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

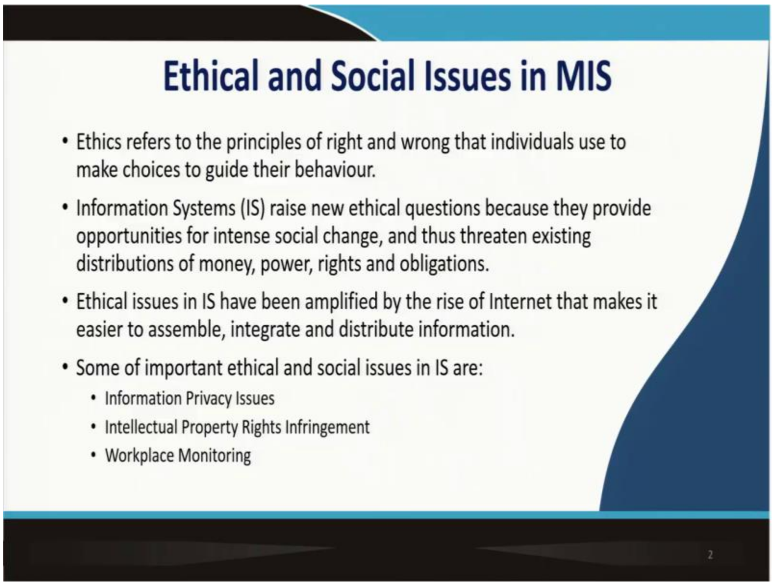
Module – 11
Ethical, Social and Security issues in MIS
Lecture – 51
Ethical and Social Issues in MIS – I

Hello, welcome back! Hope all of you are doing good and hope you have gone through the previous modules. So, today we are in the 11th module. So, in this particular module, we are going to talk about 'Ethical, Social and Security issues' in the world of information system or MIS.

So, you would of course, you know have realized that with the arrival of information system there has been an increase in the number of ethical issues that we that prevail in the world around us. So, there are issues related to privacy, there are issues related to you know copyright infringement or piracy and there are other multiple issues that the world of information system has brought along with it. Along with that we also have a lot of security issues.

So, in this particular module, we will be focusing on ethical issues, some social issues which are intertwined with the ethical issues. And of course, we will be focusing a lot on security issues that become extremely crucial in the world of information systems.

(Refer Slide Time: 01:29)



Ethical and Social Issues in MIS

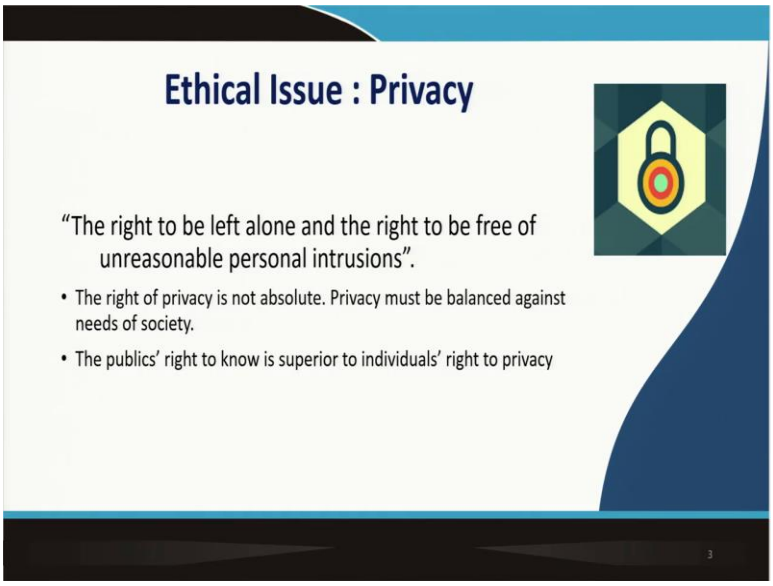
- Ethics refers to the principles of right and wrong that individuals use to make choices to guide their behaviour.
- Information Systems (IS) raise new ethical questions because they provide opportunities for intense social change, and thus threaten existing distributions of money, power, rights and obligations.
- Ethical issues in IS have been amplified by the rise of Internet that makes it easier to assemble, integrate and distribute information.
- Some of important ethical and social issues in IS are:
  - Information Privacy Issues
  - Intellectual Property Rights Infringement
  - Workplace Monitoring

So, moving on in this particular lecture we will be talking about the ethical and social issues in MIS. Ethics refers to the principles of right and wrong that individuals use to make choices to guide their behaviour. Information systems raise new ethical questions because they provide opportunities for intense social change and thus threaten the existing you know distributions of money, power, rights and obligations.

