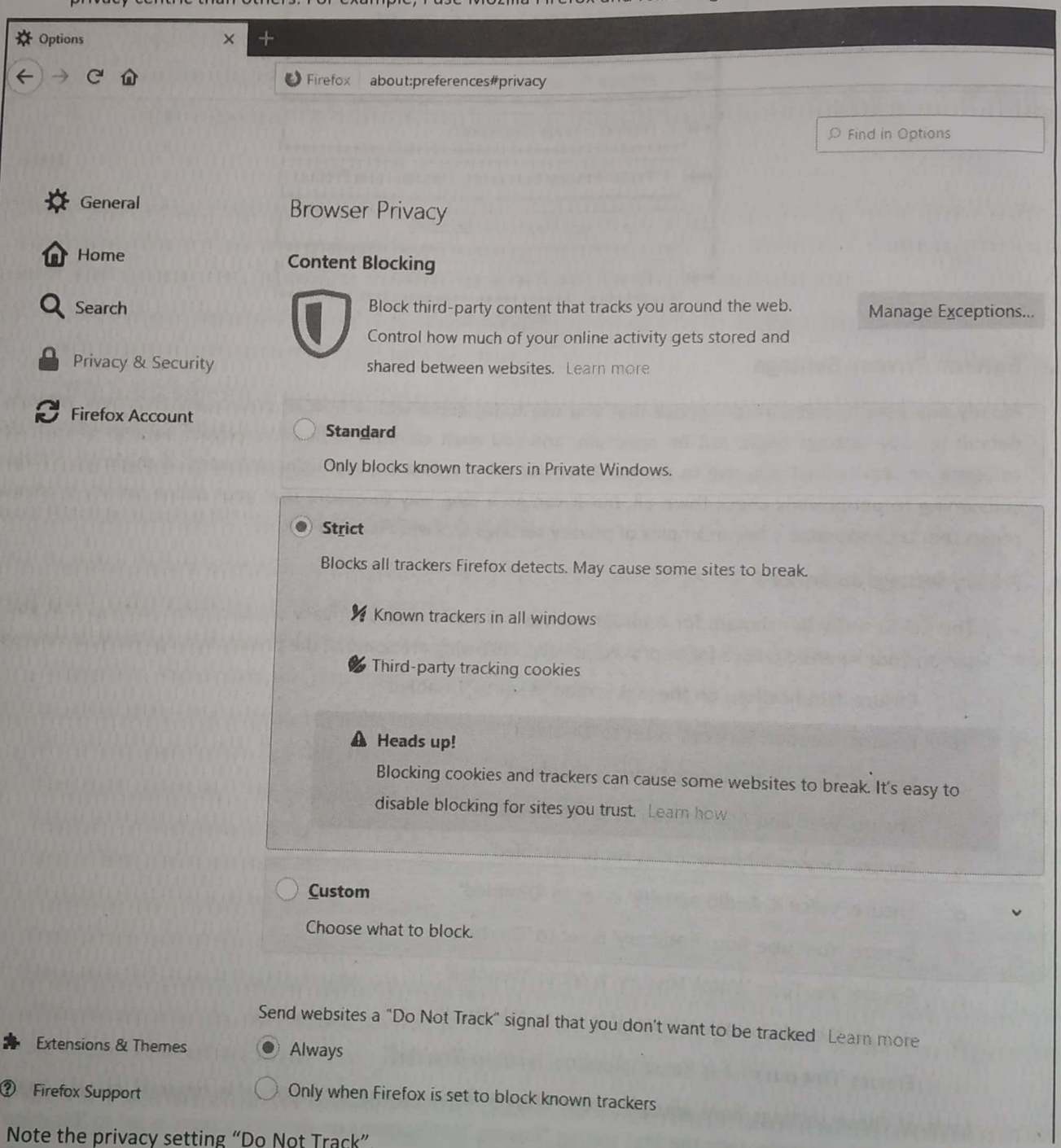
#### A. Privacy Settings on Device

- The CIS Security Benchmark for Android devices has listed several privacy enhancement settings that you could set on your Android device for improved privacy. Following are some of the privacy settings for your reference.
  - Ensure 'Notifications on the lock screen' is set to 'Disabled'
  - Ensure 'Location Services' is set to 'Disabled'
  - Ensure 'Back up to Google Drive' is 'Disabled'
  - Ensure 'Web and App Activity' is set to 'Disabled'
  - Ensure 'Device Information' is set to 'Disabled'
  - Ensure 'Voice & Audio Activity' is set to 'Disabled'
  - Ensure 'YouTube Search History' is set to 'Disabled'
  - Ensure 'YouTube Watch History' is set to 'Disabled'
  - Ensure 'Google Location History' is set to 'Disabled'
  - Ensure 'Opt out of Ads Personalization' is set to 'Enabled'
- Each of these settings help you gain control over what private information is retained or sent to the service provider. For example, take the first setting "Ensure 'Notifications on the lock screen' is set to 'Disabled'" – if you don't set this and even if your phone is locked, the app notifications can be read by anyone. Do you really want that?

- Similarly, there could be various privacy settings specific to the device you use. You should explore these settings and configure them to protect your privacy.

**B. Privacy Settings on Software**

- Software such as browsers offer quite a few privacy settings. You should configure them to provide maximum privacy even if that means a little bit of discomfort or little distorted user experience. Some browsers are more privacy centric than others. For example, I use Mozilla Firefox and following are my privacy settings.



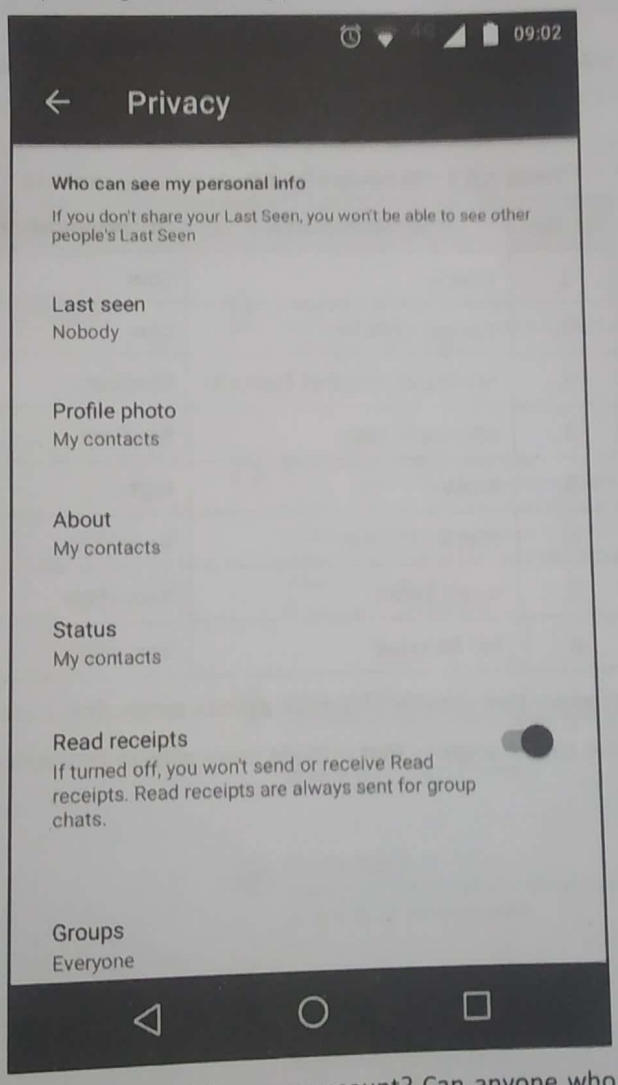

- Note the privacy setting "Do Not Track".

***Definition :*** *Do Not Track (DNT) refers to a mechanism for communicating a user's preference regarding tracking on the internet.*

- As you understand, tracking collects the user's activities. DNT is a mechanism to let the webserver know that you do not wish to be tracked. Note here that even if you have configured DNT, honouring it or not is up to the webserver. Some webservers do honour it whereas plenty others continue to track you ignoring your tracking preference.
- So, look at all the software that you use for your online activities on all your devices and ensure to configure the privacy settings on them to maximise your privacy protection.

**C. Privacy Settings on Service**

- Once you have protected your device and software, you should look at what specific privacy enhancing settings does the online service provide you specifically and configure them suitably.
- For example, here are privacy settings on WhatsApp.




- Is it similar to what you have configured for your account? Can anyone who has your number see your online presence, your photos and your status? Is this desirable?
- Those are some of the questions to be evaluated when you consider the privacy settings. Similarly, you should review your privacy settings for other services that you use such as Google, Apple, Facebook, Twitter, etc. and ensure that they are configured to provide you maximum privacy protection.

**2. Restrict Private Information**

- In sports, there is a usual saying that "the points saved are equal to points scored". Similarly, restricting your private information to yourself is way easier than trying to safeguard it later on once the information is already given out.
- Do not give your personal information to any random sites, forms, competition, surveys, piracy websites, or social media. The more information you put out there the more difficult it is to protect it later on. Refrain from updating about your status and whereabouts very frequently.
- Do not disclose much in advance about your activities in plans. Be careful about what you post online and what effect it might have for your privacy now or in the future.

**3. Prefer Privacy Honouring Services and Products**

- You have a variety of options these days to choose what services and products you use. When making a choice, prefer services and products that honour your privacy and have controllable privacy configuration options. Let's see some examples.
- As I indicated earlier, some browsers are more privacy centric then others. You would be better off using them than others. Table 6.5.1 shows a list of browsers and their probable privacy ranking based on the features they provide.

