Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 10
Lecture: 28

So, good afternoon and welcome back to Cybersecurity and Privacy course. So we have slowly moved from the cybersecurity space to information privacy space and well, we as we go we will observe that a lot of concepts are common but privacy seems to be a concern, right. Privacy is a concern as I presented yesterday, particularly information privacy concerns. Individuals and groups and organizations are concerned about their personal privacy as well as their information privacy. So how do you address that privacy concern? So a focus of cybersecurity is to address privacy concern. So how you address, how well you address, how badly you address, all that is part of the information privacy domain and therefore both are closely related and today as part of this, today's session we have a case for discussion and that case will show us how cybersecurity and information privacy are closely related.

And what should organizations do and what they should not do and that will highlight and also teach us lessons that as future managers, you should learn about cybersecurity

and privacy. So today's topic, with today I want to start discussion on the need for regulation, okay. So privacy exists at the individual level and it, when it becomes collective it becomes groups or organizations or industry, industry domains and then country, okay. So certain instances of breaches will teach lessons to government as to, if certain breaches can affect millions of people, okay then the government should be concerned.

it is not one individual who is affected but there is a pervasive effect of privacy breaches on individuals. So it also brings to light the fact that organizations are storing citizens data and role of government is the welfare of citizens . So therefore if the industry is not regulated then people's welfare will be affected. So that is the aspect that we will see in today's session as well as in today's case. So let us move on.

I hope we start with the old country song, Eagles fan here, in the of course, this is a song of the 70s and it got Grammy Award and in my college days, this used to be very popular. So when you walk through the rooms, you hear the song playing and it is sort of you know, it is a lovely song and it is a lovely, it talks about a lovely place called Hotel California, it is a lovely place. So you see the, how the lyrics end, you can check out anytime you like but you can never leave. In business or in management literature, we call this lock-in, right. There is something called lock-in, you lock into something, you enter there and once you enter, you cannot leave.

So you know many products and services are like that. So lock-in is a part of digital products management. You see, why you go to Amazon all the time or why you have your preferred bank, why you have your preferred mobile service provider. Because you are locked into it, you know. There is a switching cost, when you actually try to move from that service or that product to another, right.

So the switching cost is inhibitive or prohibits us from moving on and so is the world, the world, the world of the web or particularly the social media you are actually locked in there and even the social media platforms also do not want to actually let you go, okay. They will not let you go because your connections are so strong there. So oftentimes we are in Hotel California when we are in the, when we are in the digital world. Okay, we thought we could sign out anytime but we are not able to sign out . So lock-in is built into the business strategy of platforms, large number of participants and participation is a important part of building any digital platform.

You look at Facebook or you look at any of, not just social media, even operating systems. Okay, you find it difficult to change from one OS to the other, it is a lock-in strategy. So therefore certain information that you have disclosed about yourself and certain

connections that you have made, it is forever. So there is a, so you can choose not to go there, you can choose to be anonymous. I know I have friends particularly in Germany who do not use any social media.

One of my colleagues in Information Systems with whom I collaborate, does not have a WhatsApp, does not have any of the social media use at all or accounts at all, that is one choice that you make. You do not want these services, you can opt out of email as a whole. You do not need to have your cell phones also. You can still be alive and live, right. We have lived that life also, you know for several decades.

So all these are actually necessities that is, you know created for you and you actually get in there, choice is yours, okay. Whether you want to share your data to get a service, whether you want to give your search key to Google or not, is your choice. Once you give your search key, Google knows what you are searching for and it is linked to you, what you are actually looking for, and that is your choice. So what you search for, is a part of your profile. So therefore disclosure is left to the individual as this cartoon shows.

I like privacy but it makes it difficult to enjoy life, right. We can still be alive but we cannot have a life, right. That is what, that is how businesses define life for us or very shrewd entrepreneurs have thought through what your needs are and created systems for that and created exchanges for that purpose. Well, yesterday I talked about one of the matrimonial sites, okay that is where you share a lot of personal data and have you ever read this fine print of a privacy clause, the clauses in the privacy statement which you clicked. I agree you have to, of course press that radio button and it is a long statement, okay.

So if you read the fine print, it will read like this, With respect to content you submit or make available for inclusion on publicly accessible areas of the site including but not limited to your contact details, you hereby unconditionally and irrevocably grant to Shaadi, the license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such content on the site and Shaadi.com center members from time to time. This is sort of perpetual agreement with them that you clicked, I agree you did not pay them anything, right. What you give them is what, it is a exchange, where you give your data and they give you service. Gmail is free but in business you learn there is nothing free.

There is no free lunch, somebody pays. So sometimes these exchanges are not monetary, right this is you know, non-monetary exchanges is a part of digital platforms. So that is why we saw yesterday that it is difficult to challenge or difficult to win a case of data exchange with corporations in the court because you have agreed. Legally you have agreed to the clauses and they have evidence for it. But the other side of it is, you know it is like,

well they have made all that statement in a long privacy legal document which you do not have the time to read, one because you have some need to gratify, you know economists call it immediate gratification, you know, you are looking for some service and you are in a hurry.