Ethical issues in information systems have been amplified or have increased manifold by the arrival of internet; that makes it easier to assemble, integrate and distribute information. Now, some of the very important and critical ethical and social issues that we will discuss about today are information privacy issues, intellectual property rights infringement issues and workplace monitoring issues.

So, all of these three issues are very crucial in the world of information system and need to be discussed or need to be understood to the fullest to be able to do justice in the world of information system right. So, moving ahead.

(Refer Slide Time: 02:46)



Ethical Issue : Privacy

"The right to be left alone and the right to be free of unreasonable personal intrusions".

- The right of privacy is not absolute. Privacy must be balanced against needs of society.
- The publics' right to know is superior to individuals' right to privacy

Ethical issue: Privacy, the first issue that we will talk about today is related to privacy. So, what is the formal definition of privacy? Privacy is the right to be left alone and the right to be free of unreasonable personal intrusions. Having said that, privacy comes with its own disclaimers, the right of privacy is not absolute and privacy must be balanced against the needs of the society.

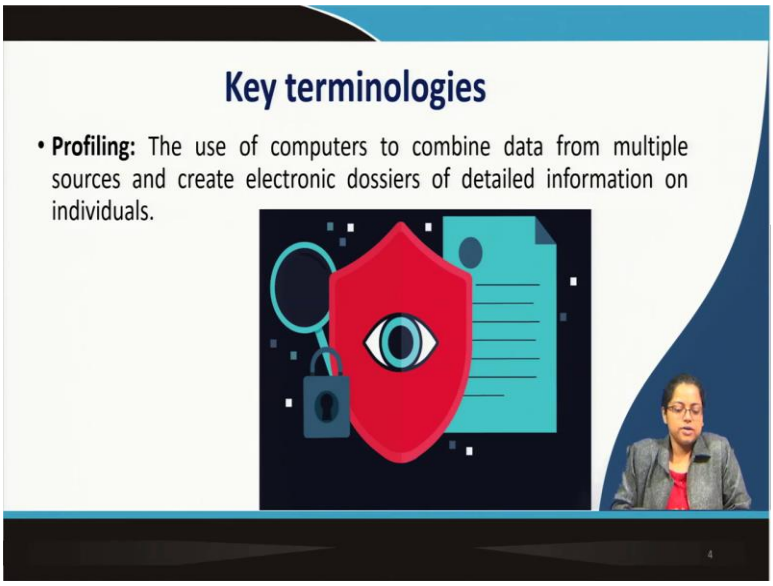
So, though privacy refers to the right to be left alone and the right to be free from unreasonable personal intrusions it the right to privacy is not absolute. And if the society requires you know your privacy could be at stake because if the needs of the society are more than your privacy then of course, there will be greater weightage given to the needs of the society.

So, there must be some sort of a balance between privacy and needs of society. If the society needs to know something very private or confidential about you for the overall good of the society, then of course, that prevails over your privacy.

The public's right to know is superior to the individual's right to privacy. This is again very important because the public's right to know is much more superior to an individual's right to privacy.

Therefore, you know in case an individual deserves privacy, but public's right to know is much more critical, the individual may not have his privacy in that context.

(Refer Slide Time: 04:36)



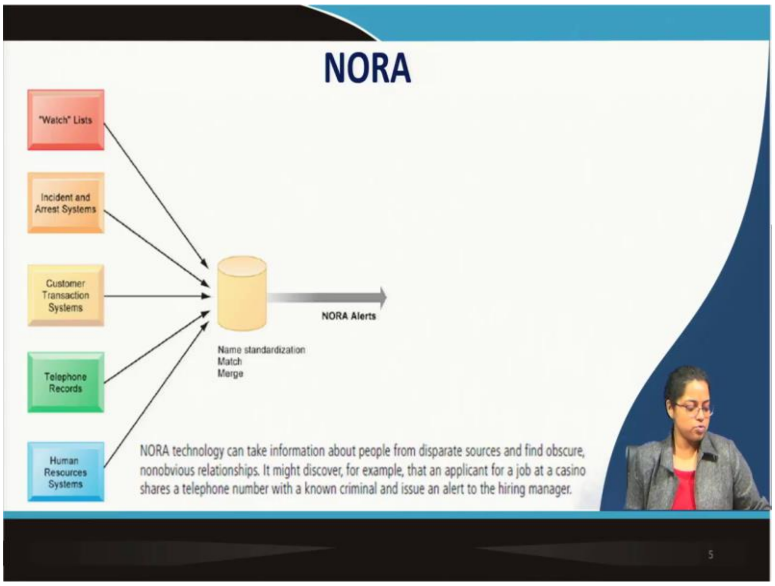
Key terminologies

- **Profiling:** The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals.