**Table 6.5.1 : Browsers and their privacy ranking**

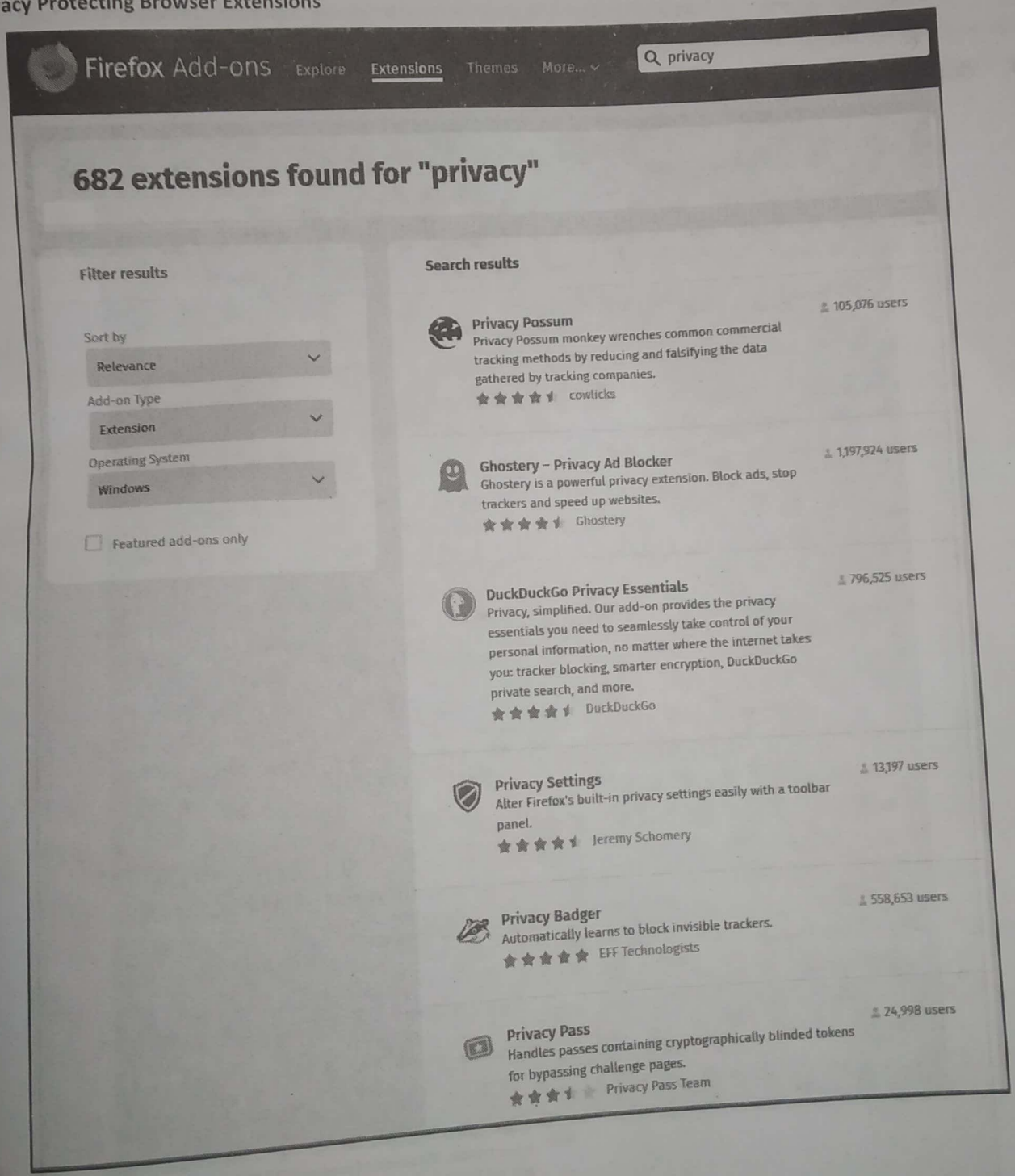
| Sr. No. | Browser Name | Privacy Ranking |
|---|---|---|
| 1. | Opera | Low |
| 2. | Google Chrome | Low |
| 3. | Microsoft Internet Explorer | Medium |
| 4. | Microsoft Edge | Medium |
| 5. | Brave | High |
| 6. | Mozilla Firefox | Very High |
| 7. | Apple Safari | Very High |
| 8. | Tor Browser | Very High |

- You should choose the browser that provide you more privacy protection. I use Mozilla Firefox.
- Similarly, you could choose search engines that provide more privacy protection than Google Search. Some of the options are as following.
  - Search Encrypt
  - StartPage
  - DuckDuckGo
  - Gibiru
  - Swisscows
  - Yippy
  - BitClave
  - Qwant
  - Discrete Search
  - Oscobo

**4. Use Privacy Protection Software**

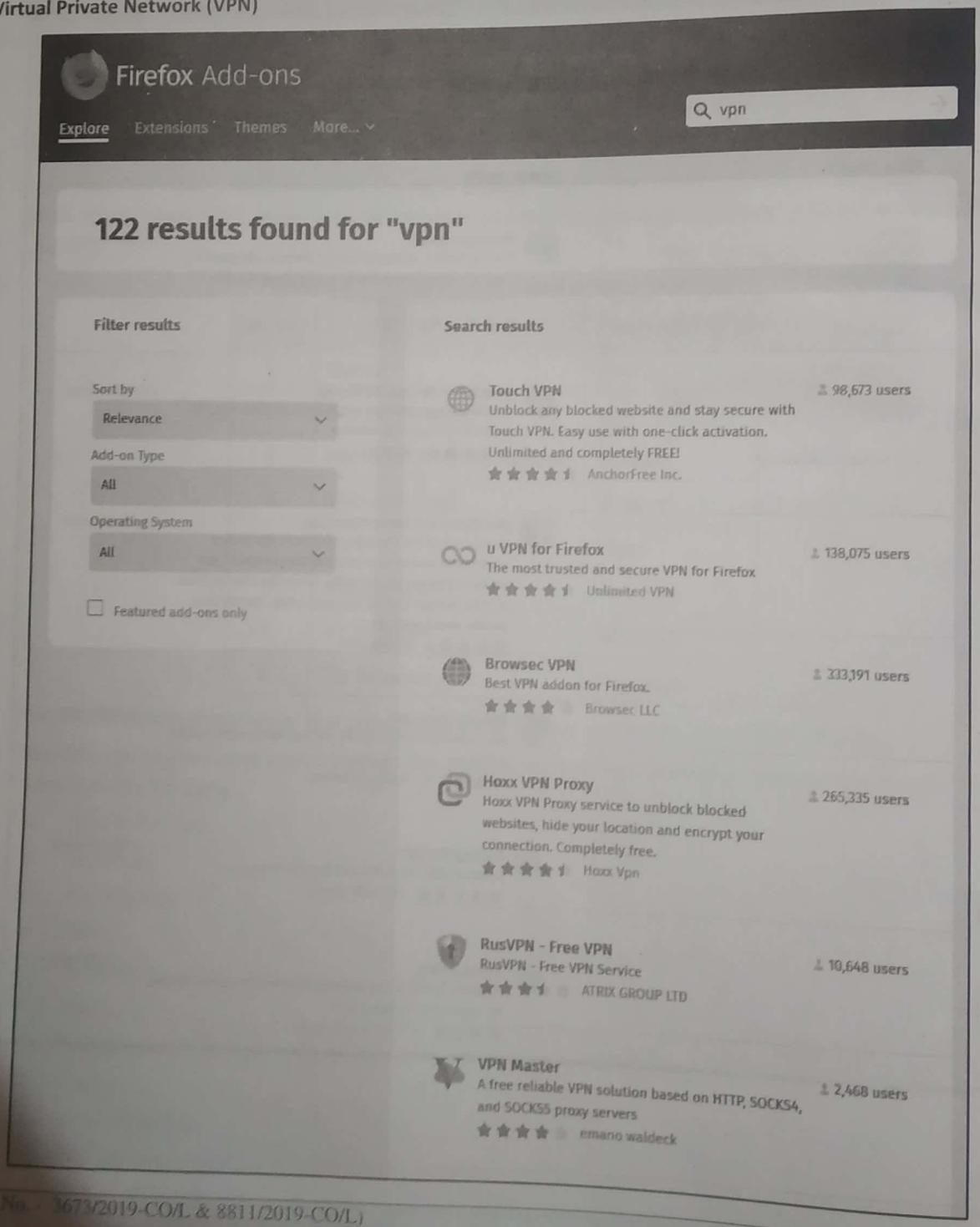
- You can add multiple extensions to your existing software (browsers, OS, network connections, etc.) that could provide enhanced privacy protection.
- These additions top-up the privacy protection capabilities that are lacking in the base software. Let's see some examples.

