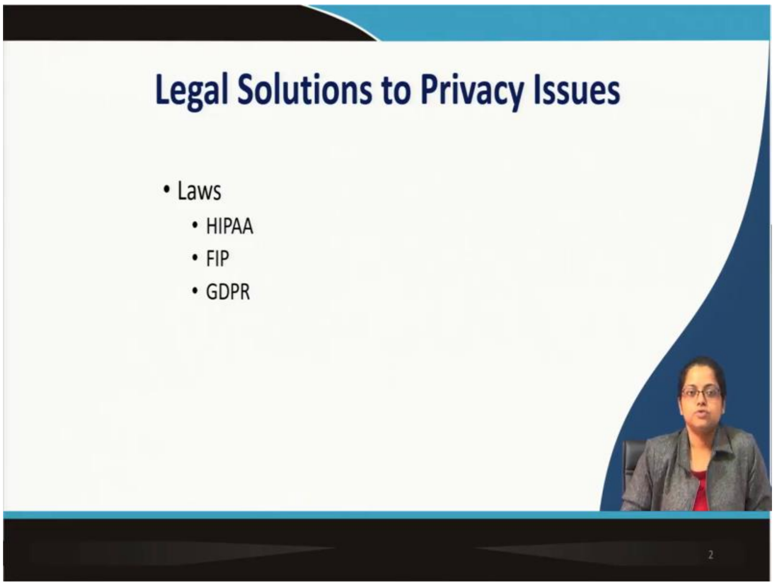
Management Information System
Prof. Saini Das
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Module – 11
Ethical, Social and Security issues in MIS
Lecture – 52
Ethical and Social Issues in MIS – II

Hello, welcome back! So, this is the second session on ‘Ethical and Social Issues in Management Information System’. So, in the previous session, we had spoken about very-very important ethical issue that pertains to the digital world and the world of information system. So, we had discussed about privacy, information privacy. In today’s session, we will continue with information privacy.

So, we had discussed the challenges and we had also discussed the technical solutions to privacy. Today, we will be talking about, we will be focusing on the legal challenges, sorry, the legal measures that or companies or say, countries adopt to protect customer privacy while they are on the internet or while they are using information system.

(Refer Slide Time: 01:13)



Legal Solutions to Privacy Issues

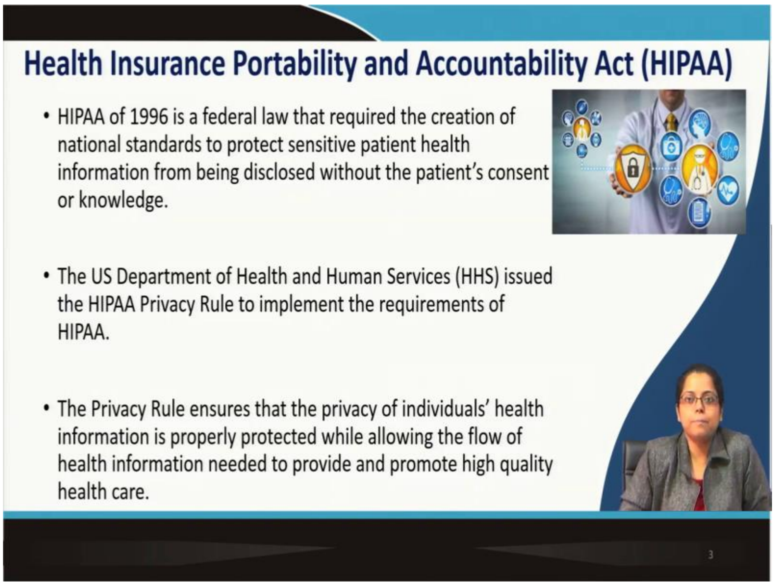
- Laws
  - HIPAA
  - FIP
  - GDPR

So, moving on legal solutions to privacy there; so, there are lot of laws that many countries implement to protect the privacy of their individuals. So, today we will be talking about three very important laws with respect to consumer privacy, in using, while using information system.

The first one pertains to HIPAA, which stands for Health Insurance Portability and Accountability Act. So, as you can understand by the title itself, this pertains to health records of electronic health record or electronic medical records of patients. The second one talks about FIP or Fair Information Practices.

So, this is again this pertains to you know E-commerce companies or online when people are browsing online, what are the principles that are adopted to protect their information. And, the third one pertains to GDPR, the General Data Protection Regulation adopted by the European Union.

(Refer Slide Time: 02:21)



Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA of 1996 is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
- The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA.
- The Privacy Rule ensures that the privacy of individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care.

3

So, let us move on, let us understand each of these HIPAA. The first one HIPAA stands for Health Insurance Portability and Accountability Act. So, HIPAA of 96 is a federal law of the United States that require the creation of national standards to protect sensitive patient health information from being disclosed without the patients consent or knowledge. So, in the United States patient's information is stored in the form of electronic medical records or electronic health records.

