**Chapter 1:**

# Introduction to Information Technology and the Law

# 1.1. Unpacking terminologies: Internet Law, Computer Law or Information Technology Law?

- **What Is Cyber Law?**
- Cyber-law is any law that applies to the internet and internet-related technologies.
- Cyber-law is one of the newest areas of the legal system. This is because internet technology develops at such a rapid pace.
- Cyber-law provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet.
- Cyber Law has also been referred to as the “law of the internet.”

# Cont…

- **Cyber law**, also called information technology law, or Internet law, pertains to laws involving technology related to the Internet and includes computers and networks.
- **Cyber law** is a newer area of the legal system. It pulls from many areas of traditional law and provides legal protection for individuals using the Internet.
- This type of law is wide reaching, encompassing cyber-bullying and cyber stalking, access to the Internet, intellectual property infringement, consumer protection, financial crimes, freedom of expression, online privacy, jurisdiction, freedom of religion,

# Cont...

- Cyber security is one of the fastest-growing challenges across the globe and is becoming increasingly important.
- Furthermore, cyber-security has enormous implications for government security, economic prosperity, and public safety.
- **Cyber laws** have been enacted by every nation.
- In the **United States**, the federal government and individual states are improving cyber-security through legislation, better security measures and security practices, increasing fines for computer crimes, and addressing the most serious cyber risks to critical

# Cont...

- **Cyber Law Terms and Laws**
- There are three main terms that people need to know related to cyber law.:

1) **Information Technology Law.** These laws refer to digital information. It describes how this information is gathered, stored, and transmitted.
2) **Cyber Law/Internet Law.** These laws cover usage of the internet. This is a newer legal area. Many laws can be undefined and vague.
3) **Computer Law.** This covers a large legal area. It includes both the internet and laws related to computer IP.

## Cyber Law Trends

- Cyber-law is increasing in importance every single year. This is because cybercrime is increasing. To fight these crimes, there have been recent trends in cyber law. These trends include the following:
- New and more stringent regulations.
- Reinforcing current laws.
- Increased awareness of privacy issues.
- Cloud computing.
- How virtual currency might be vulnerable to crime.
- Usage of data analytics.
- Creating awareness of these issues will be a primary focus of governments and cyber law agencies in the very near future. India, for instance, funded cyber trend research projects in both 2013 and 2014. In addition, India held an international conference related to cyber law in 2014. This was meant to promote awareness and international cooperation.

# Cyber Security Strategies

- Besides understanding cyber law, organizations must build cybersecurity strategies. Cybersecurity strategies must cover the following areas:
- **Ecosystem.** A strong ecosystem helps prevent cybercrime. Your ecosystem includes three areas—automation, interoperability, and authentication. A strong system can prevent cyberattacks like malware, attrition, hacking, insider attacks, and equipment theft.

- **Framework.** An assurance framework is a strategy for complying with security standards. This allows updates to infrastructure. It also allows governments and businesses to work together in what's known as "enabling and endorsing'.
- **Open Standards.** Open standards lead to improved security against cybercrime. They allow business and individuals to easily use proper security. Open standards can also improve economic growth and new technology development.
- **Strengthening Regulation.** This speaks directly to cyber law. Governments can work to improve this legal area. They can also found agencies to handle cyber law and cybercrime. Other parts of this strategy include promoting cyber security, proving education and training, working with private and public organizations, and implementing new security technology.

## 1.2. INFORMATION SOCIETY AND REGULATION .

- The study of information and communications technology (“ICT”) as an area of law is relatively new and follows the development of the Internet and World Wide Web (“WWW”) for general use in the 1980s.
- In the beginning, ICT-related law was merely treated as an extension of existing areas of law. Hence, for example, the law on intellectual property (“IP”) had to evolve - copyright law, in particular, had to rebalance the interests of copyright owners, users and technology providers - because the way digitised materials

# Cont...

- A key issue in the information age is the use and abuse of information by economic and political actors as a means of control.
- It is possible, for instance, for those who provide the gateway to ICT the information service providers (ISPs) to exert significant and not necessarily consistent impediments by blocking access to certain material or by allowing content providers to pay a premium for a priority service.
- Such a practice would inevitably favour commercial providers over others. Although prejudicial behaviour against smaller content providers and consumers could, in principle, be dealt with by competition law, in both the US and EU, this led to calls to ensure **net neutrality**; the principle that 'internet service

# Cont…

- **Net neutrality** has been described as ‘a deceptively simple phrase hiding a multitude of meanings’.
- Originally the term arguably referred to a design principle that the network was itself ‘neutral’ and so it made no difference who was the provider, the user, what content was being made available and so on.
- Any departure from this general principle such as ISPs providing preferential rates or services for specific users or types of content has the propensity to be detrimental to more general access to the internet. ‘Open access’ and ‘net

# Cont...

- '**backward-looking net neutrality**' which merely seeks to ensure that users are not disadvantaged as a result of a prejudicial ISP practice and
- '**forward-looking' net neutrality** which permits a higher priced service with associated higher quality as long as it is offered on the same, fair, reasonable and non-discriminatory basis to all users.
- Overall net neutrality is likely to be difficult to achieve in practice without a more uniform approach to content

# Cont...

- through time competing policy interests (such as the development of e-commerce and free flow of information) required accommodation under the law, even as it was clear that IP protection had to be strengthened to deal with issues arising from peer-to-peer (“P2P”) file-sharing and online streaming and time-shifting technologies.
- The regulation of technology is the setting of parameters for the existence and the operation of such technology by law. The objective is mainly to counter the possible negative effects of such technology but at the same time allow it to thrive in ways that benefit society as a whole.