**A. Privacy Protecting Browser Extensions**

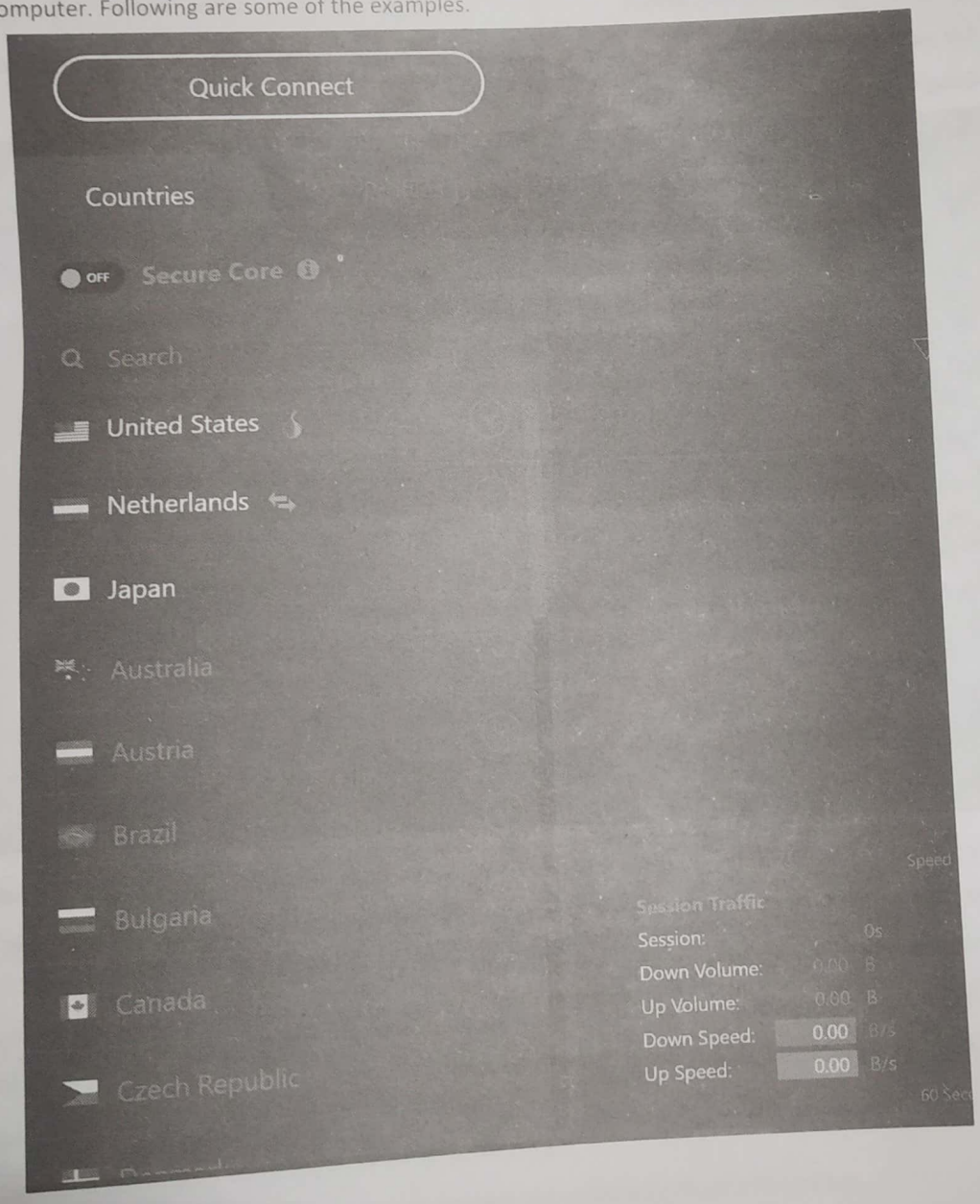


- There are several browser extensions that you can install to provide privacy protection. These extensions come with various capabilities. The most used capabilities are blocking trackers and removing advertisements whenever you visit any website.
- If you recall, I earlier gave an example of how my browser privacy protection extension blocked 98 trackers on Naukri website.
- You can search for various add-ons for your respective browsers. These add-ons are available for most of the widely used browsers and provide similar capabilities. Here is an example on Mozilla Firefox.
- You can choose the one you like and add it to your browser. I use Ghostery.

**B. Virtual Private Network (VPN)**

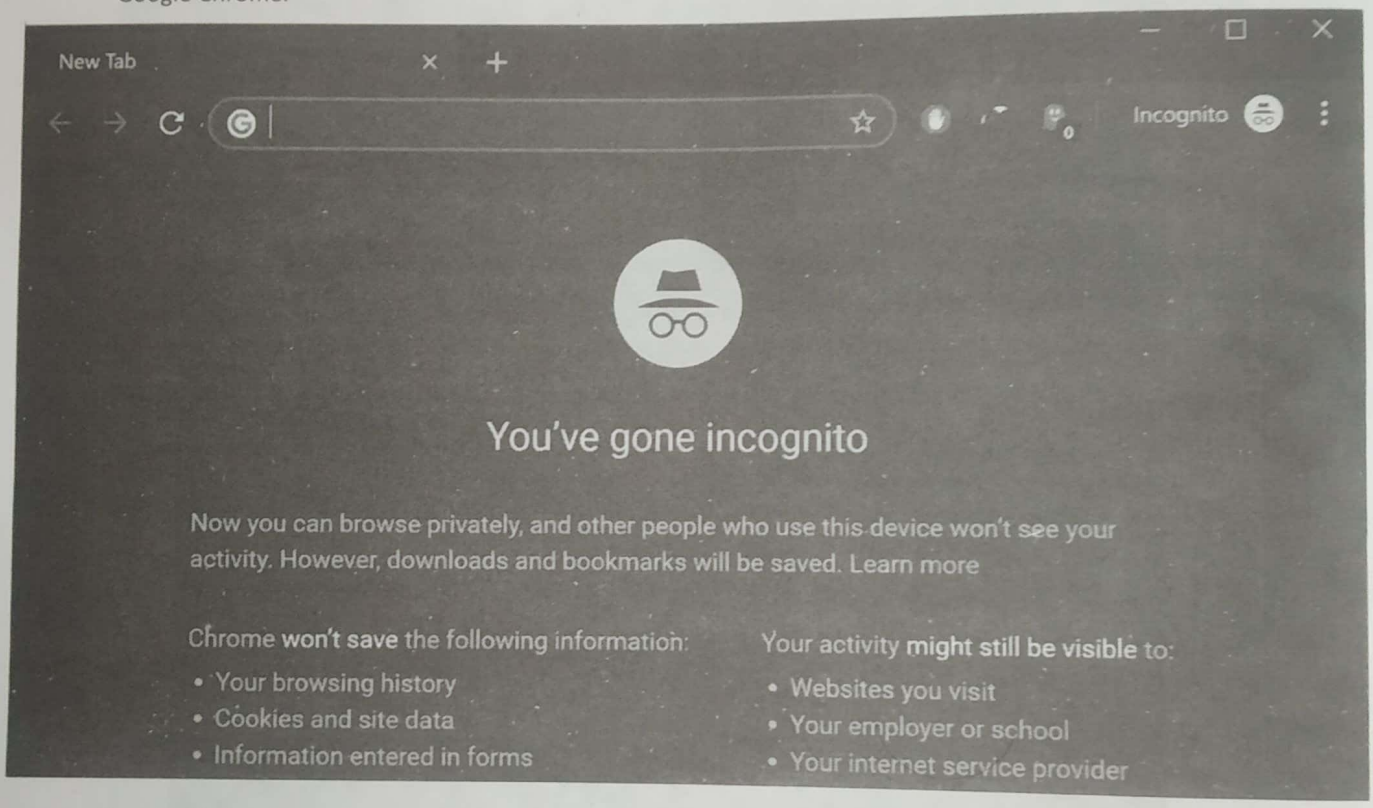


- You could use a VPN software to connect to the internet. That way your location and other demographic details are protected automatically. The IP address assigned to your device is not the actual IP assigned by your internet service provider but the one assigned by the VPN server.
- You could also alter your location. For example, being in India, you can connect via a server in Singapore. The websites that you visit would then assume that you are coming from Singapore and would not be able to track your demographics solely based on your device characteristics or IP address.
- Additionally, VPN traffic is entirely encrypted. So, even if you are browsing websites that do not yet use https, your browsing activities would still be encrypted. You could use VPN as a browser extension or as a software on your computer. Following are some of the examples.

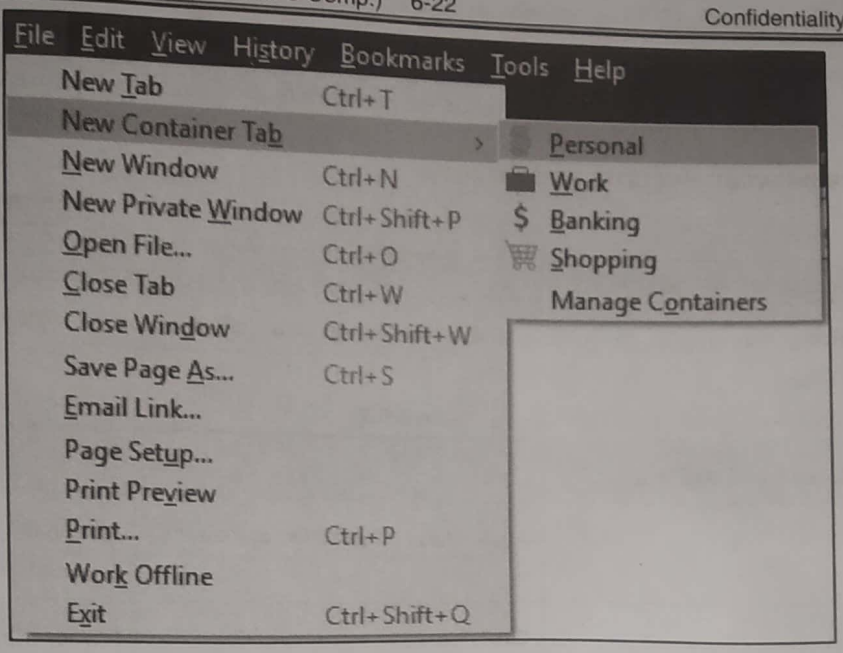


**C. Private Mode of Browsing**

- You could also choose to use the private mode of browsing. Most of the widely used browsers allow you to use private mode. Note here that the private mode does not make you anonymous on the internet and neither it hides the information from your internet service provider or the websites that your transact with.
- Private Browsing works by removing cookies, browsing history, and stored passwords while you are browsing once you close your Private Window. This makes it harder for the websites to track your browsing habits if you are not logged in. Also, if anyone else shares your device, it would be difficult to trace what websites you have visited previously using that device.
- For example, following is a snapshot of Google Chrome Private Mode of browsing. It is called incognito mode in Google Chrome.




- You could also use container tabs feature in Firefox where you can isolate your browsing environments from each other. This isolation helps to protect your privacy from other services that you use. For example, you can isolate your online shopping browsing environment from your banking environment.
- You could also isolate personal environment from business environment and likewise. Following is an example of containers (environments) that I have defined for myself.