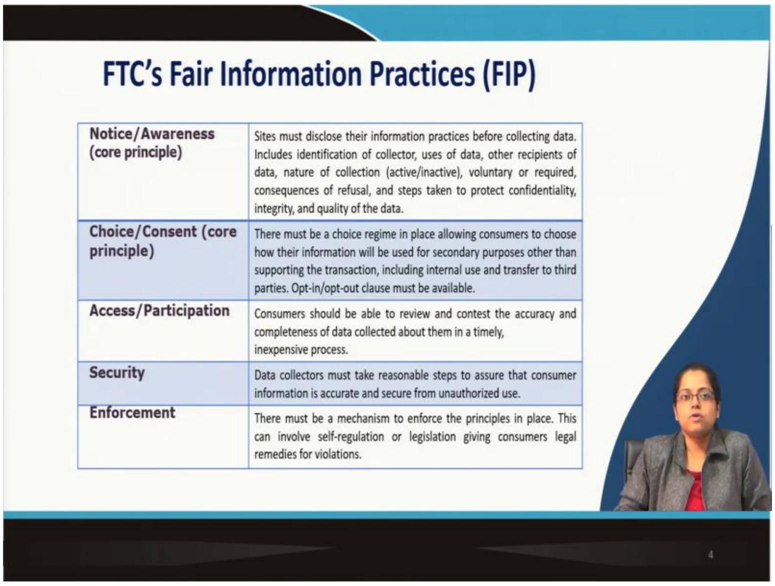
So, HIPAA pertains to that particular category of information patient information, which is stored electronically or digitally and which can be transferred to different third parties in the healthcare service itself to provide better quality of service to the patient. The US Department of Health and Human Services issued the HIPAA Privacy Rule to implement the requirements of HIPAA.

What is this HIPAA Privacy Rule? The Privacy Rule ensures that the privacy of individuals health information is properly protected, as in the privacy of the individuals health information is maintained and is not shared with anybody, any other third party in the health care value chain without the consent of the patient.

But, at the same time it should allow the flow of health information needed to provide and promote high quality and timely health care service to the patient. So, here there should be a balance between the privacy of individual’s health information and you know the high quality health care, high quality and timely health care provided to the patient. So, there should be a balance between the two.

So, HIPAA represents the Privacy Rule of the HIPAA says that there should be a balance, when health information is being transferred or transmitted between individuals in a health care value chain. But, it should not compromise the health, or the service, or health care service that is provided to the patient. So, that is the first law.

(Refer Slide Time: 04:38)



FTC’s Fair Information Practices (FIP)

Notice/Awareness (core principle)	Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of the data.
Choice/Consent (core principle)	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties. Opt-in/opt-out clause must be available.
Access/Participation	Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security	Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement	There must be a mechanism to enforce the principles in place. This can involve self-regulation or legislation giving consumers legal remedies for violations.

The second law that we are talking about here is the FTC’s the Federal Trade Commission’s of United States fair information practices. And, of course, we have mentioned United States, but FIP is one of the most critical, legal principles, which are followed by online companies all across the world today.

So, FIP has certain core principles, which sites must follow if they are collecting data online. The first one stands for notice or awareness. It is a core principle; it says that sites must disclose their information practices before collecting data. And, this is usually done in form of a privacy policy, which all of you must have observed on websites, but many of you do not read, because of the length, or because of the because of the you know the way in which the privacy policy is actually drafted.

For many of you might seem it might seem intimidating but, it is very important for all of us to go and have a look at the privacy policy before we are dealing with a particular website, to be sure that our data is handled our private data is handled in the way in which we would actually want it to be.

So, notice awareness includes identification of collector, uses of data, other recipients of data, nature of collection, voluntary or required, consequences of refusal, and steps taken to protect confidentiality integrity and quality of data.

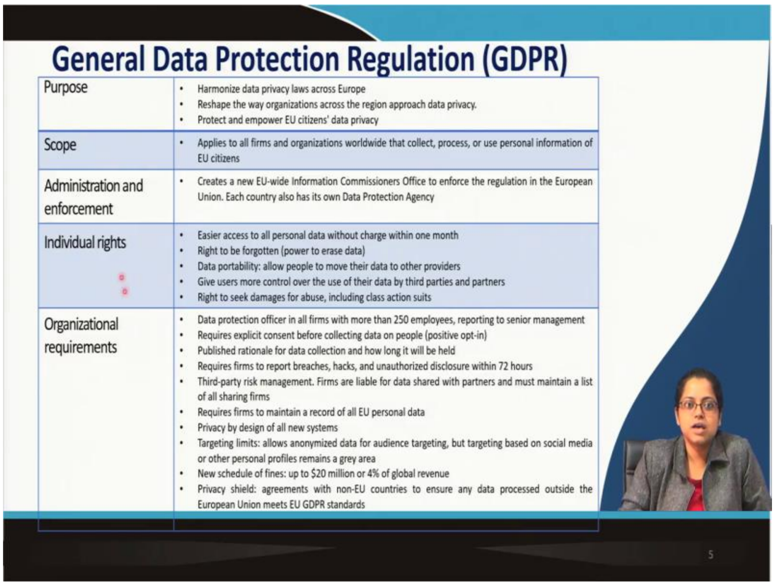
So, all of these must be mentioned in the privacy policy according to fair information practices, if, you want to collect and use customer information online. The next core principle pertains to choice or consent. So, there must be choice regime in place allowing consumers to choose how their information would be utilized. In the sense that how their information would be collected, stored and transmitted to third parties.

So, opt in and opt out clause which we had just discussed in the previous lecture must be available to the customers. Access or participation so, FIP mentions that consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.

Security, goes without saying security and privacy are intertwined with each other. So, data collectors must take reasonable measures to assure that consumer information is accurate and secure from unauthorized use. Enforcement finally, there should be a mechanism to enforce the principles in place. This can involve self-regulation or legislation giving consumers legal remedies for violations.