# Cont…

- There are many different forms of regulations to meet different needs. Government regulation through laws and subsidiary rules such as codes of practice and directives form the first layer. Administrative processes and decision-making are increasingly used in various jurisdiction.
-

# Cont…

- Generally, once information is available online there is, on the one hand, the state seeking to use data, often generated by private communications, as a way in which to enhance law and order recently under the guise of anti-terrorism measures.
- The initial helplessness of the state vis-à-vis activities on the internet has given way to the recognition of its unique potential for keeping a tab on the connections, whereabouts, and moves of everyone – on the premise that everyone harbours the risk of delinquencies.
- On the other hand, there are the large multinational companies scrambling for control over consumers through pinning down their preferences, shopping habits, lifestyle choices, and general web behavior.
- The surveillance interests of these commercial actors sometimes overlap with those of consumers, but this is by no means always the case, as is illustrated, for example, by the debate surrounding “cookies’.

# Cont...

- The threat and, to some extent, the reality of a surveillance society driven by both private and public actors has prompted a heightened interest by civil society in data protection and privacy.
- Thus a large chunk of IT law can be understood as the conflict of the legitimate boundaries of surveillance with the legitimate expectation of a private life away from the prying eyes of government or business. How these legal boundaries have been shifting in recent years provides a wider commentary about our society in general.

# Cont...

- Similarly, the abundance of information to which the regulator has access will not necessarily allow for greater regulatory efficiency.
- First, the instances in which a huge amount of information
  has been accidentally lost or made public by public servants show that the informational abundance also significantly multiplies the risk for the management of that data, with breaches of confidentiality and data protection and security threats looming large in the background.
- Second, by the same token, the retention of information as part of a regulatory agenda must be coupled with intelligent systems that allow for the efficient use of the information; otherwise, it is worthless. For example, there is evidence that the growing DNA database in the UK has not livedup to

# 1.3. Regulating IT or regulation by IT?

- The internet also provokes fundamental questions about regulation: generally, what are the appropriate forms of regulation for online activities, how much regulation is required, and who should regulate? Regulation of and on the internet has been considered and examined in many different situations.
- **regulation** :- It can refer to a specific set of commands devised for a particular purpose. More broadly, it can cover all government action designed to respond to a particular type of behaviour or activity.
- also, it can refer to any form of influence that affects behaviour, whether or not this emanates from the state or from other sources, such as the market.
- The last of these definitions is considered here, in the context of the interrelationship of various factors,

# Cont...

- Importantly, the state cannot only use ‘law’ (direct regulation) to achieve a certain desired result, but can also influence and change the other three factors via regulation.
- Here, the regulation is indirect and often invisible to the subject, because it is channelled through the non-legal modalities.
- As an illustration, Lessig uses the example of the regulation of smoking and the consumption of cigarettes: the law may **ban** smoking (that is, the **direct regulation** of behaviour); it may tax cigarettes (that is, market regulation); it may provide a public education programme (that is, an attempt to regulate **social norms**); or it may control the amount of nicotine in cigarettes (that is, changing the ‘**architecture’ of cigarettes**).

# Cont...

- Many believe that cyberspace simply cannot be regulated. Behavior in cyberspace . . . is beyond government's reach. The anonymity and multi jurisdictionality of cyberspace makes control by government in cyberspace impossible.
- The nature of the space makes behavior there unregulable.
- This belief about cyberspace is wrong, but wrong in an interesting way.
- It assumes either that the nature of cyberspace is fixed that its architecture, and the control it enables, cannot be changed – or that government cannot take steps to change

# Cont…

- the following terminology were developed, these are ‘control systems’ (that is, methods of controlling or modifying behaviour):
- hierarchical control (Lessig’s ‘law’);
- competition-based control (Lessig’s ‘market’);
- community-based control (Lessig’s ‘norms’); and
- design-based control (Lessig’s ‘architecture’).
- However, Scott and Murray elaborate on these ‘control systems’ by identifying three stages in the regulatory process in respect of each of the above four modalities:
- (1)*Standard setting* – that is, what is the source and content of the restraint?
- (2)*Information gathering* – that is, how does the restraint interact with its subject? how is its compliance monitored?
- (3)*Behaviour modification* – that is, how is the restraint

# Cont...

- Another way of viewing the control systems is to think of them in terms of regulatory strategies variously involving legal authority, the deployment of wealth, the use of markets, the provision of information, direct action, or the conferment of rights.
- 1) criminal and admnistrative law :command and control.
- 2) self regulation and enforced self regulation.
- 3) co-regulation.
- 4) laws enacted has to look forward, backward and sideways.

# 1.4. Internet governance: notions and institutions

- **Internet Governance** :- refers to the rules, policies, standards and practices that cordinate and shape global cyber space.
- Many information policy experts emphasize that "Internet governance" is not the product of an institutional hierarchy, but rather, it emerges from the decentralized, bottom-up coordination of tens of thousands of mostly private-sector entities across the globe.
- States control Internet-related policies within their own borders, such as passing laws prohibiting online gambling, protecting intellectual property, or blocking/filtering access to certain content.
- ICANN Established in 1998 under contract to the U.S. Department of Commerce, the Internet Corporation for Assigned Names and Numbers is a private nonprofit headquartered in California that, among other things, manages the global Domain Name System.
- Often referred to as the Internet's "phone book," the DNS is a worldwide network of databases mapping domain names (samplesite.com) to IP addresses (7.42.21.42) so that users can send and receive information from any of the billions of web-connected devices.