**5. Protect Your Account and Devices**

- Privacy protection also requires that you secure your devices and accounts. Follow regular security practices such as
  - Strong passwords for your accounts and devices
  - Multi-factor authentication
  - Security hardening
  - Installing anti-malware protection
  - Locking your devices when you are not using them
  - Not sharing your account details
  - Watching out if someone is overlooking as you type
  - Cautious when clicking links
  - Cautious when opening email attachments
  - Cautious when providing your personal details anywhere
  - Cautious of which websites you go to
  - Cautious of which services you subscribe to
  - Cautious of which accounts you have linked for identity management
- Such security hygiene practices go a long way to ensure that your private information is kept secured and is not disclosed.
- As an organisation, you should also ensure that you
  - Limit the collection, use and retention of private data
  - Have operational safeguards in place to protect the collected private information
  - Create policies and procedure to ensure that any private data is appropriately handled

- Conduct privacy awareness training throughout your organisation
- Conduct privacy impact assessments periodically to identify and minimise privacy risks

### 6.5.1 Difference between Security and Privacy

SPPU – March 19(In Sem.)

**Q. List the differences between Security and Privacy. (March 19, 5 Marks)**

Security and Privacy may appear to provide similar protection and services. But, in reality, there are some key differences between them.

**Table 6.5.2**

| Sr. No. | Comparison Attribute | Security | Privacy |
|---|---|---|---|
| 1. | Scope | All business information and assets | Personally Identifiable Information |
| 2. | Based on | CIA Triad | Privacy principles and laws |
| 3. | Usual attack targets | Security Vulnerabilities | Information disclosure |
| 4. | Implemented and enforced using | Technical products and services | Principles and rights |

## 6.6 Concept Building - Privacy Laws Around the World

– As you learnt earlier, there are several privacy laws around the world. Some of them are as shown in Table 6.6.1.

**Table 6.6.1 : Privacy Laws**

| Region | Law / Protection |
|---|---|
| Argentina | Personal Data Protection Act 2000 |
| Australia | Australia's Privacy Act 1988 |
| Canada | Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 |
| France | France's Data Protection Act 2 |
| European Union | General Data Protection Regulation (GDPR) |
| India | Personal Data Protection Bill, 2018 |

– Out of these, GDPR really turned heads around privacy around the world with suggesting penalties of up to 20 million Euros, or 4% of annual global turnover, whichever is higher. Companies and organisations that handle personal or private data must abide by the respective local laws to ensure sustainable business and avoid steep penalties and loss of reputation.

– Let's look into GDPR at a high-level so that you understand what it contains.

- GDPR has :
  - Eighty-one pages
  - Eleven Chapters
  - Ninety-nine Articles
- It came into effect on 25-May-2018. It applies to any company processing personal data of EU citizens. Fundamentally, it gives data subjects (users) eight rights via seven principles.
- Table 6.6.2 shows the rights of the individual under GDPR.

**Table 6.6.2**

| Sr. No. | Rights | Description |
|---|---|---|
| 1. | The right to be informed | How will the collected data be used? Privacy Notice is one of the ways to define how data is collected and used. |
| 2. | The right of access | Users can check what personal data about them is held by the company and how it is being used. Companies must respond within 1 month of receiving such a notice. |
| 3. | The right to rectification | Users should be able to correct / update information about them. |
| 4. | The right to erasure | Users have the right to ask to erase their personal data. |
| 5. | The right to restrict processing | Users have the right to restrict processing of their personal data temporarily. |
| 6. | The right to data portability | Users should be able to download their personal data in human readable format and be able to port it to a different processor (company). |
| 7. | The right to object | Users can object to processing of their personal data for any reason. |
| 8. | Rights in relation to automated decision-making and profiling | Where profiling or automated decision making takes place, there should be a provision to challenge the automated decision and be able to involve a human to reconsider the decision. |

- The seven principles defined by GDPR are as following.

1. Personal data must be processed fairly and lawfully
2. Personal data must be collected for specified explicit and legitimate purposes
3. Personal data collection should be adequate, relevant and limited to only what is necessary
4. Personal data must be accurate and kept up to date
5. Personal data must not be kept for longer than necessary
6. Personal data must be processed in a manner that ensures appropriate security
7. Personal data must be only used where the data controller can demonstrate accountability

## 6.7 Cybercrime

- Before you understand cybercrime, let's understand what crime is. In plain terms, crime is an illegal act for which someone can be punished.
- Crime involves defying (challenging) the laws and results into a penal action based upon the magnitude and impact of crime done.

**Note :** A quick note folks, it is incorrect (as an industrial practice) to give a space between Cyber and terms related to it. For example, you should not write "Cyber <Space> Security". Always, write Cybersecurity (as one word without any space between the words Cyber and Security). Other terms related to Cyber as well should be written without any space between them. These include (but not limited to)

- Cybersecurity
- Cyberspace
- Cyberattacks
- Cybercrimes, etc.

### 6.7.1 Introduction, Definition and Origin

- The term cyber means something that relates to computers. So, a cybercrime is usually understood and defined as

✍ ***Definition :*** *Criminal offenses that are performed using computers are called cybercrime.*

- Note here that the term computer is relative here – it includes but is not limited to Desktops, Laptops, Mobile Phones, Tablets or any other form of a computing device.
- The means to carry out a crime could involve internet, or other forms of communication such as telephone lines or Bluetooth connections.
- Stealing money physically from people remains a crime. It is just that when stealing happens using computers (say via online fraud), the same act of stealing money becomes a cybercrime.
- The exact origin of cybercrime is hard to tell. With the increasing adoption of computers in 1970s and the invention of internet in 1990s, a lot of people with varied background became experimenting with what is possible with technology.
- The early systems were still under development as the technology was new and their implementations were not fool-proof or matured then. Encryption, hashing and other security related technologies were not then invented. From what is reported and documented, Table 6.7.1 shows some of the major cybercrimes from the past.

**Table 6.7.1 : List of some cybercrimes**

| Sr. No. | Year | Reported Cybercrime |
|---|---|---|
| 1. | 1971 | Phone Phreak attack – used whistle to make free long-distance calls |
| 2. | 1973 | A bank employee used computer to steal 2 million dollars |
| 3. | 1981 | Ian Murphy – first person to be convicted for cybercrime. He hacked AT&T network to make calls at cheap |

| Sr. No. | Year | Reported Cybercrime |
|---|---|---|
| 4. | 1982 | Elk Cloner, a virus, affected Apple II OS |
| 5. | 1986 | US congress passed the Computer and Fraud Act, making hacking and theft illegal |
| 6. | 1988 | A worm infects more than 600,000 networked computers on US Defense Department's APRANET |
| 7. | 1989 | First large-scale case of ransomware |
| 8. | 1994 | Internet was born and gave rise to several cybercrimes |
| 9. | 1995 | Macro-based viruses start attacking computer files and programs |
| 10. | 1997 | The FBI reports that over 85% of US companies had been hacked |
| 11. | 1999 | Melissa Virus is released. It becomes the most virulent computer infection |
| 12. | 2000+ | Several new types of cybercrimes begin showing up as frequent as daily... |

### 6.7.2 Cybercrime and Information Security

- The term information security is now widened further to include some of the elements from cybersecurity.

✍ ***Definition :*** *Cybersecurity at a broad level means the security measures taken to protect computers and networks exposed to the internet against unauthorised access or attack.*

- Earlier information security primarily meant safeguarding information and information system and provide CIA triad protection. As and when more systems got connected and were exposed over the internet, it was required to add another dimension to safeguarding the assets and data – cyberspace.

✍ ***Definition :*** *Cyberspace is the term used to refer the online world of computer networks and especially the Internet.*

- Cybercrimes typically involve not only crimes against the information (or data) but also the general systems and networks that constitute (or live) in the cyberspace. It could be
  - Stealing information
  - Defacing a website
  - Bringing down a website
  - Tricking users in online fraud
  - Distribution of pirated software, books, music, videos, movies and anything else and
  - Several other forms of illegal offenses
- Information security domain was never meant to address such cybercrimes. Hence, a new field of security called cybersecurity has evolved to address such issues. Table 6.7.2 provides a quick comparison summary between information security and cybersecurity (dealing with cybercrimes).

**Table 6.7.2 : Comparison of information security and cybersecurity**

| Sr. No. | Information Security | Cybersecurity (dealing with cybercrimes) |
|---|---|---|
| 1. | Information focused (irrespective of internet). | Internet focused (protect systems and data exposed over internet). |
| 2. | Physical security is within the scope. | Physical security is out of the scope. |
| 3. | Threats scope is limited. | Threat scope is unlimited (as exposed over internet). |
| 4. | Exposure is usually called leakage. | Exposure is usually called cyberattack. |
| 5. | Quite an old field. | Recent development and focus. |

- NIST has developed a Cybersecurity Framework that addresses the risks from cybercrimes and provides a general layout of protection from cybercrimes.

**Table 6.7.3**

| Function | Category |
|---|---|
| Identify | Asset Management |
| | Business Environment |
| | Governance |
| | Risk Assessment |
| | Risk Management Strategy |
| | Supply Chain Risk Management |
| Protect | Identity Management and Access Control |
| | Awareness and Training |
| | Data Security |
| | Information Protection Processes and Procedures |
| | Maintenance |
| | Protective Technology |
| Detect | Anomalies and Events |
| | Security Continuous Monitoring |
| | Detection Processes |
| Respond | Response Planning |
| | Communications |
| | Analysis |
| | Mitigation |
| | Improvements |
| Recover | Recovery Planning |
| | Improvements |
| | Communications |

### 6.7.3 Categories of Cybercrimes

- At a broad level, there are three categories of cybercrimes.

1. Computer-assisted crime
2. Computer-targeted crime and
3. Computer is incidental

- The categorization of cybercrimes helps the jurisdiction to attach the relevant punishment to the attacker.