So, all of these five are principles of fair information practices and most E-commerce websites not only in the United States, but all across the world; follow FIP practices, in drafting their privacy policies and also when they are in reality, you know collecting, storing and transferring customer information online.

(Refer Slide Time: 08:00)



General Data Protection Regulation (GDPR)

Purpose	• Harmonize data privacy laws across Europe • Reshape the way organizations across the region approach data privacy. • Protect and empower EU citizens' data privacy
Scope	• Applies to all firms and organizations worldwide that collect, process, or use personal information of EU citizens
Administration and enforcement	• Creates a new EU-wide Information Commissioners Office to enforce the regulation in the European Union. Each country also has its own Data Protection Agency
Individual rights	• Easier access to all personal data without charge within one month • Right to be forgotten (power to erase data) • Data portability: allow people to move their data to other providers • Give users more control over the use of their data by third parties and partners • Right to seek damages for abuse, including class action suits
Organizational requirements	• Data protection officer in all firms with more than 250 employees, reporting to senior management • Requires explicit consent before collecting data on people (positive opt-in) • Published rationale for data collection and how long it will be held • Requires firms to report breaches, hacks, and unauthorized disclosure within 72 hours • Third-party risk management. Firms are liable for data shared with partners and must maintain a list of all sharing firms • Requires firms to maintain a record of all EU personal data • Privacy by design of all new systems • Targeting limits: allows anonymized data for audience targeting, but targeting based on social media or other personal profiles remains a grey area • New schedule of fines: up to $20 million or 4% of global revenue • Privacy shield: agreements with non-EU countries to ensure any data processed outside the European Union meets EU GDPR standards

Now, coming to the third you know legal measure that European Union has taken to protect it is customer information online is the General Data Protection Regulation or GDPR. So, GDPR the purpose of GDPR is to harmonize data privacy laws across Europe. And, most Indian and as well as all other e commerce companies of the world which are transacting with the European Union, because today E-commerce companies are in general global in nature.

So, they have to abide by the GDPR, if they want to collect and handle you know customer information from the European Union in their websites. So, another purpose of GDPR is to reshape the way organizations across the region approach data privacy. And, also it is purpose is to protect and empower European Union citizen’s data privacy.

Scope, it applies to all firms and organizations worldwide that collect process or use personal information of European Union citizens. Now, European sorry the GDPR has two different categories of rights; one pertains to individuals and the other pertains to organizations.

So, for individuals the rights are easier access to all personal data without charge within 1 month right to be forgotten. So, individuals have the right to delete or erase their data, data portability so, allow people to move their data to other providers.

So, in case particular user wants to shift it is provider say health care provider or insurance provider, GDPR mandates that the customer has the right to do. So, and data should be transferred by the health care provider or the insurance provider to the new provider. Give users more control over the use of their data by third parties and partners. And, right to seek damages for abuse including class action suits.

So, these are the individual rights which come under the purview of GDPR, there are certain organizational rights requirements, which are very important, an organization should abide by these requirements, if they want to you know transact or if they want to trade or deal in the European Union.

So, a data protection officer should be there in all firms, which have more than 250 employees very very critical. So, if you are a firm operating in the European Union, you should definitely and you have more than 250 employees you should have a data protection officer in place, who should report to the senior management.

Requires explicit consent before collecting data on people, so, there should be an opt in clause; very important. Published rationale should be there for data collection and how long data will be held? So, everything about consumer data, which is being collected should be clearly represented to the consumer. So, that the consumer is well aware beforehand, before transacting, is well aware of how his or her data is going to be handled by this particular website.

And, if required the customer can opt out. It require this is very important the 4th point, it requires firms to report breaches, hacks and unauthorized disclosure within 72 hours, very very critical why I am mentioning this; is because the United States and also European Union after arrival of GDPR mandates. That in case a company operating within it is premises, undergoes a data breach, it should report to the data breach within 20-72 hours.

So, but this any such law is not there in other many other geographies of the world including India. In India if Indian companies suffer any data breach, they are not mandated by a law to disclose the data breach within any stipulated period of time. So, very often because of fear of you know reputation image or reputation, lot of or maybe you know even if we can go a step ahead and consider that stock market impact.

A lot of companies because of fear of all of these do not disclose any data breach that happens on them. Which is very very difficult, because if consumers are not in intimated about data breaches. Data breaches are not disclosed, not reported, they cannot take appropriate measures to protect their data.

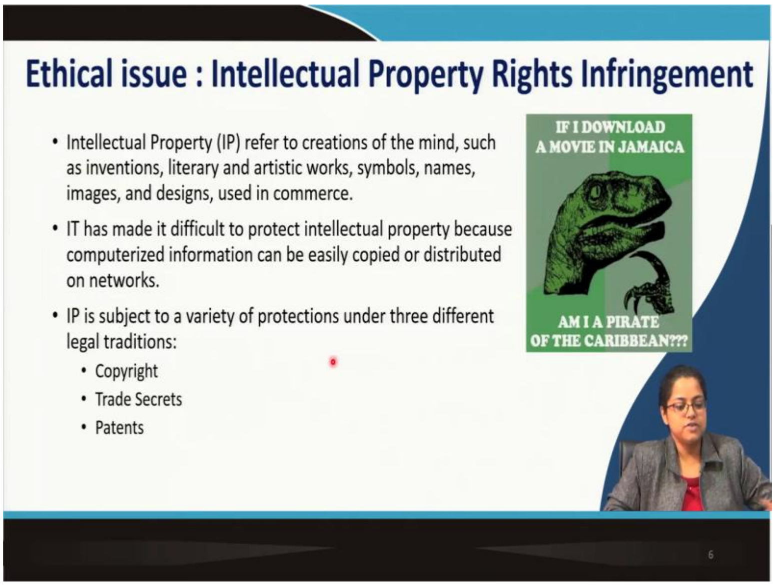
Now, third party risk management. So, firms are liable for data shared with parties and must maintain a list of all sharing firms. Requires firms to maintain a record of all European Union personal data very important, privacy by design of all new systems, so, we had when we were talking about IOT we had discussed about privacy by design, for all IOT devices is a must.