# Chapter Two

## Crime in Cyberspace: Cybercrimes

### 2.1.1. Understanding cybercrimes

- Areas that are related to cyber law include cybercrime and cyber-security.
- With the right cyber-security, businesses and people can protect themselves from cybercrime.
- Cyber-security looks to address weaknesses in computers and networks.
- Cyber-security policy is focused on providing guidance to anyone that might be vulnerable to cybercrime. This includes businesses, individuals, and even the government. Many countries are looking for ways to promote cyber-security and prevent cybercrime. For instance, the PROCLAMATION No. 958/2016 Computer Crime Proclamation.

# Cont…

- Information is another important way to improve cyber-security. Businesses, for example, can improve cyber-security by implementing the following practices:
- Offering training programs to employees.
- Hiring employees who are certified in cyber-security.
- Being aware of new security threats.
- Cybercrimes can be committed against governments, property, and people.

# Cont...

- **Cybercrimes** are relatively new criminal offenses that are the result of recent advances in computer technology and the Internet.
- While advances in technology have benefited society, they have also created new opportunities for cybercriminals who use these innovations to cause harm to others.
- As technology has developed, so have new crimes that rely on that technology. Many of these crimes, such as computer hacking or the introduction of spyware, would not exist if it were not for computer technology. And as the computer technology becomes more advanced, so do the illegal activities.
- New criminal offenses are constantly being developed in the realm of cyberspace.

# Cont...

- Not only have new crimes emerged but some more traditional crimes have also been transformed for the new medium. Traditional crimes such as fraud, theft, stalking, and bullying, which have been part of our society for years, now occur in new ways. Illegal drugs and child pornography, both of which existed before the development of network technology, are now sold via the Internet.
- Financial transactions (e.g., misuse of credit cards) and money-laundering offenses have evolved into new forms of crime. In some cases, the Internet has made commission of these crimes much simpler.

# Cont...

- These new crimes are occurring because they are comparatively easy to commit. Cyber criminals can easily hack into computer systems anywhere in the world with little cost and little risk of being caught. They can alter records and information, steal money, or steal the identities of innocent victims.
- They can offer goods and products for sale that cannot be purchased elsewhere. Messages can be posted with the intent of harming a person's reputation.
- The software needed to carry out all of these malicious
attacks can be purchased online for a small fee

# Cont…

## 2.1.2Definition of Cybercrime

- "**Cybercrime"** is very a broad term that is often used to refer to different concepts. Consequently, there is some debate as to the exact meaning of the term. For the purposes of this course, cybercrime can be thought of as **crime that involves computers and computer networks.**
- **Generally**, it refers to acts that involve criminal uses of the Internet or other networked systems to cause harm to others or some form of a disturbance.
- It can include any criminal activity—not only on computers, networks, or the Internet but also on **mobile phones** or other **personal devices—that is intended to cause harm to others.**
- These are illegal activities that are conducted through global electronic networks.
- In short, the term "**cybercrime"** refers to methods by which computers or other electronic devices are used to carry out criminal activity and cause harm to others.

# Cont…

- A **cybercrime** could be the **misuse** of computer systems or networks to carry out criminal offenses by unauthorized access to a computer system, illegal interception or alteration of data, or misuse of electronic devices.
- Other examples **are the theft of intellectual property**, that is, theft of a **patent, trade secret, or anything protected by copyright laws**.
- It can also include attacks against computers to deliberately disrupt processing or acts of espionage to make unauthorized copies of classified data.
- It includes downloading illegal music, stealing money from bank accounts, creating viruses, posting confidential business information on the Internet, committing identity theft or fraud, trafficking in child porn, money laundering and counterfeiting, and committing denial-of-service attacks.

# Cont…

- Other examples of **cybercrimes** include computer viruses; malware; fake emails or websites; identity theft; cyber-bullying, stalking, or harassment; hacking; online scams (e.g., Nigerian scams); credit card theft; or phishing.
- The term "**cybercrime**" often encompasses other, more specific categories of illegal behavior such as computer-assisted crimes and computer-focused crimes.
- Other terms that refer to the same acts are computer crimes, **digital crimes**, **techno-crimes,** and **high-tech crimes.** These terms all refer to criminal activities that are committed by the use of emerging digital, network, or computer technologies, such as the Internet.

# Cont…

- In the **European Union**, the Council of Europe provides a more complete **definition of cybercrime**. It describes **cybercrime** as "**applied to three categories** of criminal activities.
- The **first covers** traditional forms of crime such as **fraud or forgery,** though in a cybercrime context relates specifically to crimes committed over electronic communication networks and information systems.
- **The second concerns the publication of illegal content over electronic media** (i.e., child sexual abuse material or incitement to racial hatred).
- **The third includes crimes unique to electronic networks, that is, attacks against information systems, denial of service and hacking.".**

# 2.1.3.Key Terms Related to Cyber Crime

- **Cybercriminal:-** are those who use mobile phones, laptop computers, or network servers to commit a cybercrime. Although a criminal does not need special computer skills to commit a computer crime, he or she usually needs to have more than a basic level of computer knowledge to commit a computer crime.
- **Drop Account:-**is an account that is opened by a criminal as a way to receive profits from his or her criminal activity. Most times, the accounts are opened with a false identity so they are difficult for law enforcement to track.
- **Advanced Persistent Threats:-** (APTs) are attacks on computer systems that involve multiple techniques or approaches. In some instances, cybercriminals will use multiple techniques or methods in their attacks rather than a single method to ensure a particular result.