#### 1. Computer-assisted crimes

✍ ***Definition :*** *Computer-assisted crimes are the ones where computers are used as a tool to carry out the crime.*

In this type of crime, computers are just used as a means to carry out the crime. These generally involve less technical expertise and rely on general human behaviour or weaknesses for exploit. Some of the examples of computer-assisted crimes are as follows:

- Attacking financial systems to carry out theft of funds and/or sensitive information
- Obtaining military or intelligence information
- Carrying out industrial spying
- Attacking critical national infrastructure systems
- Spreading fake news to disrupt national peace

#### 2. Computer-targeted crimes

✍ ***Definition :*** *Computer-targeted crimes are the ones where the computer itself was the victim of the attack and then was used to cause harm to its owners.*

In this type of crime, victim's computers are directly exploited by attacker's computers. These types of attacks require significant technical expertise. Also, these are usually targeted to a specific group, organisation or an individual. Some of the examples of computer-targeted crimes are as follows:

- Distributed Denial-of-Service (DDoS) attacks
- Capturing passwords or other sensitive data
- Installing malware with the intent to cause destruction
- Exploiting other system weaknesses or vulnerabilities

#### 3. Computer is incidental

- This is not really a cybercrime category as such. In such type of crimes, having a computer or not having a computer would not matter much.
- For example, if you got some sensitive and confidential military information from a friend and stored it in the computer instead of writing it on a paper, this would be purely a case where storing information in the computer could have been avoided. Computers do not play any significant role in committing such a crime.

- Computer is purely incidental where such information could be just hiding or encrypted but the source of crime was human behaviour or getting information from other intelligence sources. Having a computer or not having a computer in such cases does not matter considering the impact of the crime.

### 6.7.4 Classification of Cybercrimes

- Various institutes and organisations have classified cybercrimes on various basis. There is no fixed or accurate classification of cybercrime as such.
- Classification of cybercrime depends upon the point of view you are looking cybercrime from. Some of the broad classification levels that exist today are as shown in Fig. 6.7.1. Each of these can be further divided into various sub-types and categories.

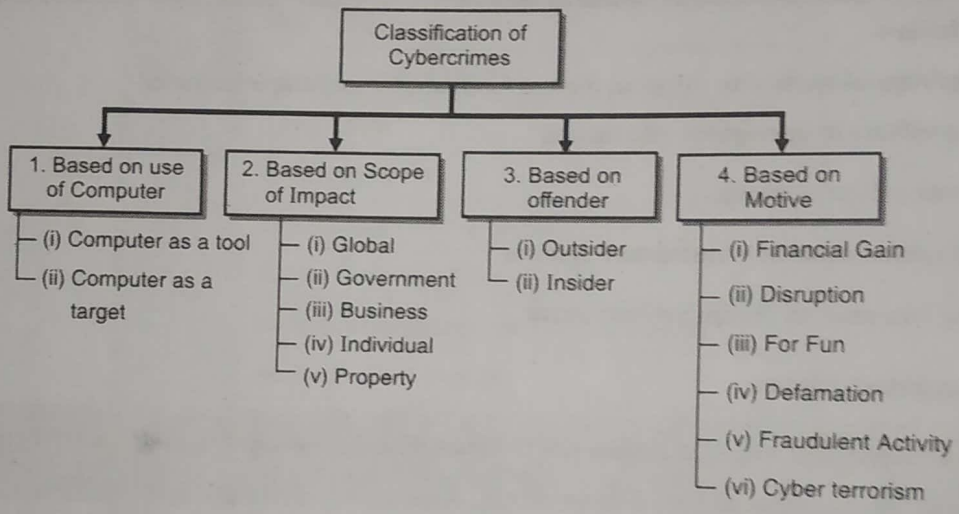



Fig. 6.7.1

- You have already learnt about the classification of cybercrimes based on the use of computer in the previous section. Classification based on motives are self-explanatory. Let's dive a little deeper on the classification based on the scope of cybercrime.

**Classification of cybercrimes based on the scope of impact**

Based on the scope of impact, cybercrimes can be classified as following.

1. **Global**

These are cybercrimes that have global impact. More than one nation is impacted either directly or indirectly. Examples of this could be cyberterrorism, wide-spreading virus or worms or carrying of fraudulent activities that violate the rights for various citizens.

2. **Government**

These are cybercrimes specifically targeted at the Government. This could be online anti-campaigns, fraudulent activities during election times or defaming Government by spreading fake news or altered videos or sound clips. The core objective is to spread unrest and fear amongst the mass.

3. **Business**

These are cybercrimes targeted at organisations or specific businesses. For example, during festive season, a competitor website might try to do a DDoS attack to bring down the website of the competitor to boost up its sales. Another types of cybercrimes might include corporate espionage (spying) on company internal communication, business plans or trade secrets.

4. **Individual**

Cybercrimes targeted at individuals try to elicit (get) the sensitive or confidential information such as banking account details, personal details such as passport number or any other personal information. For example, during a ransomware attack, the attacker could lock the computer of the victim and may demand a sum of money for unlocking it. There could be attacks such as password sniffing or social engineering where the attacker tricks the user to provide sensitive information that could be further used to cause financial or reputational loss for the individual.

5. **Property**

Cybercrimes against property are the criminal acts against the digital property such as computers, domain names, websites, etc. These includes cybercrimes such as the following.

a. **Cybersquatting :** Cybersquatting or domain squatting is the practice of registering names, especially well-known company or brand names, as Internet domains, in the hope of reselling them at a profit. For example, someone could try to buy the domain name of goooogle.com. It looks so similar to the original google.com that the person owning goooogle.com may try to sell the domain name to Google for a huge amount of money or may trick the users to come to the fake website instead of the original one.

b. **Cyber vandalism :** It is a cybercrime that damages someone's data from the computer in a way that disrupts the victim's business or image. It involves anything that damages your digital content, websites, personal or private data.

c. **Cyber trespass :** This involves intentional and unauthorised acts of accesses, alterations, deletions, damages, or disruptions to any computer system, computer network, computer program, or data.

## 6.7.5 The Legal Perspectives of Cybercrimes

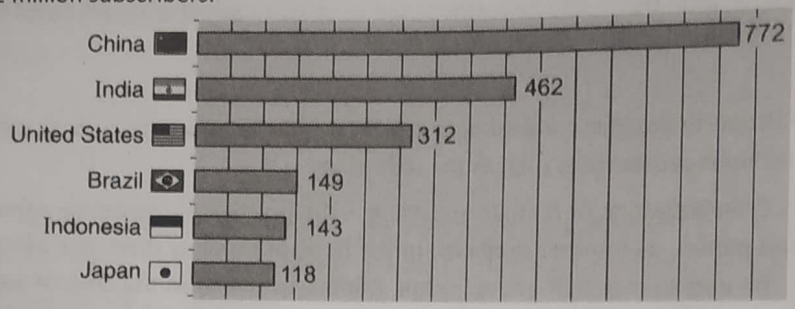
- The technology is changing every day at an exponential rate. New ways to commit cybercrimes are being experimented and adopted. The laws, by their nature, do not have such a flexibility to cope up with all the ways of performing cybercrimes and stay at the top of technology.
- The legal perspective of cybercrimes becomes even more challenging when the criminal acts are cross-border or across different legislations.
- Who executes the cybercriminals? How much support will the different nation provide to prosecute its citizen and held her accountable for the act? These are all complex scenarios where the answer really depends on case-by-case basis.
- To straighten out such complex scenarios and provide an over-arching guideline about how the law would apply to cybercrime, the nations define and adopt cyberlaws.
- Some developed countries like the US have cyberlaws from 1970s onward whereas countries like India felt the need for cyberlaws only in the year 2000. Let's review the legal perspective of cybercrimes from Indian perspective as well as Global perspective.

## 6.7.5(A) The Indian Perspective

- The first cyberlaw in India came into force in the year 2000 and was called Information Technology Act. It was later amended in 2008 to widen the scope of the act as per the need and the feedback received on the original bill.
- Post amendment, it is now called Information Technology (Amendment) Act 2008 herein after referred to as ITAA 2008.

### 1. Cybercrime scenario in India

- At the end of 31st December 2017, as per the reported statistics by https://www.internetworldstats.com/top20.htm, India is the 2nd largest consumer of the internet in the world. It has around 462 million subscribers.




- The National Crime Records Bureau reported the following number of cybercrimes in India between 2014-2016.

| Crime Incidence | | | Percentage Variation | |
|---|---|---|---|---|
| 2014 | 2015 | 2016 | 2014-2015 | 2015-2016 |
| 9,622 | 11,592 | 12,317 | 20.5% | 6.3% |

- Top 3 states for cybercrimes were:
  1. Uttar Pradesh (2,639 cases) (21.4%) followed by
  2. Maharashtra (2,380 cases) (19.3%) followed by
  3. Karnataka (1,101 cases) (8.9%)
- During 2016, Top 3 motives for cybercrimes were:
  - 48.6% for illegal gain (5,987 out of 12,317 cases) followed by
  - 8.6% for revenge (1,056 out of 12,317 cases) followed by
  - 5.6% (686 out of 12,317 cases) insult to the modesty of women
- The Government of India has created a Cybercrime Reporting Portal where you could file cybercrime grievances. You can also reach out to your nearest cybercrime investigation cell for reporting cybercrimes. The portal can be accessed at https://cybercrime.gov.in/cybercitizen/home.htm. You can register a complaint anonymously or by identifying yourself. Following details are required for reporting a complaint.
  1. Category of Crime
  2. Suspect details [social media ID, message number, email ID, etc.]
  3. Crime incident details

a. Date of incident
b. Time of incident
c. State
d. District
e. Police Station
f. Crime detailed information
g. Website URL, if any
h. Evidences [snapshots of messages, email copy, attachment copy, etc.]