So, now moving on there are certain key terminologies which we would want to discuss with respect to privacy. Profiling, the use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals.

So, profiling refers to the technique in which information technology or system is used to combine data from multiple disparate data sources and create an electronic dossier of detailed information that could actually be related to one particular individual.

(Refer Slide Time: 05:14)



NORA

NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

With that we come to another very interesting and important concept called NORA. So, what is NORA? So, here you see there are you know multiple databases, there are watch lists, incident and arrest systems, customer transaction systems, telephone records and human resources systems.

So, what NORA does is, NORA, the NORA the term NORA stands for Non Obvious Relationship Awareness. NORA technology can take information from about people from disparate sources as we have just mentioned in the previous slide and find obscure non obvious relationships.

So, very important, it does not find relationships that are obvious, it finds relationships that are hidden somewhere and which are absolutely non obvious. So, that is why that explains why NORA is a very unique technology. So, NORA technology can take information about people from disparate sources.

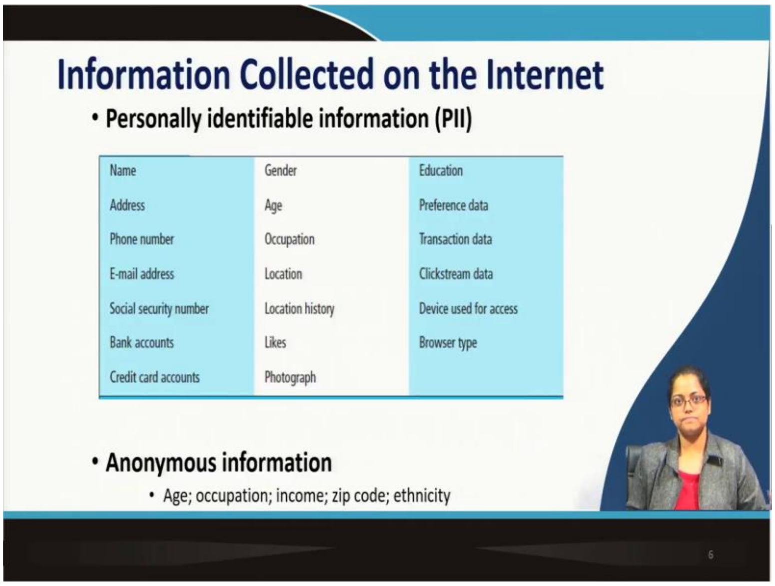
So, here we have disparate sources; a watch list, an incident and arrest system, a customer transaction system, telephone records, human resource system these are all disparate systems. So, NORA technology collects data from multiple disparate sources and finds hidden non obvious relationships which would have been very difficult to find out without this particular technology.

So, what NORA does is, it does name standardization, matching and merging to come up with what is called NORA alert, out of data from all of these disparate data sources. So, an example. So, NORA technology might discover for example, that an applicant for a job at a casino, shares a telephone number with a known criminal and issue an alert to the hiring manager.

So, this is so, not obvious right. So, an a person might have casually applied to a particular job at a casino, but NORA technology will find out that this particular applicant shares a telephone number with a known criminal and would issue an alert to the hiring manager which is a NORA alert.

So, now you see what, how NORA technology can intrude into somebody’s private world because of a greater good that is good of the society right. So, this is what NORA technology is all about.

(Refer Slide Time: 07:48)



Information Collected on the Internet

- Personally identifiable information (PII)

Name
Address
Phone number
E-mail address
Social security number
Bank accounts
Credit card accounts

Gender
Age
Occupation
Location
Location history
Likes
Photograph

Education
Preference data
Transaction data
Clickstream data
Device used for access
Browser type

- Anonymous information
  - Age; occupation; income; zip code; ethnicity

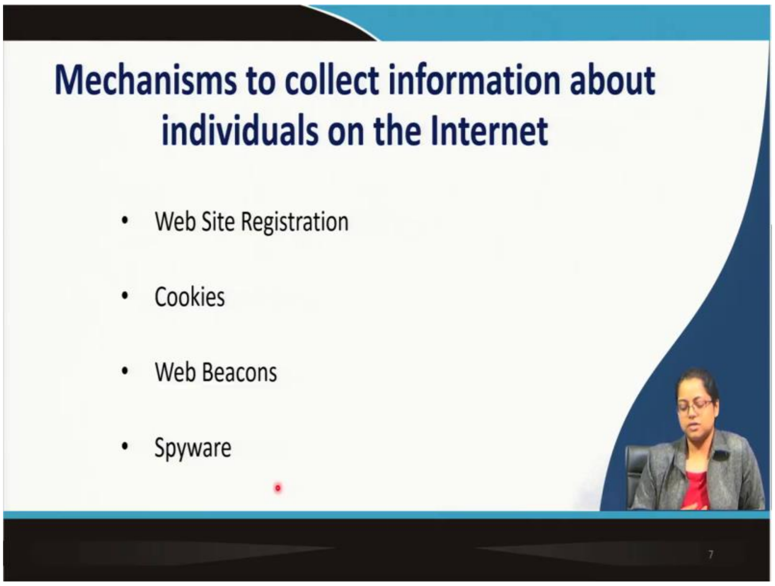
So, moving on, let us talk about information collected on the internet. So, on the internet information can be collected from you know through multiple methods or modes and the information that is collected could be categorized into two groups. Personally identifiable information, that we see here personally identifiable information and then anonymous information.