# Cont...

- **Computer Forensics:-** refers to the examination of computer components and their contents, including hard drives, external drives, compact disks, and printers, to investigate allegations of possible crimes and collect evidence of those crimes. Sub-disciplines of computer forensics include malware forensics and mobile device forensics. These sub-disciplines are focused on collecting evidence of wrongdoing by use of malware and mobile devices .

- **Malware:-** which is short for “malicious software,” is a general term for software programs that affect how a computer functions. Most malware is spread through an email attachment. When the receiver opens the attachment, the malware installs itself onto the victim’s computer.
- **Crimeware:-**refers to the software that is used to commit acts of cybercrime. The term encompasses a multitude of different malicious, or potentially malicious, software products. Examples of crimeware are bots and Trojan horses.

# Cont…

- **Botnet:-** One form of malware is a botnet, or bot network. These are comprised of many computers that have been infected with malware that allows them to be controlled remotely through commands sent through the Internet, possibly from thousands of miles away.
- **Packet Sniffers:-** are small pieces of malware that are attached to computer systems and have the capability of “sniffing out” or inspecting data that is being sent along a computer network. If an important piece of data is detected, such as a password, that information is recorded and sent to the criminal.

# Cont…

- **Personally Identifiable Information:-** refers to any information that can be used to identify an individual. If stolen, a criminal can use this information to steal that person's identity or cause other harm to them. Examples of PIIs are a person's full name, Social Security number (or other
federal identification number, such as a passport number or driver's license number), birth date and place of birth, credit card account numbers, and
bank account information.

# Cont…

- **Cyber-terrorism:-**is the use of the Internet by terrorist groups who are attempting to affect a nation’s policies. As defined by the Federal Emergency Management Agency, cyber-terrorism is the “unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.”.
- **Zero-Day Exploit:-** occurs when a computer hacker is able to uncover a weakness in a software program that is unknown to the owner or business and has not been exploited by a cyber-criminal.

# Cont…

- **Exploit Kits:-**are malicious programs that allow criminals to identify vulnerabilities in computer systems and then spread malware to those computers.
- **Script Kiddies:-**Hackers who do not possess the technical skills to carry out complicated attacks are sometimes called “script kiddies.” Their attacks are often aimed at systems with weak security. They tend to make more mistakes and are not as capable at hiding their attacks, which makes it easier for law enforcement officials to track them down.
- **Cyber Black markets**:-are online stores that provide criminals with the materials or tools they need to carry out cybercrimes.

# 2.1.4. Motives of Cyber criminals

1. **Financial Reasons**
2. **Disrupt Business**
3. **Terrorism**
4. **Theft (Nonfinancial)**
5. **Political Reasons**
6. **Amusement/Curiosity/Challenge**
7. **Organized Crime**
8. **Locating Victims**

- **Effects of Cyber crime** The victims of cybercrime, whether they are businesses or individuals, face many-repercussions, both in the short term and the long term.

# 2.2.1. Types of cybercrimes

- Generally, there are **three** major categories of cybercrimes that you need to know about. These categories include:

1. **Crimes against People.** While these crimes occur online, they affect the lives of actual people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online related libel or slander.

# Cont...

2. **Crimes against Property:-** Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and type squatting, computer vandalism, copyright infringement, and IPR violations.
3. **Crimes against Government:-** When cybercrime is committed against the government, it is considered an attack on that nation’s sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

# Cont..

- **Specifically, The United Nations lists five categories of cybercrime**:
- (1) financial (crimes that disrupt a business's ability to conduct e-commerce, such as viruses, cyber attacks or DoS attacks, or e-forgery),
- (2) piracy (copying copyrighted material),
- (3) hacking (the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access),
- (4) cyber-terrorism, and
- (5) online pornography.

# Cont...

- It is also categorized as the U.S. Department of Justice categorizes types of computer crime in three ways:
- (1) the computer as the target (attacking the computers of others by spreading viruses or a denial-of service [DoS] attack or an attack on a website),
- (2) the computer as the weapon (using a computer to commit traditional crimes, such as fraud, illegal gambling, or online pornography), or
- (3) the computer as an accessory or a device that contains data incidental to the crime (using a computer as a method to maintain records on illegal or stolen information).

## 2.2.2.Cybercrime Law Enforcement

- generally, amount of cyber crime are not known.
- cybercrimes are not reported to law-enforcement.**:- Is Difficult to Combat for the following reasons:**

1. **Cybercrimes Are Borderless**
2. **Cybercrimes Are Easy to Commit**
3. **Resources Are Lacking**
4. **Offenders Are Transient**
5. **Laws and Policies Are Ineffective**
6. **Damage Is Unclear or Unreported**
7. **Cultural Norms Differ**
8. **Turf Wars Are Common**

## 2.2.3 Law Enforcement Agencies

- Many law enforcement agencies battle cybercriminals.
- In USA, Local, state, and federal organizations attempt to enforce laws pertaining to cybercrime, and some international organizations work in cooperation to stop the harm caused by computer crimes.
- Some of these organizations are described in the following sections.

# Cont...

- **Department of Justice:-** Personnel within the Department of Justice are responsible for investigating and prosecuting those accused of intellectual property crimes, including those who have violated copyrighted materials, trademarks, and trade secrets.
- The different agencies within the Department of Justice that deal with cybercrimes are:-
- **the Computer Crimes and Intellectual Property Section (CCIPS),**
- **the Computer Hacking/Intellectual Property (CHIP) Unit,**
- **the Intellectual Property Task Force,**
- **the International Criminal Investigative Training Assistance Program,**
- **the National Security Cyber Specialists (NSCS),**
- **the Cyber security Unit, and**
- **the FBI.**

# 2.3. Emerging trends in cyber criminality

- ***Cybercrime and the Internet of Things (IoT)***

  Th IoT encompasses millions of computer-based devices that transmit data over the internet autonomously.