## 2. Objectives / Goals of the ITAA 20008

1. Boost the growth of electronic based transactions.
2. Provide legal recognition for e-commerce and e-transactions.
3. Provide legal recognition to digital signatures.
4. Facilitate e-governance.
5. Prevent computer-based crimes.
6. Ensure security practices and procedures in the context of information technology.
7. Protection of personal data and information.
8. Protection of Critical Information Infrastructure to ensure national security, economy, public health and safety.
9. Provide penal provisions to prevent cybercrimes in the respective acts.

## 3. Structure of ITAA 2008

– ITAA 2008 consists of 13 chapters and 90 clauses. Table 6.7.4 shows chapters and overall provisions defined therein for your reference.

Table 6.7.4

| Chapter number | Chapter name | Provision for |
|---|---|---|
| 1 | Preliminary | General information about the act<br>Definitions of various terms used in the act |
| 2 | Digital and electronic signature | Legal recognition for Digital Signature<br>Authentication of Electronic Records<br>Legal recognition for Electronic Signature |
| 3 | Electronic governance | Legal Recognition of Electronic Records<br>Legal recognition of Electronic Signature<br>Use of Electronic Records and Electronic Signature in Government and its agencies<br>Delivery of Services by Service Provider<br>Retention of Electronic Records<br>Audit of Documents etc. in Electronic form<br>Publication of rules, regulation, etc., in Electronic Gazette<br>Power to Make Rules by Central Government in respect of Electronic Signature<br>Validity of contracts formed through electronic means |
| 4 | Attribution, acknowledgement and despatch of electronic | Attribution of Electronic Records |

| Chapter number | Chapter name | Provision for |
|---|---|---|
| | records | Acknowledgement of Receipt<br>Time and place of despatch and receipt of electronic record |
| 5 | Secure electronic records and secure digital signatures | Secure Electronic Record<br>Secure Electronic Signature<br>Security procedures and Practices |
| 6 | Regulation of certifying authorities | Appointment of Controller and other officers<br>Duties of The Controller<br>Recognition of foreign Certifying Authorities<br>License to issue electronic signature certificates<br>Application for license<br>Renewal of license<br>Procedure for grant or rejection of license<br>Suspension of License<br>Notice of suspension or revocation of license<br>Power to delegate<br>Power to investigate contraventions<br>Access to computers and data<br>Certifying Authority to follow certain procedures<br>Certifying Authority to ensure compliance of the Act, etc.<br>Display of license<br>Surrender of license<br>Disclosure |
| 7 | Electronic signature certificates | Certifying Authority to issue Electronic Signature Certificate<br>Representations upon issuance of Digital Signature Certificate<br>Suspension of Digital Signature Certificate<br>Revocation of Digital Signature Certificate<br>Notice of suspension or revocation |
| 8 | Duties of subscribers | Generating Key Pair<br>Duties of subscriber of Electronic Signature Certificate<br>Acceptance of Digital Signature Certificate<br>Control of Private key |
| 9 | Penalties and adjudication | Penalty and Compensation for damage to computer, computer system, etc.<br>Compensation for failure to protect data<br>Penalty for failure to furnish information, return, etc.<br>Residuary Penalty<br>Power to Adjudicate<br>Factors to be taken into account by the adjudicating officer |
| 10 | The cyber regulations appellate tribunal | Establishment of Cyber Appellate Tribunal<br>Composition of Cyber Appellate Tribunal<br>Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal<br>Term of office, conditions of service etc. of Chairperson and Members |

| Chapter number | Chapter name | Provision for |
|---|---|---|
| | | Salary. allowance and other terms and conditions of service of Chairperson and Member<br>Powers of superintendence, direction, etc.<br>Distribution of Business among Benches<br>Powers of the Chairperson to transfer cases<br>Decision by majority<br>Filling up of vacancies<br>Resignation and removal<br>Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings<br>Staff of the Cyber Appellate Tribunal<br>Appeal to Cyber Regulations Appellate Tribunal<br>Procedure and Powers of the Cyber Appellate Tribunal<br>Right to legal representation<br>Limitation<br>Civil court not to have jurisdiction<br>Appeal to High court<br>Compounding of Contravention<br>Recovery of Penalty or compensation |
| 11 | Offences | Tampering with Computer Source Documents<br>Computer Related Offences<br>Punishment for sending offensive messages through communication service, etc.<br>Punishment for dishonestly receiving stolen computer resource or communication device<br>Punishment for identity theft<br>Punishment for cheating by personation by using computer resource<br>Punishment for violation of privacy<br>Punishment for cyber terrorism<br>Punishment for publishing or transmitting obscene material in electronic form<br>Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form<br>Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form<br>Preservation and Retention of information by intermediaries<br>Power of Controller to give directions<br>Powers to issue directions for interception or monitoring or decryption of any information through any computer resource<br>Power to issue directions for blocking for public access of any information through any computer resource<br>Power to authorise to monitor and collect traffic data or information through any computer resource for Cyber Security<br>Protected system<br>National nodal agency |

| Chapter number | Chapter name | Provision for |
|---|---|---|
| | | Indian Computer Emergency Response Team to serve as national agency for incident response<br>Penalty for misrepresentation<br>Breach of confidentiality and privacy<br>Punishment for Disclosure of information in breach of lawful contract<br>Penalty for publishing electronic Signature Certificate false in certain particulars<br>Publication for fraudulent purpose<br>Act to apply for offence or contraventions committed outside India<br>Confiscation<br>Compensation, penalties or confiscation not to interfere with other punishment<br>Compounding of Offences<br>Offences with three years imprisonment to be cognizable<br>Power to investigate offences |
| 12 | Network service providers not to be liable in certain cases | Exemption from liability of intermediary in certain cases |
| 12 A | Examiner of electronic evidence | Central Government to notify Examiner of Electronic Evidence |
| 13 | Miscellaneous | Power of Police Officer and Other Officers to Enter, Search, etc.<br>Act to have Overriding effect<br>Application of the Act to Electronic cheque and Truncated cheque<br>Chairperson, Members, Officers and Employees to be Public Servants<br>Power to Give Direction<br>Protection of Action taken in Good Faith<br>Modes or methods for encryption<br>Punishment for abetment of offences<br>Punishment for attempt to commit offences<br>Offences by Companies<br>Removal of Difficulties<br>Power of Central Government to make rules<br>Constitution of Advisory Committee<br>Power of Controller to make Regulations<br>Power of State Government to make rules |

- Hence, you find that the ITAA 2008 is very comprehensive defining several provisions as required to deal with cybercrimes. The legal recognition provided to several technology elements helps to clearly define the role of the technology and how it should be preferably consumed.

## 4. Challenges of the ITAA 2008

While the ITAA 2008 addresses several cybercrimes and other digital world issues, it faces several challenges to be effective. Listed following are the few of them.

1. **Rapid change of technology :** The rate of change of technology is quite higher than the rate at which laws can be discussed, presented, approved and enforced. The gap between the technology and what the law prescribes could be challenging to address during prosecution.
2. **Jurisdictional challenges :** The global nature of cybercrime makes it hard to establish the authority over the prosecution. With certain countries, the authority is not yet clear on who prosecutes the cybercriminals.
3. **Investigation :** The traditional approach to crime investigation is challenging when it comes to investigating cybercrimes. The tools used for investigation are quite sophisticated and requires deep understanding of the technology, services, protocols, etc. Sometimes, the learning curve to learn and effectively use these tools is quite steep.
4. **Cases and hearing :** Cybercrime is relatively a new field of crime. The lawyers traditionally are not IT experts. Understanding the complexities of the domain and then relating it to the law for proper prosecution could be quite challenging.

## 5. ITAA 2008 and Digital Signatures

ITAA 2008 gave legal recognition to digital signatures. Here are some provisions defined in the act with respect to digital or electronic signature in the Chapter 2 of ITAA 2008.

### a. Authentication of Electronic Records

1. Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
2. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.
3. Any person by the use of a public key of the subscriber can verify the electronic record.
4. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

### b. Electronic Signature

1. Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-
   a. is considered reliable; and
   b. may be specified in the Second Schedule
2. For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-
   a. The signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;
   b. The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
   c. Any alteration to the electronic signature made after affixing such signature is detectable
   d. Any alteration to the information made after its authentication by electronic signature is detectable; and
   e. It fulfils such other conditions which may be prescribed.

## 6.7.5(B) The Global Perspective

- As you understand, cybercrime honours no boundaries – geographical or legislative. It has become a global problem like world hunger, poverty and global warming.
- United Nations (UN), which is an intergovernmental organisation established in 1945 to promote international co-operation, acknowledged cybercrime as a global problem.

### 1. Global Cybersecurity Index (GCI)

- The United Nations (UN) International Telecommunications Union (ITU) announced the launch of the Global Cybersecurity Index (GCI) to measure the status of cybersecurity worldwide.
- Its aim in the short term was to close security gaps, particularly in developing countries, while in the long it was to drive the efforts in the adoption of cybersecurity on a global scale.

| Country | GCI Score |
|---|---|
| Singapore | 0.92 |
| United states | 0.91 |
| Malaysia | 0.89 |
| Oman | 0.87 |
| Estonia | 0.84 |
| Mauritius | 0.82 |
| Australia | 0.82 |
| Georgia | 0.81 |
| France | 0.81 |
| Canada | 0.81 |

- As per the Global Cybersecurity Index 2017, the Member Countries were classified into three categories by their GCI score:
  - **Initiating stage :** These are member countries that have recently started to make commitments in cybersecurity
  - **Maturing stage :** These are member countries that have developed complex commitments and engage in cybersecurity programmes and initiatives
  - **Leading stage :** These are member countries that have demonstrate high commitment to cybersecurity programs.
- The top 10 Member Countries with respect to GCI Score are as listed here. Higher the score, the more committed the cybersecurity program of the Member Country.
- As you see form the list, Singapore has the most committed cybersecurity program. It has a long history of cybersecurity initiatives. It launched its first cybersecurity master plan back in 2005.