So, personally identifiable information is that which can be used to pinpoint at a particular individual. For example, somebody’s address, email address, phone number which are very unique to every individual, social security number in the US context. In Indian context we have something called an Aadhaar number which is a very unique number, bank accounts, credit card accounts, you know photographs, click stream data which is again very unique, transaction data.

So, all of these are unique personally identifiable information. And also some information for example, gender, age, occupation are not personally identifiable information in isolation, but when clubbed with some others such as name, address etcetera or phone number they become personally identifiable information.

So, two people may have the same name, but it is very unlikely that two people of the same age, living in the same location and belonging to the same gender have the same name right. So, you understand what I mean. And then anonymous information, of course, age, occupation, income, zip code, ethnicity all of these are individually anonymous information.

(Refer Slide Time: 09:36)



Mechanisms to collect information about individuals on the Internet

- Web Site Registration
- Cookies
- Web Beacons
- Spyware

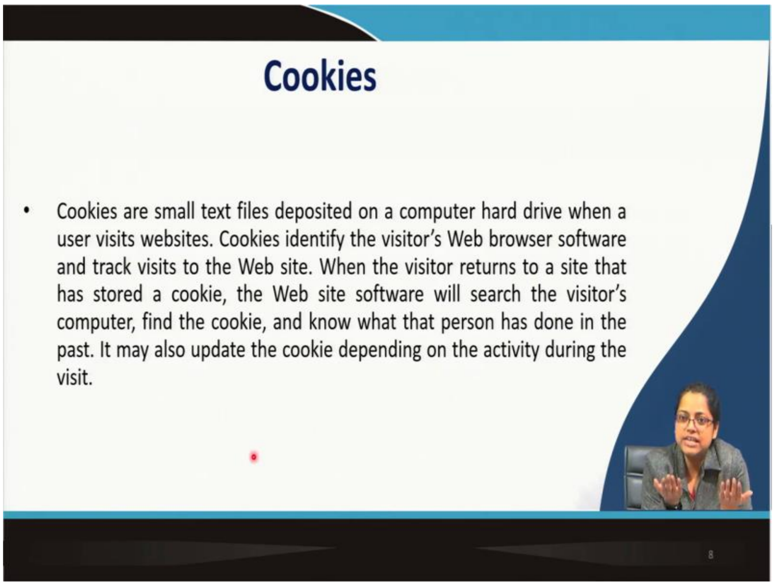
Now moving on, mechanisms to collect information about individuals on the internet. So, there are multiple mechanisms we will discuss some of those.

Website registration is of course, the most simple and the most straightforward way of collecting information about individuals on the internet. So, when people register they will willingly reveal some of their information which can be utilized by companies for their benefit to for the benefit of the individual as well of the customer as well as for the company.

So, in terms of customers benefit using webs information collected from the website or from a person’s visit on the on a particular website, the website can give appropriate recommendation and personalization and at the same time that will would in turn be beneficial to the company in getting more sales, in getting more people on more traffic on board.

The next method cookies, we will discuss in detail, web beacons and spyware. So, we will discuss three of these three technologies in detail going ahead.

(Refer Slide Time: 10:47)



Cookies

- Cookies are small text files deposited on a computer hard drive when a user visits websites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie depending on the activity during the visit.