And, GDPR again mandates that any new system that is coming up should have privacy by design implemented hm. So, so there are certain other for example, new schedule of fines. So, up to 20 dollar, 20 million dollars or 4 percent of global revenue should be the fine, in case of GDPR is violated, privacy shield, agreements with non European Union countries to ensure any data processed outside European Union Meets EU GDPR standards.

So, all of these are very important requirements for organizations, if they want to transact within the European Union or if they want to transact, if they want to establish their setup and offices within the European Union. So, we have discussed how three legal measures adopted by different geographies. The HIPPA, the GDPR and the fair information practices help in maintaining customer privacy, while they are transacting or dealing, online digital or digitally.

So, with that we have discussed a lot about privacy which is a very important ethical issue in the digital world.

(Refer Slide Time: 14:51)



Ethical issue : Intellectual Property Rights Infringement

- Intellectual Property (IP) refer to creations of the mind, such as inventions, literary and artistic works, symbols, names, images, and designs, used in commerce.
- IT has made it difficult to protect intellectual property because computerized information can be easily copied or distributed on networks.
- IP is subject to a variety of protections under three different legal traditions:
  - Copyright
  - Trade Secrets
  - Patents

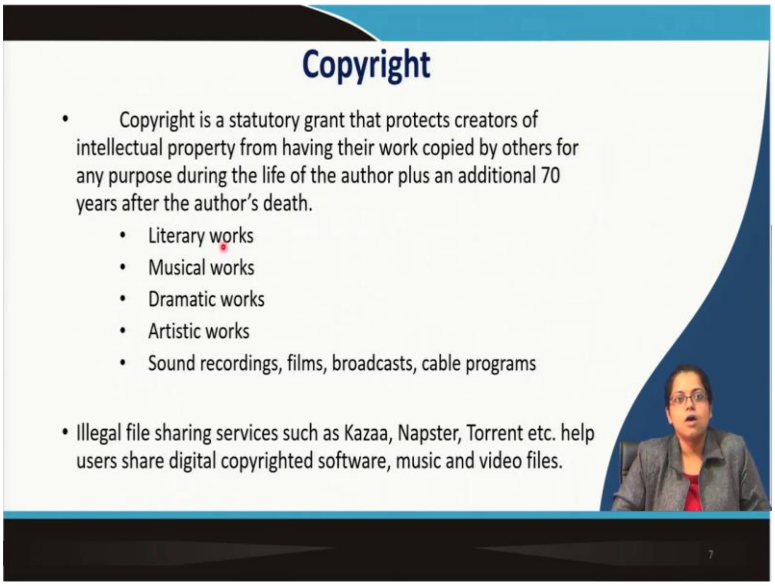
So, now we will move on to the next issue, which is which pertains to intellectual property rights infringement. So, intellectual property refers to creations of the mind such as individual inventions, literary and artistic works, symbols, names, images, and designs, used in commerce.

So, anything which refers to your creative mind, some output that has happened as a result of your creation is an intellectual property. Information technology has made it difficult to protect intellectual property, because computerized information can be easily copied or distributed on networks you know, how easy it is to copy a file or a digital media.

So, for example, a video, and a podcast, a file, a software, all of these can be easily copied but hard copies are difficult to be copied; right; you cannot easily copy; you can of course, make a photocopy, but; if ah; but if you know in the online world, all of these have become much more easy.

IP is subject to a variety of protections under three different legal traditions. So, we have copyright, trade secrets and patents. We will see each of these three and then we will understand how they can be used. How you know these intellectual properties can be their rights can be infringed upon and how they can be prevented.

(Refer Slide Time: 16:25)



Copyright

- Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death.
  - Literary works
  - Musical works
  - Dramatic works
  - Artistic works
  - Sound recordings, films, broadcasts, cable programs
- Illegal file sharing services such as Kazaa, Napster, Torrent etc. help users share digital copyrighted software, music and video files.