- These include smart home devices and automation products like smart thermostats, smart bulbs, smart TVs, and wearable sensors like heart rate and respiratory rate monitors. Due to technological advances, cheap data storage, and fast internet connections, the Internet of Things (IoT) is everywhere.

# Cont...

- ***Cybercrime: Machine Learning and Artifiial Intelligence***

  Machine Learning (ML) and Artifiial Intelligence (AI) may be beneficial in the fight against cyber attacks.

- ML, a subdivision of AI, enables a computer to learn from experience and behave with a semblance of human-like intellect.
- This goal is still largely in the future. ML can improve cyber security by spotting abnormal activity patterns in an attack much faster than a human.
- Using deception as an automated response, AI can send decoys that deceive cyber-attackers, while still adapting to new situations, learning from them, and preventing future attacks.

# Cont...

- ***Online Child Sexual Abuse and Exploitation (CSAE)***
- Besides financial rewards, cybercriminals are enticed by cyber-bullying, pedophilia, and sexual exploitation, and goals that are political and ideological.
- The internet has exponentially increased the production, distribution, and possession of child pornography images and child sexual abuse material (CSAM). The United States has addressed online child pornography with the Child Pornography Prevention Act of 1996 (CPPA)82 and the PROTECT Act of 2003.83
- Furthermore, the Council of Europe (COE)84 criminalized online activities related to child pornography and classified such behaviors as cybercrimes in its Convention on Cybercrime.
- **Crypto-currency** crimes cannot be predicted or punished properly due to user anonymity and lack of oversight by government and fiancial regulators.
- **State-Sponsored Cyberwarfare and Industrial Espionage**
- **Cyber tereorisiom**

# 1: Privacy and Data Protection

## 1.1.1. Understanding data protection

- Prior to the so-called ‘information revolution’, information and data held on individuals would only be kept in traditional filing cabinets or their equivalent. Not only might these be accessed only relatively infrequently, perhaps by the holder of the data, but it would also be difficult for other users of similar information or information about the same individual to gain access.
- In 1972, despite the fact that computerisation was then still at an embryonic stage, the Younger Committee on Privacy identified characteristics that distinguished storage of information on computer from more traditional methods. The Committee noted in particular three specific areas of concern: the use of computers to compile personal profiles; their capacity to correlate information; and the ease with which unauthorised access to data could be obtained, often from remote sites.

# Cont…

- Despite the fact that users may recognise, at least in principle, the potential threat to their privacy from these invasive technologies, it clearly does not deter use of the internet; indeed, as Kane and Delange have observed, it appears as if the internet ‘inspires a trust factor that otherwise does not exist outside of the online world’, and although the internet might have originated as ‘a one or two-dimensional system of information and transactions’, it has subsequently ‘morphed into a three dimensional platform through which we participate through online shopping, email and social networking sites .
- Unfortunately, this level of trust means that either users do not recognise any potential threat to their privacy, or, if they do, are unconcerned about it, or do not always take appropriate steps to protect their own privacy until they find that privacy unacceptably compromised.

# Cont...

- Although there have been significant legal initiatives – notably the law on data protection – the rapid development of the internet and Web 2.0 applications in particular has meant that the law has not kept pace; in particular, as we shall see later, the European Data Protection Directive 95/46/EC was drafted and implemented when the internet was still in its infancy and the extent to which its provisions can be easily applied to the circulation of personal data on the internet remains controversial.
- For this and other reasons, a new General Data Protection Regulation (GDPR)18 was adopted by the European Parliament on 14 April 2016 and came into force on 24 May 2016.

- Despite privacy and ‘privacy-invading features’ being discussed in the context of data protection, it has not always been easy to reconcile the terms ‘**data protection’,** on the one hand, and ‘**privacy’,** on the other. This is not helped by the fact that an agreed definition of privacy remains elusive.
- The analysis of the multifaceted and slippery concept of privacy continues to the present, but with no agreed conclusion or consensus, much less the emergence of any workable legal definition.
- Westin suggested that **‘Privacy** is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others’, a definition based on the right of self-determination, which may be placed at particular risk by the practice of data matching made so simple by modern information technology (IT).

# Cont…

- This notion was supported by Miller, in the specific context of this technology, who considered privacy to be ‘the individual’s ability to control the circulation of information relating to him’.
- Gavison, on the other hand, is critical of the ability to control personal information as being a determinant of the definition of privacy precisely because a dependence on subjective choice makes both a realisation of the scope of the concept and the provision of legal protection problematic.
- The definitional difficulties are exacerbated by the fact that whether or not privacy is considered to have been invaded is a very subjective issue, which will depend not only on the view of the person whose privacy is being invaded, but also on who is the invader and what information he or she is uncovering.

# Cont…

- Whether or not there is an accepted and acceptable definition of ‘**privacy**’, it is usually recognised as **a fundamental human right, and accorded specific protection under human rights conventions and national constitutions.**
- In contrast, **data protection** is often viewed as a technical term relating to specific information management practices – the preferred stance of those who would see data protection primarily as an aspect of business regulation.
- Even if the precise nature of the relationship between data protection and privacy is elusive, one approach to the undeniable tension between the rights of all those who would seek to exert control over personal information can be found in the terminology of risk and risk assessment, concepts that are, perhaps, more familiar in a business environment.