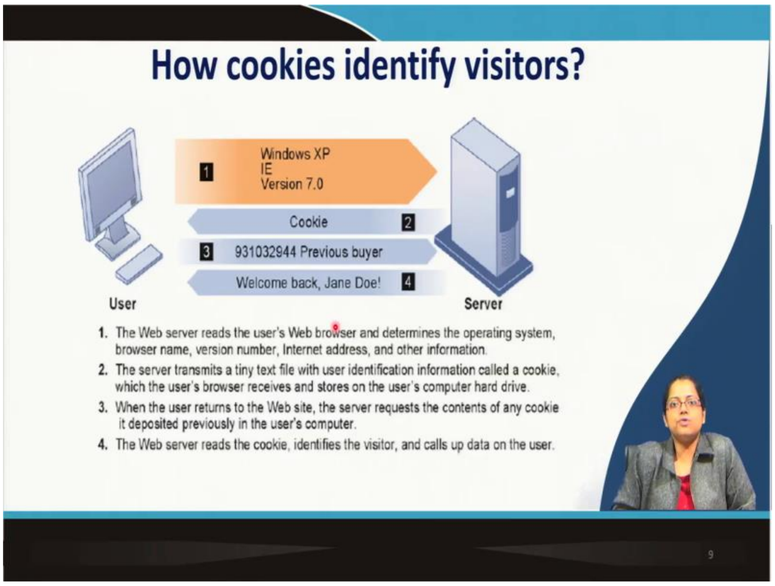
Cookies: Cookies are small text files deposited on a computer hardware when a user visits a website. Cookies identify the visit, so, I am sure all of you have heard of cookies. But, if I were to ask you what a cookie is technically, would you be able to explain this concept to me and that is why I thought it is very important to discuss what technically a cookie is and how it collects your information on the internet.

So, that going ahead you would be able to understand how it collects information and if required you would be able to prevent a cookie from collecting your information. So, cookies are small text files deposited on a computer hard drive when a user visits websites.

Cookies identify the visitor’s web browser software and track visits to the website. When the visitor returns to a site that has stored a cookie, the website software will search the visitor’s computer, find the cookie and know that the person has done what the person has done in the past. And if you if the cookie knows what the person has done in the past the cookie can take it up from there, the website can actually take it up from there.

So, it may also update the cookie depending on the activity during the visit. So, during this visit the activity may be updated again, so, that in future visits again we have the updated cookie passing on more recent and relevant information.

(Refer Slide Time: 12:20)



How cookies identify visitors?

1 Windows XP
IE
Version 7.0

Cookie 2

3 931032944 Previous buyer

Welcome back, Jane Doe! 4

User

Server

1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

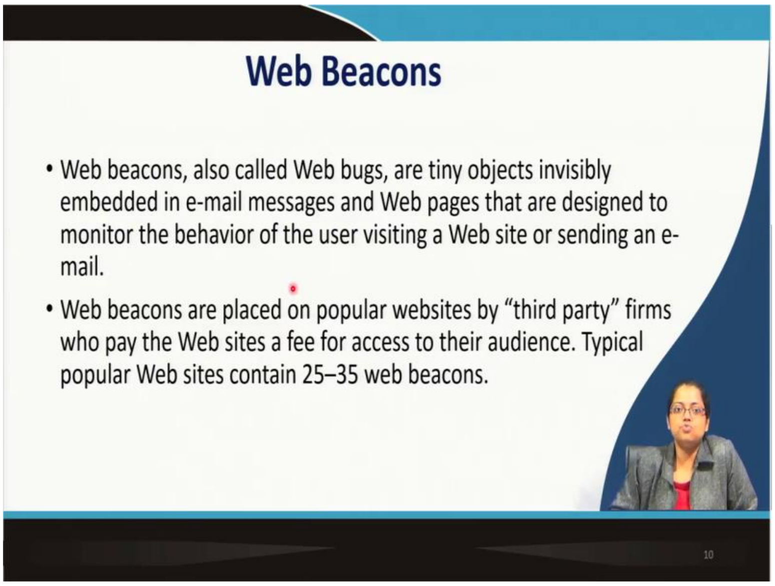
Now, moving on, how do cookies identify visitors? So, this graphic explains more or less what I would want to talk about in these four points, but again let me highlight what these four points mention. The web server reads the users web browser and determines the operating system, browser name, version number, internet address and other information.

The server transmits a tiny text file with user identification information called a cookie which the user's browser receives and stores on the user's computer hard drive. When a user returns to the website the server requests the content. So, you can see this is the first step, this is the second, third.

So, when the user returns to the website the server request the content of any cookie that it deposited previously in the user's computer. And once that information is there and it is obtained by the server, the web server reads the cookie and identifies the visitor and calls up data on the user and the web server takes it up from there.

So, welcome back Jane Doe right. So, by this by using the cookie you would be able to identify the name of the person and other details of his browsing behaviour if it stored in the cookie right. So, moving on.

(Refer Slide Time: 13:47)



Web Beacons

- Web beacons, also called Web bugs, are tiny objects invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending an e-mail.
- Web beacons are placed on popular websites by "third party" firms who pay the Web sites a fee for access to their audience. Typical popular Web sites contain 25–35 web beacons.

Cookies are very simple and if you understand them you will have obviously, you know there are certain ways to prevent cookies from collecting your personal information and we will discuss those subsequently. The next you know topic that I want to discuss about here pertains to web beacons.