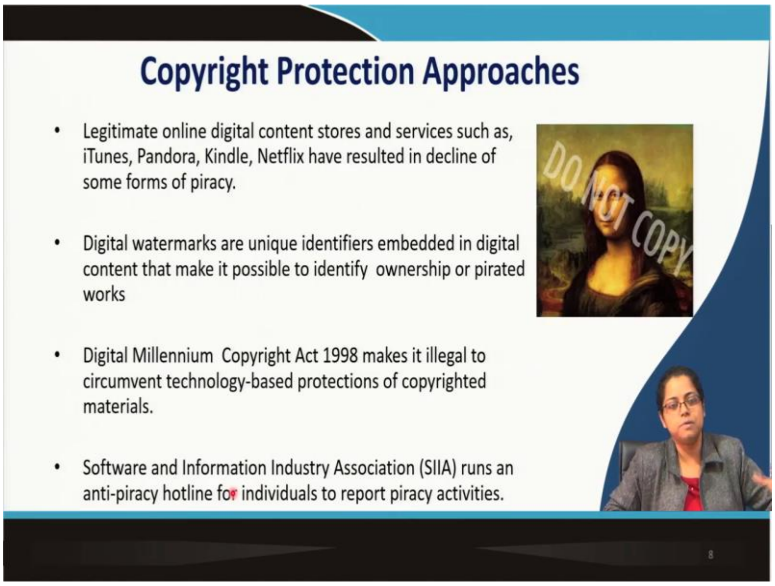
Copyright; copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death.

So, copyright pertains to literary works, musical works, dramatic work. So, anything that is that comes out of out of somebody's creativity. Artistic works sound recording films broadcast cable programs; so, all of these come under the purview of copyright. Illegal file sharing services such as Kazaa, Napster, Torrent etcetera, help users share digital copyrighted software, music and video files.

So, many of us I am sure many of you might have used torrent to download movies, which is not legal, because you are violating, you are infringing upon a copyright here. So, there are there were a lot of such software, such as services such as Kazaa, Napster etcetera, some of which came under the legal scanner and had to shut down also.

Because, they were promoting piracy and they were helping in sharing copyrighted media without appropriate permission. So, this is the problem that happens with copyright infringement.

(Refer Slide Time: 18:03)



Copyright Protection Approaches

- Legitimate online digital content stores and services such as, iTunes, Pandora, Kindle, Netflix have resulted in decline of some forms of piracy.
- Digital watermarks are unique identifiers embedded in digital content that make it possible to identify ownership or pirated works
- Digital Millennium Copyright Act 1998 makes it illegal to circumvent technology-based protections of copyrighted materials.
- Software and Information Industry Association (SIIA) runs an anti-piracy hotline for individuals to report piracy activities.

There are of course, certain measures which can be implemented, some of them are technical, some of them are legal in nature again, which can be implemented to protect against copyright infringement.

So, let us look at those. Legitimate online digital content stores and services such as, iTunes, Pandora, Kindle, Netflix have resulted in decline in some forms of piracy. So, earlier before the arrival of these services, which we have mentioned here and many more other such other services.

Piracy was rampant there was a time, when it was it was thought that piracy would actually destroy the entire music industry. Because any new music that was getting created was pirated and shared. So, there was a huge problem, then came up certain legitimate online digital content stores, such as iTunes, Pandora, which is an online form of online radio, kindle all of us are aware of so, online books Netflix online media.

So, all of these have actually you know they have legitimized paying for these services and have resulted in decline in some forms of piracy. And, using these services, it is also very difficult to download and copy any digital media, there are certain restrictions, towards downloading and copying certain media. Now, the next technology is digital watermark. And, this is very very relevant for files, so, online files.

Digital watermarks are unique identifiers embedded in digital content that make it possible to identify ownership of pirated works. So, here you see a do not copy. So, once this is there you know that this is a watermark which mentions that this is this has a copyright and this should not be copied. There are you know for let me take the example of Harvard business review articles.

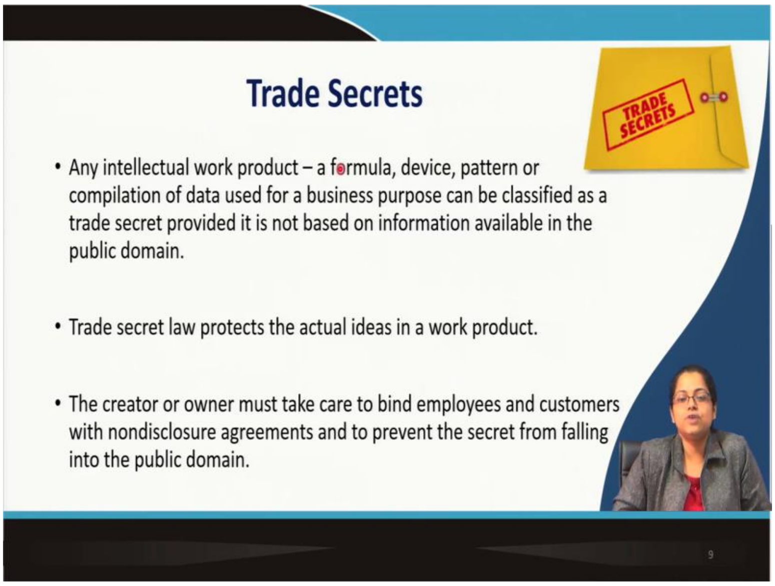
So, if you have a license and if you are paying for it, Harvard business review articles would be available to you. But, if you search on the internet you would see, that there are certain Harvard business case studies or articles, which are flying there on the internet, with a do not copy watermark. Which means that somebody who is not supposed to copy it has actually shared it which is illegal absolutely illegal and you downloading that and using that is also illegal.

So, digital watermarks are unique identifiers through with the help of technology, which make it possible to identify pirated works and maybe prevent pirated works that is the purpose. So, now moving on to you know legal measures of protecting, copyright preventing copyright infringement. The Digital Millennium Copyright Act of 1998 makes it illegal to circumvent technology based protections of copyrighted materials right.