You want to connect with someone, you want to, you know my friend has it. I also need to have it. Who cares, what is privacy statement ? Click, then you went on. So nobody has time, immediate gratification and that is something that is exploited by platforms. They know that you will agree and a study by Luca and Bazerman, both are faculty in Harvard Business School and they recently brought out a book on online experiments which I read.

So I came across this facts which they present, takes 76 working days to read and understand, a typical privacy policy. So you may read some of it but you will not understand because it is legal language and you are not a legal expert. So there it is a technical language which is difficult. And number one and therefore you have no choice. If you want the service you just agree.

It is by design like this. This is an issue which is one sided, you know privacy agreements are sort of one sided documents. Regulation is trying to accept it because it is not a fair play. A user has to agree without understanding what it means. And of course, that is a need but it is not fair, there is a issue of fairness here.

That is why somewhere there is a need for regulation and when we discuss GDPR as we go, we will say GDPR actually tries to address this issue of, you know unfair exchange of information. And these scholars also found that they report a number of online experiments platforms too. When you actually sign into your Facebook account, you are a participant in their experiments almost every day. They are actually testing out, which where you go, which profiles you spend time on or which advertisements you respond to etc. They are constantly observing but actually in experiments or in any research which involve human subjects, they are supposed to take your consent to participate in an experiment or a survey.

It should be an informed consent process but they do not. And again there are legal safeguards in their favour, for example in experiments if you actually tell you, it is an experiment then the purpose of experiment can be defeated. Now this is one side of privacy and the legal safeguards for privacy etc. But on the user side okay, you see there is absence of regulation or regulation is still evolving and you also see that it is in favour of corporations to actually exploit certain, certain needs or desires of individuals which they can actually exploit using these platforms. So there is a question of fairness there but

on the other side very few people, very few people want to be let alone.

Privacy is the right to be let alone but actually you do not want to be let alone, you want others to know about us. You know that is the sort of, yeah that says that is a social need, the need to socialize and that social life is moved from physical to virtual, you know that is what we see but the need to socialize is basically human need. And they, so human beings also want to make selective disclosure. What is your Facebook profile, what is my Facebook profile, do people know about what I am really, do I disclose that, you know you have a selective disclosure, and that is to make an impression or a statement about yourself, you want, what you want to be, right. And so the platforms have to be designed in such a way that it fulfill your need to define yourself in a way that you want to do it and in that need, in that sort of strong desire, you actually end up disclosing a lot of information about yourself.

So the another scenario is you know, you when you go for buying things, be it online or be physical stores, there are loyalty programs. So today you do not need a loyalty card, you just need to give your cell phone number, That is your primary key, you know against which, you know they insist often that you share your phone number with the retailer but is it mandatory? I do not. I stop sharing. I said No, I do not have a phone number. So then you still can buy but sharing that number is up to you.

The moment you share that number, next time when you go they are actually keeping track of what you buy. So buyer's behaviour, your preferences, all that constitute your profile. Now if you have a loyalty card or a, you are a member of a loyalty program, say of Titan, for example where I am a member. So they actually accumulate certain loyalty points for you and then you get some discount or you know you get some money back and so you have signed in, wherein you have disclosed your information. Sometimes Adhar number, sometimes phone number and some basic descriptive data about yourself.

But who compels you. There is no compulsion. Can you, it is a request. You sign in, Why you sign in? Because you get some benefits and all benefits, some comes at a cost. The cost is, they are actually monitoring what you buy. So there is data about you that is involved in any loyalty program.

You get bribed to share your data, the discounts that they gave or the benefits that you get is a small remuneration for letting them know you. One is they are able to offer you services in a targeted way. In the sense, they understand your preferences and recommend products for you. The other is, data has a monetary value and they can actually sell your data. So many retailers in the United States, I have read, make more money from data than from their products.

So we agree because we need service. They use your data, make money out of it but when you get to see that, in the moment you are affected by the trade of data, then you raise privacy concerns. Otherwise you do not have a concern. So this is known as privacy paradox. People want both. You want both, you want to experience service, you want the best email experience from Gmail and they you want them to give it free to you which obviously cannot happen.

They want to share what you write with advertisers. They want to make their money. So an individual may not be reading your emails but the text is scanned to understand what you are actually writing, you know. A lot of analysis is possible with emails.

So they make their money with your data. You want service. So it is a, it is designed an exchange and therefore there is a paradox. It is conflicting to claim privacy when you are actually getting something using your data from a service provider. So to sum up, personal experience and privacy, these are conflicting needs. You want the best personal experience in online services.

At the same time, you also want privacy which is not possible, okay. If you have to take something from the top, you raise your hand, something falls off, right. So this is known as privacy paradox. Now can this paradox be resolved? No, that is a difficult question. So you give your, share your identity and you get certain privileges and it is your choice.