So, what are web beacons? Web beacons also called web bugs are tiny objects invisibly embedded in email messages and web pages that are designed to monitor the behaviour of the user visiting a website or sending an email. So, these are also called web bugs and these are tiny objects that are invisibly embedded in email messages or web pages which are designed to monitor the behaviour of user visiting a website or sending an email.

So, you understand how web beacons would be able to collect your information and pass it on to a third party. So, for example, you are browsing on Amazon or you are browsing a popular website right. So, web beacons are placed on these popular websites by third party firms, which specialize in this particular technology web beacon technology. And these firms third parties actually pay the websites a fee the popular websites have fee for access to their audience.

So, a web beacons are placed on popular websites by third party firms who pay a fee to the website for access to their audience. So, if you are browsing a very popular website you would not even be sure of the fact that there are web beacons hidden in that particular website.

And your browsing history is being shared with a third party this third party is actually paying that popular website for collecting your information. But this is a very crude way of collecting information and an unethical way of collecting information, but nonetheless web beacons are meant for that particular purpose.

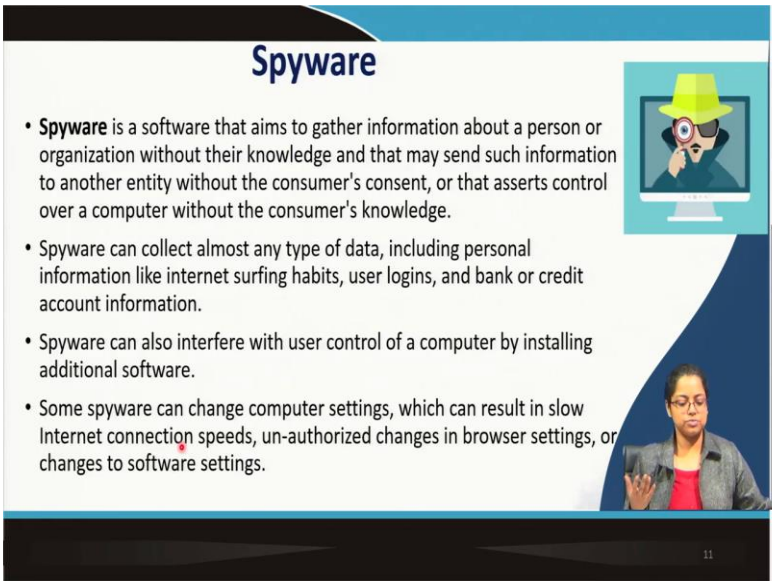
Now, with the arrival of a lot of laws pertaining to privacy such as the fair information practices which is a very important law by in the by the Government of United States, the GDPR which is the General Data Protection Regulation in the European Union. So, these actually these laws prohibit the collection of data by third parties without consent by the individual without the customers consent.

So, now, only once the customer gives his or her consent the web beacons can collect information. But you know there are countries there are geographies where we have a long way to go and there are no laws as such to implement there are there are very few laws as such actually or may be few to none to implement these you know strict measures in for collection of customer data or information.

Now, this is a very very important fact here typical popular websites contain around 25 to 35 web beacons. So, you may not even be aware you are browsing a very popular website and you are content that since the website is popular your information will not be shared with the third party without your consent.

However, there are certain around 25 to 35 web beacons that are planted in these particular websites which collect information about you and share your information to third parties and you are not even aware right.

(Refer Slide Time: 17:42)



Spyware

- **Spyware** is a software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- Spyware can collect almost any type of data, including personal information like internet surfing habits, user logins, and bank or credit account information.
- Spyware can also interfere with user control of a computer by installing additional software.
- Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings.

So, web beacons that is about web beacons, cookies, then web beacons and then we will move on to the fourth technology which is used to collect you know information customer information. So, the fourth technology that collects customer information is spyware. What is a spyware?

Spyware is a software that aims to gather information about a person or an organization without their consent again unethically or illegally. And that may send such information to another entity without the consumers consent or that asserts control over a computer again without a consumers concern.

So, spyware is a software which could be embedded you know in any website or it could be embedded in with your email, it would not only gather information about individuals, it could also assert control over your computer without your knowledge. So, spywares are also very malicious in their nature and as the name suggests spyware can collect almost any type of data including personal information like internet surfing habits, user logins and bank or credit card account credit account information.

So, spywares are you know very malicious and they can collect a lot of information from you including personal information like you know. So, a lot of personal information collected from you without your consent you know information internet surfing habits still user logins bank or credit card information which is so, critical for you such information can also be collected by spyware and they can be sold to third party.