So, with that you know, if you are trying to circumvent technology based protections of copyrighted material such as do not copy option, that is here you are committing a crime. And, you are you would come under you may come under the legal scanner.

The software and information industry association, runs an anti piracy hotline for individuals. So, in case you know you are coming across any piracy related activity you can actually report it here. So, that so, that appropriate measures would be taken. So, these are certain ways and measures of preventing copyright infringement.

(Refer Slide Time: 22:00)



Trade Secrets

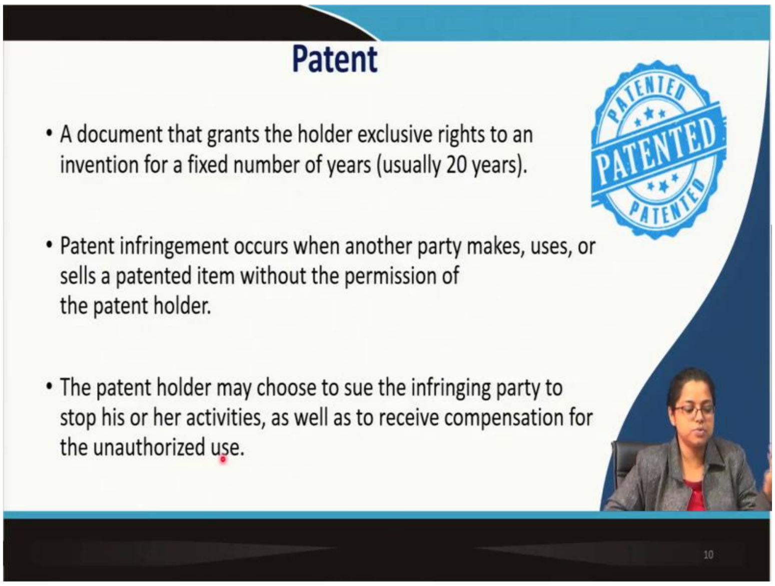
- Any intellectual work product – a formula, device, pattern or compilation of data used for a business purpose can be classified as a trade secret provided it is not based on information available in the public domain.
- Trade secret law protects the actual ideas in a work product.
- The creator or owner must take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.

Now, moving on trade secrets. Any intellectual work, a formula, a device, a pattern compilation of data used for a business purpose can be classified as a trade secret provided it is not based on information available in the public domain. So, it is used if it is used for a business purpose and it is not based on information available in the public domain; then it can it is considered to be a trade secret, for that particular company.

So, trade secret laws or you know it can pertain to a particular company, it can also pertain to a particular industry or a forum or a group they can have a trade secret, provided it is not available in the public domain. Trade secret laws protect the actual ideas in a work product. The creator or owner must take care to bind employees and customers with non disclosure agreements and to prevent the secret from falling into the public domain very important.

The onus lies with the creator or the owner of the trade secret. So, that you know you can have adequate non disclosure agreements in place. So, that employees or customers cannot steal that trade secret and make it available in the public domain. So, this is how you can protect your trade secrets.

(Refer Slide Time: 23:21)



Patent

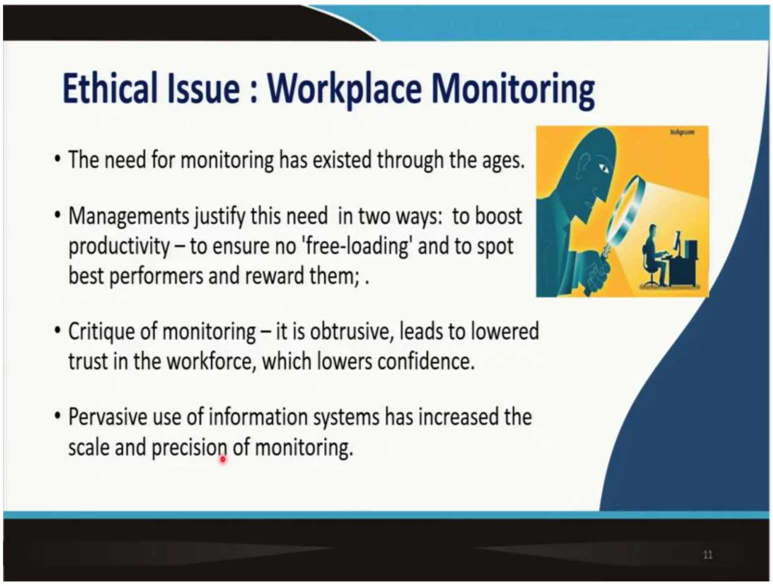
- A document that grants the holder exclusive rights to an invention for a fixed number of years (usually 20 years).
- Patent infringement occurs when another party makes, uses, or sells a patented item without the permission of the patent holder.
- The patent holder may choose to sue the infringing party to stop his or her activities, as well as to receive compensation for the unauthorized use.

Now, moving on patents; a patent is a document that grants the holder exclusive rights to an invention for a fixed number of years usually 20. Patent infringement occurs when another party makes, uses, or sells a patented item without the permission of the patent holder. Of course, you know that if you are making a discovery a new invention you.

For example, Google has a large number of patents technique technological universities have a large number of patents. So, any new invention can have a patent. And, patent infringement happens, when you are stealing or making use of that patented item without the permission of the patent holder. The patent holder may then choose to sue the infringing party to stop his or her activities, as well as to receive compensation for the unauthorized use.