- The Cyber Security Agency of Singapore was created in 2015 as a dedicated entity to oversee cybersecurity and the country issued a comprehensive strategy in 2016.

**Member Countries at the Initiating Stage**

| | | |
|---|---|---|
| Afghanistan | Guatemala | Palestine (State of) |
| Andorra | Guinea | Papua New Guinea |
| Angola | Guinea-Bissau | Saint Kitts and Nevis |
| Antigua and Barbuda | Guyana | Saint Lucia |
| Armenia | Haiti | Saint Vincent & the Grenadines |
| Bahamas | Honduras | Samoa |
| Barbados | Iraq | San Marino |
| Belize | Jordan | Sao Tome and Principe |
| Benin | Kiribati | Seychelles |
| Bhutan | Kuwait | Sierra Leone |
| Bolivia (Plurinational State of) | Kyrgyzstan | Solomon Islands |
| Bosnia & Herzegovina | Lebanon | Somalia |
| Burkina Faso | Lesotho | South Sudan |
| Burundi | Liberia | Sudan |
| Cambodia | Libya | Suriname |
| Cape Verde | Liechtenstein | Swaziland |
| Central African Republic. | Madagascar | Syrian Arab Republic |
| Chad | Malawi | Tajikistan |
| Comoros | Maldives | Timor-Leste |
| Congo | Mali | Togo |
| Cuba | Marshall Islands | Tonga |
| Democratic Republic. of the Congo | Mauritania | Trinidad and Tobago |
| Djibouti | Micronesia | Turkmenistan |
| Dominica | Monaco | Tuvalu |
| Dominican Republic | Mongolia | Uzbekistan |
| El Salvador | Mozambique | Vanuatu |
| Equatorial Guinea | Myanmar | Vatican |
| Eritrea | Namibia | Viet Nam |
| Ethiopia | Nauru | Yemen |
| Fiji | Nepal (Republic of) | Zambia |
| Gabon | Nicaragua | Zimbabwe |
| Gambia | Niger | |
| Grenada | Palau | |

**Member Countries at the Leading stage**

| | | |
|---|---|---|
| Australia | Korea | Russian Federation |
| Canada | Malaysia | Singapore |
| Egypt | Mauritius | Spain |
| Estonia | Netherlands | Sweden |
| Finland | New Zealand | Switzerland |
| France | Norway | United Kingdom |
| Georgia | Oman | United States |
| Japan | | |

| Member Countries at the Maturing stage | | |
|---|---|---|
| Albania | Ghana | Peru |
| Algeria | Greece | Philippines |
| Argentina | Hungary | Poland |
| Austria | Iceland | Portugal |
| Azerbaijan | India | Qatar |
| Bahrain | Indonesia | Romania |
| Bangladesh | Iran (Islamic Republic of) | Rwanda |
| Belarus | Ireland | Saudi Arabia |
| Belgium | Israel | Senegal |
| Botswana | Italy | Serbia |
| Brazil | Jamaica | Slovakia |
| Brunei Darussalam | Kazakhstan | Slovenia |
| Bulgaria | Kenya | South Africa |
| Cameroon | Laos | Sri Lanka |
| Chile | Latvia | Tanzania |
| China | Lithuania | Thailand |
| Colombia | Luxembourg | The Former Yugoslav Rep. of Macedonia |
| Costa Rica | Malta | Tunisia |
| Côte d'Ivoire | Mexico | Turkey |
| Croatia | Moldova | Uganda |
| Cyprus | Montenegro | Ukraine |
| Czech Republic | Morocco | United Arab Emirates |
| Dem. People's Rep. of Korea | Nigeria | Uruguay |
| Denmark | Pakistan | Venezuela |
| Ecuador | Panama | |
| Germany | Paraguay | |

## 2. Benefits of Global Co-Operation to Fight against Cybercrime

- As you understand, cybercrime is not specific to a particular country or region. It affects almost all the countries and their nationals. The countries are now coming together to provide co-operation at the global level to fight cybercrime.
- Some of the benefits of global co-operation are as following:

**1. Sharing intelligence**

This is perhaps the most critical area where co-operation is required. Previously, countries did not use to disclose the investigatory details about the cybercrimes that it was hit from. Because of this lack of information, other countries could not learn from the affected country. In-turn, all such countries would get affected by exactly the same cybercrime. With global co-operation in place, countries can share the intelligence information about the cybercrimes that it knows about and can then mutually benefit by preventing cybercrimes to occur by utilizing the intelligence information.

**2. Stronger defence**

The cooperating countries can benefit from technology and skills available across the countries to fight cybercrime. Together, these bonds create a strong defence mechanism and makes it easier to fight the global problem of cybercrime. The skills or technology not available to any country will then no more be a

3. **No offense**

The cooperating countries also pledge to not promote any cybercrimes from itself (on its land) and provide support and assistance in curbing (destroying) any such attempts. If the countries help each other to restrict the cybercrime right at its origin, then the cross-border legislation need not be required.

4. **Capacity building**

Technology and policy considerations can dominate cybersecurity discussions, overlooking the fundamental human element at its core. Capacity building addresses the challenges related to advancing cybersecurity practice and awareness-raising among government entities, citizens, businesses and other organisations which is crucial to enabling a country's digital economy. Such programs help various countries to build upon each other's experience and expertise.

5. **Collective action**

There might be some countries that repeatedly attempt to disrupt the digital economy. The cooperating countries can then fight collectively against such countries to limit its powers or to threat it against supporting cybercrimes.

## 3. Adaptive Jurisdiction Principles

- World Bank and United Nations 2017, in their collateral named "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies", state that "Faced with the increasingly limited applicability of the traditional notion of jurisdiction to cybercrime, a series of adaptations have been developed".
- These adaptations are useful when looking at prosecuting cybercriminals from global perspective. Let's review some of these global principles that help in prosecuting cybercriminals irrespective of where they are located.

**Table 6.7.5**

| Sr. No. | Adaptive Principle | Notion |
|---|---|---|
| 1. | Principle of Territoriality | A cybercrime "initiated" in the territory of one state but launched "at" another state, or made to occur "in", another state's territory gives the affected state the power of jurisdiction.<br>Cyberspace is deemed a territory like air, land and sea. |
| 2. | Principle of (Active) Nationality | Nationals of a state are obliged to comply with that state's domestic law even when they are outside of its territory. |
| 3. | Principle of Passive Nationality | If the national is the victim rather than the attacker, then the state has jurisdiction over the crime by which its national is victimized |
| 4. | Protective Principle | When a cybercrime affects not just a national of the state, but a national security interest, this principle is applied. |
| 5. | Principle of Universal Jurisdiction | The principle of universal jurisdiction applies to specific crimes but requires international or universal acceptance and cooperation. Piracy is regarded as one of the first international crimes. |

## 6.8 Cyberstalking

SPPU – May 19

**Q. What is cyberstalking? (May 19, 4 Marks)**

✍ ***Definition :*** *Cyberstalking is the use of internet or other electronic means to stalk (or harass) an individual, group or organisation.*

- Stalking (or physical harassment) existed even before the rise of the internet and is also existent now. Cyberstalking has just evolved in today's digital age where the physical form has taken an electronic form. Nothing else changes.
- Cyberstalking is also called as cyberbullying when the target is a minor (anyone aged below 18 years).

### 6.8.1 Cyberstalking Harassments

While cyberstalking can lead to any form of harassment, following are some of the common forms of harassments.

1. Posting comments on social media intended to cause distress to the victim.
2. Repeatedly sending unwanted messages that are hateful, obscene, derogatory, defaming, etc.
3. Impersonating (faking as the victim) and posting offensive content assuming the victim's profile.
4. Hacking or taking over the victim's computer or email accounts.
5. Signing up the victim's email or phone number for spam, porn sites or questionable offers.
6. Posting victim's email or phone number on the internet and inviting people to use it for illegitimate purpose.
7. Following the victim into chat rooms, discussion boards, group chats, or other forms of online presence.
8. Creating sexually explicit images of the victim and posting them on the internet.
9. Forcing the victim to perform illegal or harmful actions.
10. Convincing the victim to meet offline.

**Comparison between Online (Cyberstalking) and Offline (Physical) Stalking**

- As I told you earlier, stalking always existed. It is just that it has evolved in the digital age to use technology to stalk. You could, at a broad level, classify stalking into online and offline.

**Table 6.8.1**

| Sr. No. | Online Stalking (Cyberstalking) | Offline Stalking (Physical Stalking) |
|---|---|---|
| 1. | Target is usually randomly selected. | Target is usually known. |
| 2. | Target could be anywhere in the world. | Target and stalker are in the same geography. |
| 3. | Stalker's identity is usually fake. | Stalker could be visually seen and reported. |
| 4. | Multiple ways of harming or stressing the target. | Forms of harassment are limited to physical assaults only. |
| 5. | Difficult to locate and prosecute the stalker. | Comparatively easier to find and punish the stalker. |
| 6. | Difficult to prove stalking actions. | Comparatively easier to prove stalking actions. |

## 6.8.2 Types of Stalkers

There could be several types of stalkers. Some of them are listed here. These stalkers could be either online or offline stalkers.

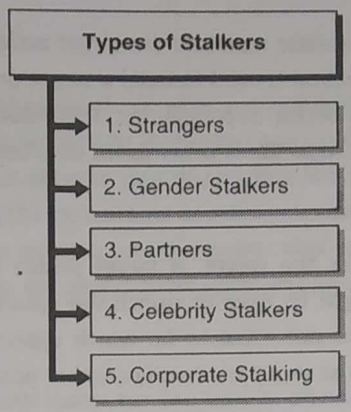



**Fig. 6.8.1**

### 1. Strangers

These are stalkers who randomly choose their targets. The target chosen is mostly unknown.

### 2. Gender stalkers

These are stalkers who target a particular gender – male, female or trans. More than 90% of the stalking cases are targeted towards females making them completely go offline in fear.