So, imagine your bank information or your credit card information now is stolen without your consent and it is given to a third party. So, you can imagine if the third party gets into your bank account and can transacts you can imagine what will happen right. Credit card information again if credit card information it gets leaked to a third party you know what happens right. So, spywares are very malicious spyware can also interfere with the control of a computer by installing additional software.

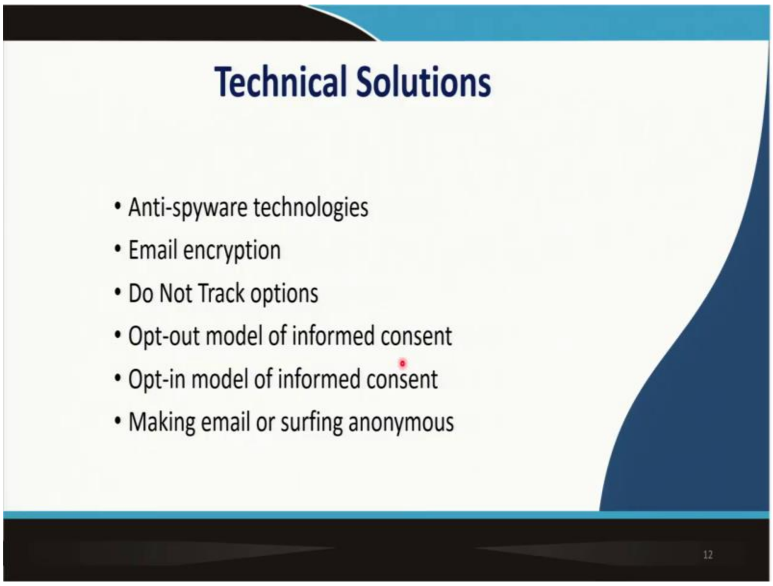
So, spyware are a step ahead of web beacons; because they can interfere with the user control of a computer also by installing additional software they not only collect information, they also tamper or tamper with the control of your computer. Some spyware can change computer settings which can result in slow internet connection speeds, unauthorized changes in browser settings or changes to software settings.

So, spywares can take control over your computer they can change your computer settings, they can make your internet connection speed slow, they can make unauthorized changes to your browsers, changes to software. So, spyware can once they are into your system they can you know you are browsing a website happily, but if they come into your system without your knowledge they can wreak havoc.

They can steal data, they can they can sell data to third parties data that they collect from you, they can also gain control over your computer at the same time they can gain control over critical documents that you might have stored in your computer and they can you know they can they can even charge a ransom. So, if spyware is actually intertwined with the ransomware, they can take control over your computer your data and they can charge a ransom to actually release control over that data.

So, all of these technologies from cookies to the web beacons to the spyware, cookies are more or less you know they are we are all aware that cookies are there and we have ways and means to stop them, but what will you do about web beacons and spyware? So, these are absolutely unethical ways of collecting customer information. Now these are the different ways through which data is collected from about you on the internet.

(Refer Slide Time: 21:49)



Technical Solutions

- Anti-spyware technologies
- Email encryption
- Do Not Track options
- Opt-out model of informed consent
- Opt-in model of informed consent
- Making email or surfing anonymous

12

So, let us talk about some solutions. Are there some solutions we know that our data is being collected what do we do about it right? As individuals as users as individuals or you know as individual users browsers of the internet what do we do about this? There are some technical solutions and also there are some legal solutions.

So, the legal solutions we will discuss in the next lecture, but in this lecture we will let us talk about some of the technical solutions. So, anti spyware technologies there are certain anti spyware technologies available. So, these technologies could actually play a very important role in protecting your system against spyware.

So, spywares are absolutely malicious I have been highlighting this point time and again. So, anti spyware technologies could actually help you in protecting your system against some of these spywares.

Email encryption. So, email encryption is another technical solution using which you can actually encrypt your email which is being sent to a particular recipient. So, that the email is not you know intercepted during the transit and the email is your private email which you have sent to somebody should not be intercepted and should not be tampered with red or even you know tampered with, manipulated, deleted or even read.

So, none of these should happen to your email. So, email encryption technique is a technique through which your email is encrypted and is converted to a form which can be considered it is the term for that encrypted email is a cipher. So, that cipher can be transmitted to the recipient and once it reaches the recipient, the encryption software there would again decrypt the cipher to get the original email.

So, in transit the email the flows is of the form of a cipher and it cannot be deciphered by somebody who is not aware of the encryption technology at the back end. So, encryption is another way in which you can make your systems more secure and at the same time maintain the privacy of information that you are sharing. Do not track option this is another option that is available in all browsers.