So, this is a way in which patent holders may take care of preventing patent infringement right. So, we have discussed about intellectual properties and how they are infringed upon or violated and ways and means of preventing their infringement. So, this is the second social and ethical issue that we were talking about.

(Refer Slide Time: 24:43)



Ethical Issue : Workplace Monitoring

- The need for monitoring has existed through the ages.
- Managements justify this need in two ways: to boost productivity – to ensure no 'free-loading' and to spot best performers and reward them; .
- Critique of monitoring – it is obtrusive, leads to lowered trust in the workforce, which lowers confidence.
- Pervasive use of information systems has increased the scale and precision of monitoring.

11

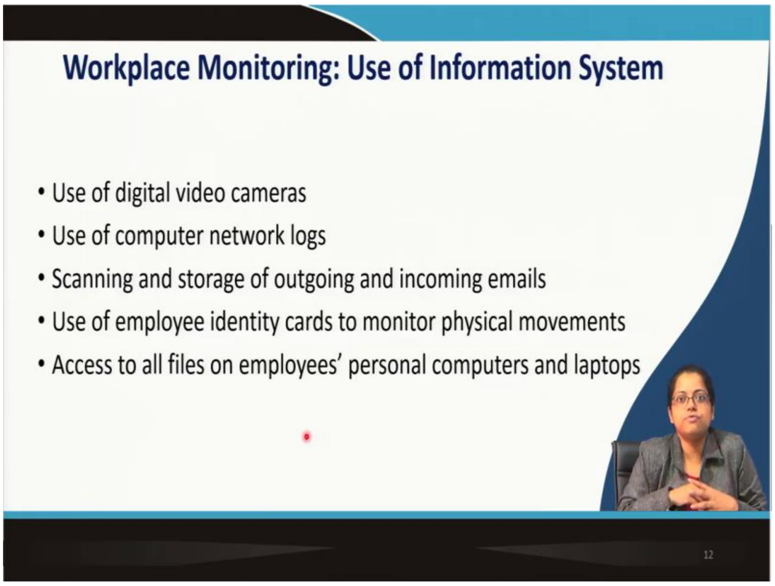
Now, moving on we will talk about the third ethical issue that is very very prevalent today in the world of; in the world of information systems in organizations. So, here we are talking about workplace monitoring. The need for monitoring has existed through ages of course; you know that monitoring was there always managements justify this need in two ways.

Firstly, they say that you know monitoring is important, because it boosts productivity to ensure that no free loading happens and, secondly, to spot best performers and reward them. So, management say that workplace monitoring is important, because it would boost productivity. And, ensure that nobody is you know freeloading or spending time, watching movies in office or spending time, you know maybe on the internet browsing his favorite social media platform and, secondly, to identify who the best performers are and to reward them.

Now, there are a lot of critiques. Who say that monitoring is not a good idea; because it is obtrusive, leads to lowered trust in the workforce which lowers confidence and eventually leads to lower productivity. So, there are a lot of people who critique monitoring, workplace monitoring. Pervasive use of information systems has increased the scale and precision of monitoring. Earlier monitoring would happen physically.

But that was very difficult and crude. But with the arrival of information systems, technology has helped in a, has helped in a huge way in improving the scale and precision of monitoring. So, let us talk about how technology can, you know, enhance workplace monitoring but how it can also be difficult for the employees many a times.

(Refer Slide Time: 26:43)



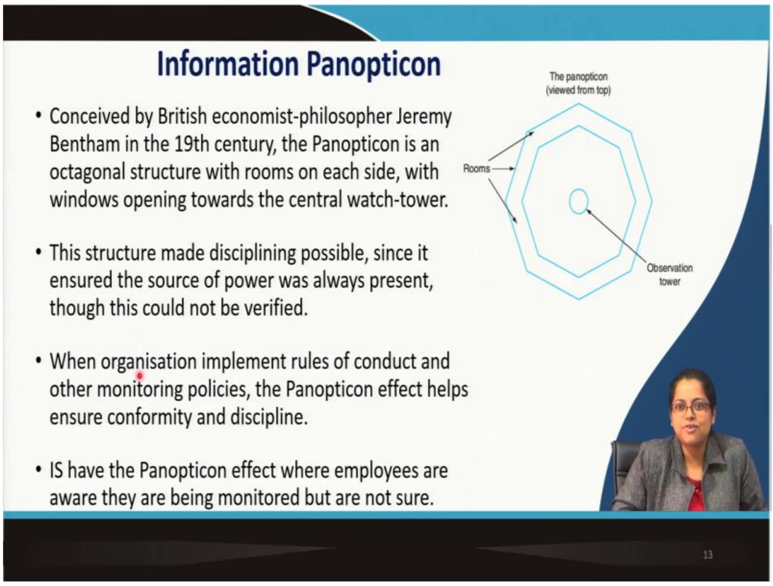
Workplace Monitoring: Use of Information System

- Use of digital video cameras
- Use of computer network logs
- Scanning and storage of outgoing and incoming emails
- Use of employee identity cards to monitor physical movements
- Access to all files on employees' personal computers and laptops

Workplace monitoring use of information system, so, use of digital video cameras, to continuously log what your employees are doing. Use of computer network logs to know, which sites your employees are visiting during work hours, scanning and storage of outgoing and incoming emails, to know what your employees are doing during work hours again.