# Cont…

- Three risk factors can be identified that could be considered to be elements of privacy.
- **The first** of these is the **risk** of injustice due to significant inaccuracy in personal data, unjust inference, ‘function creep’ (the gradual use of data for purposes other than those for which it was collected), or reversal of the presumption of innocence, as seen in data matching when correlation of information from disparate sources may produce an impression that is greater than the sum of the parts.
- **The second risk** is to one’s personal control over the collection of personal information as a result of excessive and unjustified surveillance (which would presumably include monitoring the use of particular websites), collection of data without the data subject’s consent, and also the prohibition or active discouragement of the means to remedy these risks, such as the use of encryption and anonymising software.

# Cont…

- **Finally, there is a risk** to dignity as a result of exposure or embarrassment due to an absence of transparency in information procedures, physical intrusion into private spaces, unnecessary identification or absence of anonymity, or unnecessary or unjustified disclosure of personal information without consent.
- data protection measures may be considered as risk management devices that need to balance the risk to the individual from unnecessary invasion of privacy with the measures necessary to control that risk.
- The precise relationship between privacy and

# Cont…

- Art 1 of the Data Protection Directive explicitly protects the privacy of an individual with respect to the processing of data; on the other hand, there is no mention of the word ‘privacy’ in the Data Protection Act 1998 intended to implement the Directive. In contrast, a parallel provision has not been included in the General Data Protection Regulation which makes very little mention of privacy at all. Although this could be viewed as a move away from a focus on privacy Costa and Poullet believe that ‘it is certain that affirming the autonomy of the right to protection of personal data does not imply denying privacy as its fundament.’

# Cont...

- Mayer Schönberger has further traced this development in terms of a succession of generations of data protection legislation.
- Of these, he suggests that the **first generation** represents those laws passed in the early 1970s that reacted to the onset of large databanks and the overall phenomenon of data processing.
- **The second generation**, which emerged in the late 1970s, began to focus more explicitly on the individual rights of citizens.
- This was further developed by the **third generation** of regulation in the 1980s, which emphasised informational participation and self-determination.
- **The fourth generation**, which Mayer-Schönberger suggests focuses more on holistic and sectoral perspectives, is exemplified by Directive 95/46/EC and emerged in the 1990s.

# Personal data

- **Personal data** is defined in Art 2(a) of the Directive as ‘any information relating to an identified or identifiable natural person. This person is known as the ‘data subject’ and is someone who can be ‘identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.
- In contrast, DPA 98, s 1(1) defines personal data as data relating to a living individual who can be identified from those data, or from a combination of those data and other information in the possession of the data controller. This specifically includes ‘any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.’
- In Art 8 the Directive identifies certain ‘special categories’ of data namely that relating to ‘racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life’, the processing of which is prohibited unless certain conditions are met as discussed below. DPA 98 refers to this as ‘sensitive data’ and, in addition to the above list, the definition includes data relating to criminal offences or related proceedings.

## The data protection principles

- The Directive sets out to protect the privacy of data subjects with respect to the processing of their personal data by embedding principles of good data management within the legislative framework.
- Five of these principles are listed in Art 6:

1. personal data should be processed fairly and accurately
2. personal data should be collected for specific purposes and not further processed for other purposes;
3. personal data processed should be relevant and not excessive;
4. personal data should be accurate and kept up to date; and
5. personal data should be kept no longer than is necessary.
6. processing in accordance with the rights of the data subject, security and trans-border data flow which are dealt with elsewhere in the Directive.
7. Some guidance as to the interpretation of the Data Protection Principles in contained in Pt II of DPA 98 Sch 1.

# Exemptions Data protection principle

- **National security.**
- **Crime and taxation**
- **Health, education and social work**
- **Regulatory activity**
- **Journalism, literature , self incrimination**
- **Research, history, statistics,** Legal professional privilege
- **Manual data held by public authorities**
- **Information available to public by or under any enactment**
- **Disclosures required by law or in connection with legal proceeding**
- **Parliamentary privilege,** Negotiation, Exa mi nation mark
- **Domestic purposes,** Corporate finance,

# 1.2. Digital surveillance and the law

- In contrast to the laws relating to the protection of privacy and personal data are those laws that justify, formalise, and regulate state and private party actions likely to impact upon individuals' normal expectations of privacy, in the pursuit of other legitimate social, political, and economic goals. These include laws that influence the use of information technologies, such as telecommunications
  and the internet, by:
- ● facilitating the tracing of links between individuals – for example, permitting collection of 'traffic data' identifying when and with whom technology users communicate;
- ● facilitating the collection of information about the detail of individuals' interactions – for example, permitting interception of the content of their communications; or

# Cont…

- In the digital information environment, the primary aim of UK state surveillance has been to ensure that law enforcement and national security agencies have suitable access and powers to maintain effective investigatory practices across the diverse range of public communications options.
- A secondary aim, motivated largely by external pressures – notably European Court of Human Rights (ECtHR) rulings – has been to place both access and investigatory powers within a legal framework.
- Such a framework, in theory, allows oversight of their lawful use, meaningful penalties for their abuse, and greater public transparency about their operation, without unduly compromising their effectiveness.
- While, on paper, considerable advances have been made toward this second aim, achieving and maintaining a proportionate balance between efficiency and legitimacy in an area in which technology is in a state of constant flux is far from a simple task.
- As a result, both legislators and judiciary have struggled to keep pace with developments.