### 3. Partners

These stalkers were previously in a relationship with the target. Once the relationship loses value, the partner chooses to harass the previous partner in revenge, hate or anger.

### 4. Celebrity stalkers

These stalkers only harass celebrities or people who have a huge fan following or public presence such as sports person, actress, politicians or anyone else whose reputation is very prone to such behaviour.

### 5. Corporate stalking

This is usually done by a company to an individual. The company may threaten the individual to gain anything financial or just intend to terrify the target to post good reviews about the company's products or avoid posting negative comments about the company's product or services.

## 6.8.3 How cyberstalking works ?

Typically, cyberstalking works through 4 stages.

### 1. Identify target

At this stage, the cyberstalker searches for a target. If she has a pre-determined group to choose the target from (like celebrity, based on gender, based on company, etc.) then the search is carried out within this group.

Searches are carried out through search engines, randomly checking out social media profiles or following comments or likes on popular music or video playing sites. Searches could also be made at the online forums, chat rooms, news groups or any other online presence opportunity.

2. **Monitor target activities**

Once a target is identified, the cyberstalker monitors the target activities. What the target does, when, where, with whom, how, etc. and this information is used to build a target profile. The cyberstalker collects as much as information that she can via various online opportunities. This information could also include email address, home address, phone number, social media IDs or other forms of private and sensitive information.

3. **Build target profile**

From the information collected about the target, a target profile is created. The cyberstalker has enough information about the target that might be used to launch the cyberstalking activity. Sometimes, at the target profile building stage, the target does not seem to be worth cyberstalking. The cyberstalker then drops the current target and starts all over again at step 1 to identify another potential and more promising target.

4. **Cyberstalk**

The cyberstalker can choose the various harassment actions based on the target profile. It may begin with anonymous emailing and gradually go up to more severe harassments and assaults.

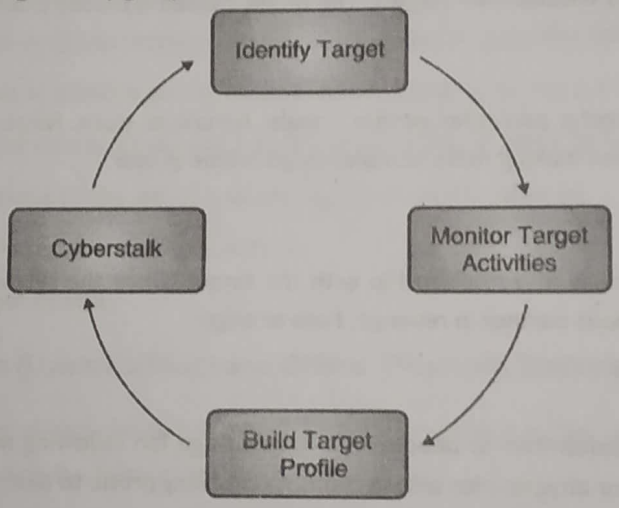



**Fig. 6.8.2**

## 6.8.4 How to safeguard yourself from stalking ?

SPPU – May 19

**Q. How to identify and detect cyberstalking ?** **(May 19, 4 Marks)**

Here are some of the points that you might want to consider remaining careful about not being an easy target and safeguard yourself from cyberstalking.

1. **Watch out for your privacy settings**

Are your social media profile settings too open? Can anyone and everyone see your photos, messages, locations, etc.? If yes, then edit the settings to allow only people whom you exclusively know and trust to view your profile details and posts.

2. **Be wary about the people you meet online**

You might get friend requests, email messages, likes, comments, etc. from unknowns. Be wary about replying or accepting their requests. This might be your first move to show that you are an easy target. Be extremely cautious with what you do online.

3. **Status updates**

Do you provide minute-by-minute status update of what you are doing, with whom you are and where? This is very sensitive data about yourself that can be used to locate you and build a target profile about yourself. The stalker, by following you just for a week or so, would know your day routine and places you go. She can also determine how good or bad you are financially by knowing the restaurants or cafes you visit or the frequency of shopping or entertainment activities that you engage into. These are also sensitive points that can be used to build your personality profile and could motivate the stalker to stalk you. Be careful about what you provide updates on and to whom.

4. **Protect your systems**

You should protect your systems (both computer and mobile phones) and online accounts using strong passwords and multi-factor authentication wherever possible. Cyberstalkers tend to hijack your systems and online accounts and use them to create fake identities to stalk others. You should not be the person to be caught for any stalking activity done by a cyberstalker.

5. **Inform local police**

If you are being cyberstalked, then inform your local police immediately. Cyberstalking is just a digital way of stalking. There are several provisions under the law to protect yourself from both physical stalking as well as cyberstalking. Keep all the messages, emails or any other forms of harassment that you went under as evidences to report.

### 6.8.5 Provisions in the Indian Jurisdiction for Stalking

For your reference, Table 6.8.2 shows some of the provisions in the Indian Jurisdiction for stalking.

**Table 6.8.2**

| Sr. No. | IPC Sections | Provisions for Offenses |
|---|---|---|
| 1. | 354D | Stalking (both online and offline are covered) |
| 2. | 499 | Defamation |
| 3. | 507 | Criminal intimidation by an anonymous communication |
| 4. | 509 | Word, gesture or act intended to insult the modesty of a woman |

## 6.9 Phases of Cyber Forensics

SPPU - May 19

Q. What are different phases of cyber forensics ? Explain with suitable diagram. **(May 19, 8 Marks)**

The goal of performing forensics is to gain a better understanding of an event of interest by finding and analysing the facts related to that event. At a high level, there are four phases of cyber forensics. They are as shown in Fig. 6.9.1.

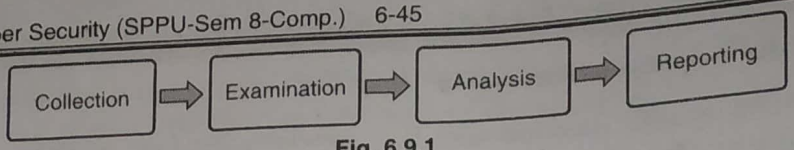



Fig. 6.9.1

1. **Phase 1 : Evidence Collection**

   During collection, data related to a specific event is identified, labeled, recorded, and collected, and its integrity is preserved. The sources of data could be logs, memory dumps, process tables, users logged in, hard disk state, system photograph, etc.

2. **Phase 2 : Examination**

   In the examination phase, various forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes.

3. **Phase 3 : Analysis**

   The analysis phase involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

4. **Phase 4 : Reporting**

   The final phase involves reporting the results of the analysis, which may include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

## Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

### Privacy on Web

**Q. 1** Adam is reading about privacy and is concerned about his privacy on web. He decides to educate his friends and family about privacy and its importance. What would he likely explain? **[4 Marks]**

**Q. 2** Write a short note on Personally Identifiable Information (PII). **[4 Marks]**

**Q. 3** An organisation is building a privacy program for its users. You are a privacy consultant that the company hires. On day 1 of the privacy orientation, you want the people in the organisation to understand the core privacy principles that lay the foundation of any privacy program. What are the principles that you would likely explain? **[8 Marks]**

**Q. 4** Draw a Venn diagram and show the relation between security and privacy. **[4 Marks]**

**Q. 5** List the various ways using which you can protect your privacy on the web. **[6 Marks]**

**Q. 6** It is recommended to use privacy honouring services and products. Why? **[4 Marks]**

**Q. 7** Which Privacy Protection Software could you use and how do they protect your privacy? **[8 Marks]**

| | | |
|---|---|---|
| Q. 8 | What is the role of Virtual Private Network (VPN) in privacy? | [5 Marks] |
| Q. 9 | Private Mode of Browsing makes you anonymous on the internet. Comment. | [4 Marks] |
| Q. 10 | Describe the PII confidentiality impact levels. | [8 Marks] |
| Q. 11 | Explain the factors for determining PII confidentiality impact levels. | [8 Marks] |
| Q. 12 | As on organisation, what should you do to appropriately handle PII? | [6 Marks] |
| Q. 13 | Compare Security and Privacy. | [4 Marks] |

## Cybercrime

| | | |
|---|---|---|
| Q. 14 | Define the term cybercrime. List a few examples of major cybercrimes reported around the world | [4 Marks] |
| Q. 15 | Differentiate between information security and cybersecurity. | [6 Marks] |
| Q. 16 | Describe the various categories of cybercrimes and give examples for each. | [8 Marks] |
| Q. 17 | Draw a classification chart for cybercrimes and explain. | [8 Marks] |

## The Legal Perspectives of Cybercrimes

| | | |
|---|---|---|
| Q. 18 | Write a short note explaining the cybercrime scenario in India. | [4 Marks] |
| Q. 19 | List the objectives / goals of the ITAA 20008. | [8 Marks] |
| Q. 20 | Describe the various challenges of the ITAA 2008. | [8 Marks] |
| Q. 21 | Describe the ITAA 2008 with respect to Digital Signatures. | [6 Marks] |
| Q. 22 | Write a short note on Global Cybersecurity Index (GCI). | [4 Marks] |
| Q. 23 | What are the benefits of global co-operation to fight against cybercrime? | [8 Marks] |
| Q. 24 | Describe Adaptive Jurisdiction Principles. | [8 Marks] |

## Cyberstalking

| | | |
|---|---|---|
| Q. 25 | What is cyberstalking? List the common forms of cyberstalking harassments. | [8 Marks] |
| Q. 26 | Provide a comparison between online (cyberstalking) and offline (physical) stalking. | [8 Marks] |
| Q. 27 | Describe the types of stalkers. | [8 Marks] |
| Q. 28 | Explain the steps involved in cyberstalking. | [8 Marks] |
| Q. 29 | Describe the ways in which you can safeguard yourself from stalking. | [8 Marks] |
| Q. 30 | What is cyberstalking? List the provisions in the Indian Jurisdiction for stalking. | [6 Marks] |

❑❑❑