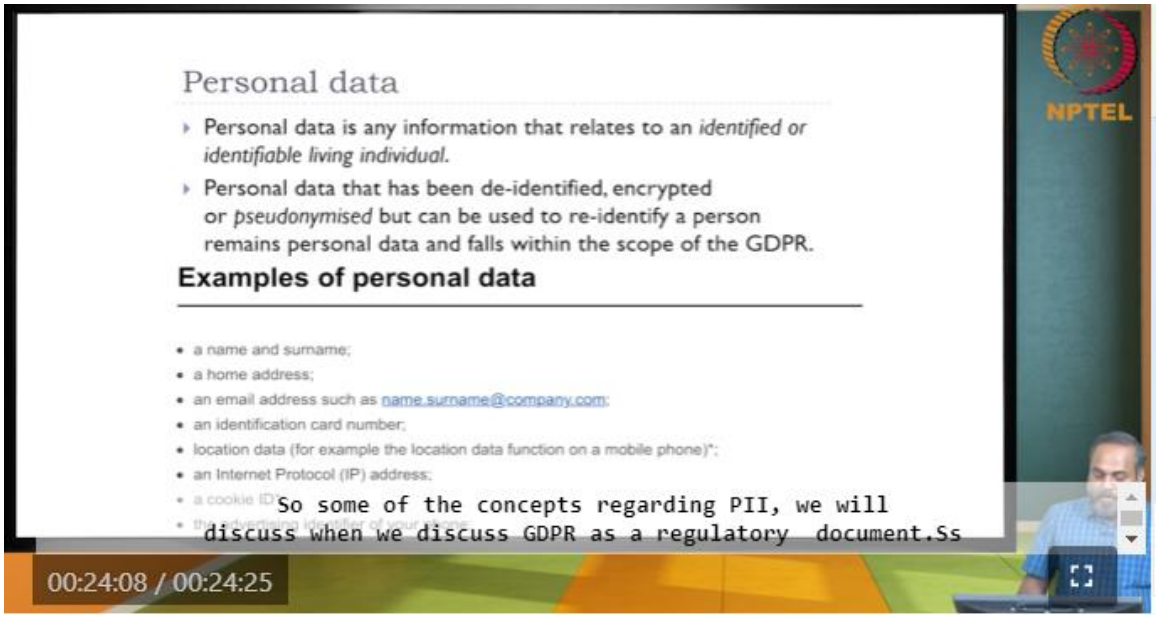
It is your decision whether you want the service or not. But what is worse is when it comes to government, when you are citizen of a country there are certain mandatory disclosures that government will require and government's point of view will be that in order to secure you in a country, we need to know you, and therefore you cannot completely hide yourself anywhere in the world. And that is what Derek Smith, CEO of Choice Point said when his company, today we are going to discuss another case which is similar to Choice Point, a credit bureau whose data breach happened in 2005. Today's case is about 2017. This was way back in 2005 which actually again brought the issue of privacy into public debate and into policy making, into regulation, everything.

So Derek Smith was under fire that time and he said and many people started criticizing the industry itself. This credit bureau or organizations which collect, process, profile and sell information about individuals, which corporations need for credentialing and many other purposes but the industry itself is fake or not fake industry itself is illegitimate because they are storing individuals information and they are not able to protect it. And so individual identities should be kept anonymous was a argument and to which Derek Smith responded, you have a right to privacy but in this society we can have a right to

anonymity. Right to privacy and right to anonymity are two different things. You have a right to privacy but you cannot be anonymous in a planet.

You have to belong to some country, right. That is how we have defined our territory. We have defined territories. In the colonial era, the British try to make most of the world theirs. But still, then it is you belong to one of the colonies. So you have some identity, you identify with some territory and that is how, that is how humanity exists in the world and therefore you cannot be anonymous anywhere.

For yourself to be affiliated and to enjoy the privileges of being a part of a country, right . You enjoy a lot of privileges when you belong to a country, when you belong to an organization but if you have to get that, you have to say who you are and some basic information needs to be with the government. So that is, that that is the other side.



We fail to see that sometimes. Now Right to Anonymity. So what is anonymity? So we need to have clear clarity about some of these concepts. What is privacy and what is anonymity, okay? So okay, let me not put that question to you. So before going into defining or understanding these concepts of privacy and anonymity and secrecy and so on, let us also understand what is personal data and personally identifiable data, okay or personally identifiable information? PII, often it is called. Personal data is any data that is related to you which is yours. Okay, your name, your age, your place of birth, your address, your cell phone, all this is personal data.

Okay and personally identifiable data is data that is able to uniquely identify, okay. You must have discussed this in databases, right. There are certain attributes that uniquely identify, right not all attributes. Like your name is not a unique identifier, but your name, when you actually combine certain attributes, it can become a unique identifier. So such identifiers which are not uniquely identifiable are sometimes called quasi identifiers.

Your name is a quasi identifier but you give your age, give your address, okay when you link all this, it can you know, almost distinctly, almost, not may not be 100 percent, distinctly identify you. So there are algorithms to identify people from whatever data is disclosed, you know by linking. So identifiable data, so email, cell phone etc are very much identifiable data we have seen this right. So the data points or the attributes that has the potential to uniquely identify you or partly identify you, they are identifiable data. So some of the concepts regarding PII, we will discuss when we discuss GDPR as a regulatory document.