# Cont...

- A complicating factor is that powers granted to state agencies to access and collect digital information generated by the public often produce, or permit the production of, datasets relevant to commercial organisations. For example, internet traffic data can be valuable to content providers wishing to monitor potential infringements of their intellectual property, or to advertising companies seeking to deploy ‘behavioural advertising’.1 This can lead to pressure from commercial organisations for greater access to such datasets, or for the wider grant of access and investigatory powers to the private sector.
- Here, too, there is a delicate balancing act for legislature and judiciary to consider – that is, the extent to which the business interests of commercial organisations can be accommodated, without undue impact upon either the public interest, or the perceived legitimacy of state access and investigatory powers.
- Thus the requirement of a legal framework for the legitimate exercise of access and investigatory powers by state agencies is mirrored by the need for a similar framework for private entities – a need that, in the UK, is again being addressed mainly following adverse rulings from the ECtHR

# Cont...

- As the UK regulatory framework for surveillance has developed in a piecemeal fashion, its legislative foundation is currently spread across a range of Acts, including:
- Regulation of Investigatory Powers Act 2000 (RIPA 2000);
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA 2000);
- Data Retention and Investigatory Powers Act 2014 (DRIPA 2014);
- Intelligence Services Act 1994 (ISA 1994);
- Part III Police Act 1997 (PA 1997);
- Data Protection Act 1998 (DPA 1998);
- Protection of Freedoms Act 2012 (PoFA 2012);
- Human Rights Act 1998 (HRA)

# Cont…

- In addition numerous regulatory/oversight bodies have been created, the primary bodies being:
  - Information Commissioner’s Office;
  - Investigatory Powers Tribunal;
  - Surveillance Camera Commissioner;
  - Office of the Surveillance Commissioner;
  - Interception of Communications Commissioner;
  - Intelligence Services Commissioner;
  - Commissioner for the Retention and Use of Biometric Material.

# Cont...

- the three key elements of the current regime for surveilling the digital environment:

- the legal framework for the **interception** of content in transit between parties – that is, the interception of communications;
- the requirement upon public telecommunications providers, including internet service providers (ISPs), to retain communications traffic data – that is, **data retention**; and
- the requirements placed on users of encryption technologies to make their communications accessible to the authorities upon demand – that is, **decryption** powers.

# Cont..

- The intention is to provide a single legal framework which deals with all **interception** of communications in the United Kingdom, regardless of the means of communication, how it is licensed or at which point on the route of the communication it is intercepted . . .
- The Government believes that it should not make any difference how a communication is sent, whether by a public or non-public telecommunications or mail system, by wireless telegraphy or any other communication system.
- Nor should the form of the communication make any difference; all interception which would breach Article 8 rights, whether by telephone, fax, e-mail or letter, should all be treated the same way in law.
- A single authorising framework for all forms of lawful interception of communications will mean that each application will follow the same laid down procedure and will be judged against a single set of criteria.

# Cont...

- The result of the government's consultation and deliberations post-*Halford* was the Regulation of Investigatory Powers Act 2000 (RIPA 2000). This repealed the **Interception** of Communications Act 1985, but still maintained much of the pre-existing public telecommunications interception regime, including the **oversight mechanisms**. The Act itself is split into seven parts covering the following:
- 'Communications';
- 'Interception';
- 'Acquisition and disclosure of communications data';
- 'Surveillance and covert human intelligence sources';
- 'Investigation of electronic data protected by encryption etc';
- 'Scrutiny etc of investigatory powers and of the functions of the intelligence services'; and

- Under RIPA 2000, it is a criminal offence, punishable by up to two years' imprisonment, for a person 'without lawful authority' to knowingly intercept communications by post, or through a public telecommunications system.
- It is also a criminal offence, punishable by up to two years' imprisonment, for a person without the express or implied consent of a person having the right to control the operation or the use of that system, and 'without lawful authority', to intercept communications through a private telecommunications system.
- Where communications are intercepted on a private telecommunications system, with the express or implied consent of a person having the right to control the operation or the use of that system, but without 'lawful authority', parties to the communication may bring a civil action.
- For example, if an employee believes that his or her employer has unlawfully intercepted their telephone conversation with a third party, either the employee or the third party may sue the employer. The individual authorising, or carrying out, the interception in such circumstances would not, however, be guilty of a criminal offence

**Interception takes place with 'lawful authority' where …**

- all parties to the communication have consented to it
- one party has consented to it, and the interception is authorised under Pt II of the RIPA 2000 as surveillance, rather than an interception;
- it is necessary for the purposes of providing the telecommunications service, and carried out by the provider of that service, or on its behalf;
- it is permitted under s 48 of the Wireless Telegraphy Act 2006;
- it is permitted under an international mutual assistance agreement;
- it is permitted under regulations made by the Secretary of State to permit certain kinds of interception in the course of lawful business practice;
- it is permitted under prison rules, in hospital premises in which high security psychiatric services are provided, and in state hospitals in Scotland;
- it is carried out under any statutory power that permits the obtaining of information or of taking possession of any document, or other property; and an interception warrant has been issued by the Secretary of State

- The Secretary of State may issue an interception warrant for the interception and disclosure of communications where the scope of the warrant is proportionate to the aim to be achieved, the information required could not reasonably be obtained by other means, and the purpose of obtaining the information is necessary to:

- protect the interests of national security; or
- prevent or detect serious crime in the UK, or in the context of any international mutual assistance agreement; or
- safeguard the economic well-being of the UK