So, if you are using you know say internet explorer or you are using you know Mozilla or you are using any Google chrome, any Browser that you are using do not track option is a very important feature. So, you can actually use this particular option to. So, this will give this as a your browser will have the feature once you enable it or check it.

You when you visit a particular website the website will be made will be alerted that you do not want the website to use cookies to collect your information. But having said that it again depends on the website because despite the fact that you have a do not track option enabled there, the website might still be unethical enough to collect your information.

So, you have do not track option at your control it is within your control. So, within your purview. So, if you want that the website should not collect information about you through your behaviour online through cookies you can actually enable it, but then again it is up to the up to the website where whether it respects this do not track option of yours or not.

Now coming to opt out model of informed consent versus opt in model of informed consent these two are very important. So, these two models of informed consent mean that the first one that is opt out option of informed content means that information is by default collected from individuals, when they are browsing the internet.

But if the individual does not want so, the advertisers to collect their information by default, they should actually go and take some explicit action to prevent say do not track option or some other you know encrypt their you know transactions or their messages or use some other technology explicitly to prevent the advertisers from collecting information.

But by default the advertisers would be collecting information about individuals once they are browsing the internet. On the contrary opt in model of information informed consent may refers to the fact that by default advertisers will not be collecting information from an individual once the individual browses the internet.

But if the individual wants the individual can explicitly go and check a feature which will give the advertiser the permission to collect his or her information while he or she is browsing. So, opt in model of informed consent.

So, lot of critiques say that opt in model of informed consent is a better option; because you here you are taking into by default you are not collecting information from your customer, but only if your customer is willing your customer can give you the permission to collect his or her information online.

So, it is a much more ethical way of dealing of treating your customer and that is today we would see most of the websites give you a pop up when you try to browse them asking you whether you give them the permission to collect your collect and use your their your information or not.

So, that is the opt in model of informed consent coming into play versus earlier where we had more of opt out model wherein, by default information was collected about us when we were browsing the internet. But only if we were careful enough to explicitly go and prevent the take certain measures to prevent the advertisers to collect our information, we would have to take some explicit measures.

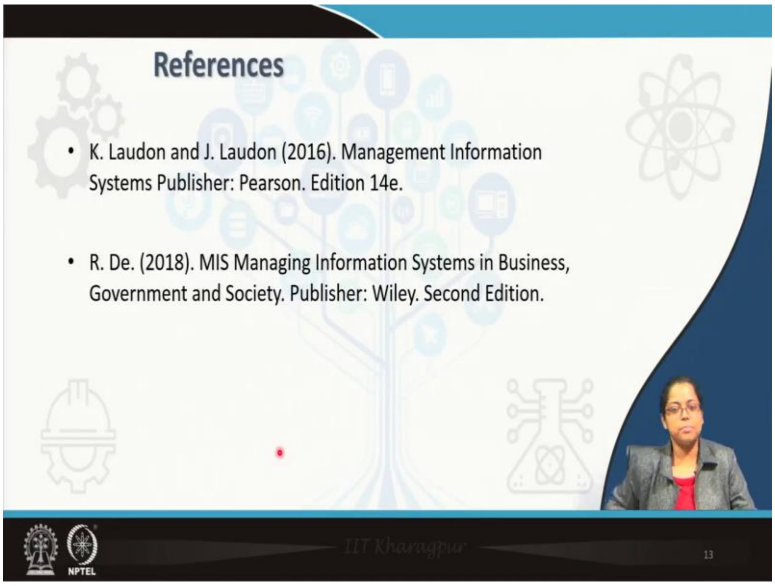
Only then we would be opted out otherwise by default our information would be collected by the advertisers and the information can be sold the information can be transferred the information can be given away to a third party right. And finally, making email or surfing anonymous.

So, that is another way in which you can make yourself absolutely secure and make your browsing very private. So, there are multiple ways to make your browsing or emailing anonymous. So, you can; you have the incognito mode in your browser which would make you anonymous when you are browsing, you can there is another there is a software called tor the onion router which is which is actually used to anonymize your internet browsing traditionally tor was used for mission critical research project.

So, all good purposes mission critical research projects very you know very high profile research, journalism for certain very you know very important military operations. So, for all of these tor browser was used to make the browsing anonymous. So, if you are actually concerned about your privacy, you could use some of these options to make your browsing behaviour anonymous on the internet.

So, these are some of the technologies that we would want to discuss. And these technologies would come in handy if you want to make your surfing or browsing anonymous on the internet and maintain your privacy on the internet. So, these are the technical solutions of course, as I mentioned there are certain legal solutions we would take those up in the next session.

(Refer Slide Time: 29:52)



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.

So, in the next session, we will talk about the legal solutions of privacy and then we will take up some other ethical and social issues and discuss how they can be handled.

Thank you!