Use of employee identity cards to monitor physical movements of employees. So, where they are going when they are coming in, when they are going out how much time they are spending in tea breaks. So, all of these can be monitored access to all files on employees personal computers and laptops. So, technology can be used these are all the all of these are different examples of how technology can be used in workplace monitoring.

(Refer Slide Time: 27:39)



Information Panopticon

- Conceived by British economist-philosopher Jeremy Bentham in the 19th century, the Panopticon is an octagonal structure with rooms on each side, with windows opening towards the central watch-tower.
- This structure made disciplining possible, since it ensured the source of power was always present, though this could not be verified.
- When organisation implement rules of conduct and other monitoring policies, the Panopticon effect helps ensure conformity and discipline.
- IS have the Panopticon effect where employees are aware they are being monitored but are not sure.

Now, let us talk about a very interesting concept called a panopticon. What is a panopticon? And, then we will come to an information panopticon. So, panopticon is a concept, which was conceived by British economist and philosopher Jeremy Bentham in the 19th century, the Panopticon is an octagonal structure here, you see an octagonal structure with rooms on each side, with windows opening towards a central watch-tower.

So, there is a central watch tower and there are rooms along the, you know, 8 sides here; it is an octagonal structure and there are windows which open. So, here there are windows on the inner wall which open towards the central watch tower and from the watchtower, anybody can watch you. So, this is the concept of a Panopticon. Now, Panopticon has a very important role in disciplining this was used for a long time the structure made disciplining possible. This concept was used to facilitate or enhance disciplining.

Since it is ensured, that the source of power that is at the center here is always present though could not be verified right. Because, you are there in these rooms, you are not sure that you are being watched, but you know that you can be watched at any point in time. But you are not sure. So, when organization implement rules of conduct and other monitoring policies, the Panopticon effect helps ensure conformity and discipline.

Information systems have the Panopticon effect, where employees are aware that they are being monitored, but are not sure. So, information systems are using you know through information system we use a lot of technologies, which we can use to monitor employees. Monitors no monitors are also aware of the fact that technologies are being used to monitor them all the time. But, they are not sure.

So, they do not know if somebody is some technology is actually monitoring their incoming and outgoing emails. They do not know, if some technology is constantly monitoring their of course, some technology is monitoring would there would be a log, but is there some technology or some mechanism by which their network logs are being monitored constantly.

So, all of these you know employees know that they are taking out time for tea breaks. So, but they are not sure that you know somebody is monitoring, because if I spend a lot of time in tea breaks during my work hour, there is a guilt feeling within I am I know that somebody is monitoring me, but since I am not sure, I may choose to take advantage or if I am little you know, if my nature is that I am little scared all the time, I might actually reduce my tea break time right. So, Panopticon concept plays a very important role in information systems in workplace monitoring.

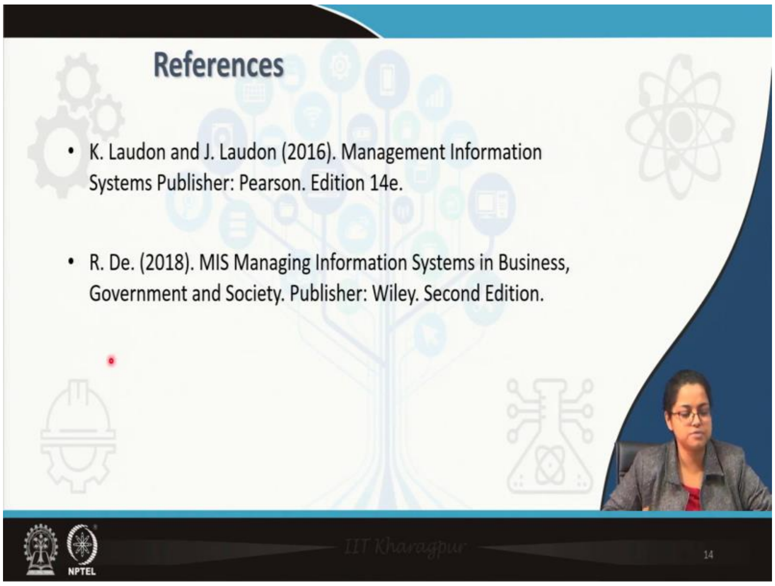
Now, the critique to this is if customers if employee's sorry employees constantly know that they are being monitored as we mentioned in the previous slide. Here, it leads to lower trust in the workforce, see I am doing my best in my job as an employee.

But, if I am monitored I might think that my employer does not trust me it would lower my confidence and in turn lead to lower productivity, I may try to resent my employer and my productivity will come down I may deliberately, there are a lot of employees who may actually deliberately reduce their productivity. They may try if I am being monitored, I will spend less and less time in at on my at my work desk and more and more time in the tea break.

So, there this is a very important ethical issue which is enhanced or amplified by the arrival of information technology and information system and technology; right. So, today we have discussed, we began with privacy ways and means to control, to prevent privacy issues.

Then, we moved on to piracy and copyright infringement. And saw how you know intellectual property rights infringement can be handled. In the digital world and finally, we spoke about workplace monitoring with the help of technology and how they can create problems or ethical issues within organizations.

(Refer Slide Time: 32:15)



References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.
- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

IIT Kharagpur
NPTEL
14

So, with that we come to the end of this particular lecture. And in the next session, we will be talking about security issues which are very-very critical in information systems today. And we will try to see how they can be handled and taken care of.

Thank you!