# Criteria for interception

- Where these criteria are met, interceptions are authorised for monitoring or recording communications:
- to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures, or to ascertain or demonstrate standards that are or ought to be achieved (for example, quality control and training);
- in the interests of national security
- to prevent or detect crime; to investigate or detect unauthorised use of telecommunication systems ; or to secure, or as an inherent part of, effective systems operation.
- They are also authorised for monitoring, but not recording: received communications to determine whether they are business or personal communications ; or
- communications made to anonymous telephone helplines

- Communications data can be broadly divided into three main types:
- ***traffic data*** – information about a communication, such as the location of a person when using his or her mobile phone;
- ***service use data*** – information about the use of a communications service, such as itemised telephone call records showing the numbers called; and
- ***subscriber information*** – information about the user of a communications service, such as the identity of the subscriber to a particular telephone number.

- The Directive set out several categories of data to be retained. These were data necessary to:
- trace and identify the source of a communication, such as the telephone number and subscriber name and address (telecoms), or user ID and name and address of the subscriber or registered user (internet);
- identify the destination of a communication, such as the number called, any number to which a call is rerouted, name and address of subscriber/user (telecoms), or user ID or telephone number of the intended recipient(s) of an internet telephony call, and name and address of subscriber/user (internet);
- identify the date, time, and duration of a communication;
- identify the type of communication, such as the telephone or internet service used;
- identify users' communication equipment, or what purports to be their equipment; and
- identify the location of mobile communication equipment, such as cell ID and the geographic location of cell.

- **Encryption** involves turning ordinary information (or plaintext), such as letters or emails, into apparent random strings of characters (or ciphertext). **Decryption** is the reversal of this process. Both encryption and decryption require the use of specific algorithms and a ‘key’.
- **Symmetric-key cryptography** refers to encryption in which both the sender and receiver share the same key;
- asymmetric key cryptography refers to encryption in which two different but mathematically related keys are used – a public key and a private key. In **asymmetric systems**, the public key is typically used for encryption, while the private key is used for decryption.
- Thus if Alice wants to send Bob a secret message, she uses her private key to generate a public key, which she passes to Bob. Bob uses the public key to encrypt the message to send to Alice, who decrypts it with her private key.

# 1.3. Surveillance capitalism and the law

- “Capitalism, as a mode of production, is an economic system of manufacture and exchange which is geared towards the production and sale of commodities within a market for profit, where the manufacture of commodities consists of the use of the formally free labour of workers in exchange for a wage to create commodities in which the manufacturer extracts surplus value from the labour of the worker in terms of the difference between the wage paid to the worker and the value of the commodity produced by him/her to generate that profit.
- The foundation on which surveillance capitalism is built is user data. Google was one of the first to discover the power of the data they can access. User data, such as search queries, were stored and initially regarded as waste or by-product, even termed ‘data

# Cont…

- the privacy is essentially a *decision right* which is claimed by surveillance capitalism. This leads, according to her, to a ‘redistribution’ of privacy, which in effect means that the decision rights of many people to decide over their data, are now held by a few surveillance corporations.

# Chapter 4: Human Rights in Cyberspace: Freedom of Expression Online

### 4.1. Digital rights and the law

- The right to express oneself is fundamental in a free and democratic society. Again this right is not an absolute one and is tempered by the need to protect other interests which also are important in a democratic society, such as the reputation and freedoms of others.
- Unfortunately, governments in some countries do not recognise a right of freedom of expression and some try to interfere with what is available in their countries over the internet. For example, The People's Republic of China imposed restrictions on internet service providers and also uses firewall technology to prevent access to certain sites. Companies like Google, Microsoft and Yahoo! Complied with certain restrictions. Examples included taking down blogs critical of the government and weeding out websites. It seems that access to content including words such as 'freedom' and 'democracy' was prevented.

# Cont...

- In Europe and other democracies, there are still controls over offensive material through a wide range of national laws. Although most cover similar issues, not all are compatible. For example, in some countries though not others, it may be an offence to advertise certain types of goods. Laws such as those relating to defamation, data protection, incitement, discrimination and the stirring up of racial hatred are just some examples of those that could apply to all forms of publishing, including publishing online.

# Cont...

- Article 10 of the Human Rights Convention sets out the right of freedom of expression thus:
  1 Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

  2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

# Cont...

- The right is without frontiers. This means, subject to para. 2, the right extends to publishing material on the internet, notwithstanding interference with the right by governments of other countries. The same point can be made about proportionality as applies to the right of privacy. Paragraph 2 also highlights the fact that the right is subject to duties and responsibilities.
- There are a number of points that can be made about the right of freedom of expression. The exercise of the right might conflict with national laws in countries other than the one in which the person exercising it resides. Or the ‘victim’, if there is one, may be in a different country. This immediately brings into play jurisdictional issues.

## 4.2. Digital speech management: filtering and ranking

- The USA has a strongly embedded commitment to free speech enshrined in the First Amendment, but this has does not mean that there has not been significant legal activity surrounding the question of regulation of content on the internet.
- In the 1990s, the use of the internet as a medium for the circulation of various types of pornography, together with the fact that such material could then easily be accessed by minors, caused both concern and controversy amongst both politicians and the public. An examination of the legislative and judicial response to this issue provides a useful illustration of some of the difficulties encountered when attempting to regulate content on the internet.

# Assignment

- **The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media**
  Kinfe Micheal Yilma  and Halefom Hailu Abraha
  read and summarize then present by group followed by question in the class at the end of the course.
  page 108-127