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: 9
Lecture: 26

There is an economic view of privacy. When economists look at privacy, they do not care much as Posner in 1975 said, Privacy is not important so long as there is no economic consequence. Does privacy have economic consequence? Any quick answer? Yes sir, means if there is any data leakage or personal information of a particular organization, then it will impact the entire organization. Absolutely right. So organizations collect and store a lot of personal information. The leakage of that actually incurs liability, therefore there is economic consequence there.

Identity theft is, may have economic consequence. So there is economic consequence of privacy and we have one session dedicated to this, the economics of privacy in as we go. So you have pointers already. Then there is post after economic view, there is a feminist view, I am actually referring to Stanford Encyclopedia of Philosophy and their discussion on privacy to give you an overview.

So feminist would see this private space not very positively. Their argument is that defining, say family as a very private space where nobody else can enter, no mediator can enter or nobody can listen or overhear etc, actually is in the favour of man but not women because in many communities women are very vulnerable and there is lot of women abuse. And if there is no guardian, there is no guardian, sort of third person it can lead to violence and abuse of women and therefore strict private boundary for privacy is not in favor of females. That is one argument. Now let us actually move slowly from Privacy, the concept of Privacy to Information Privacy which is our focus area.

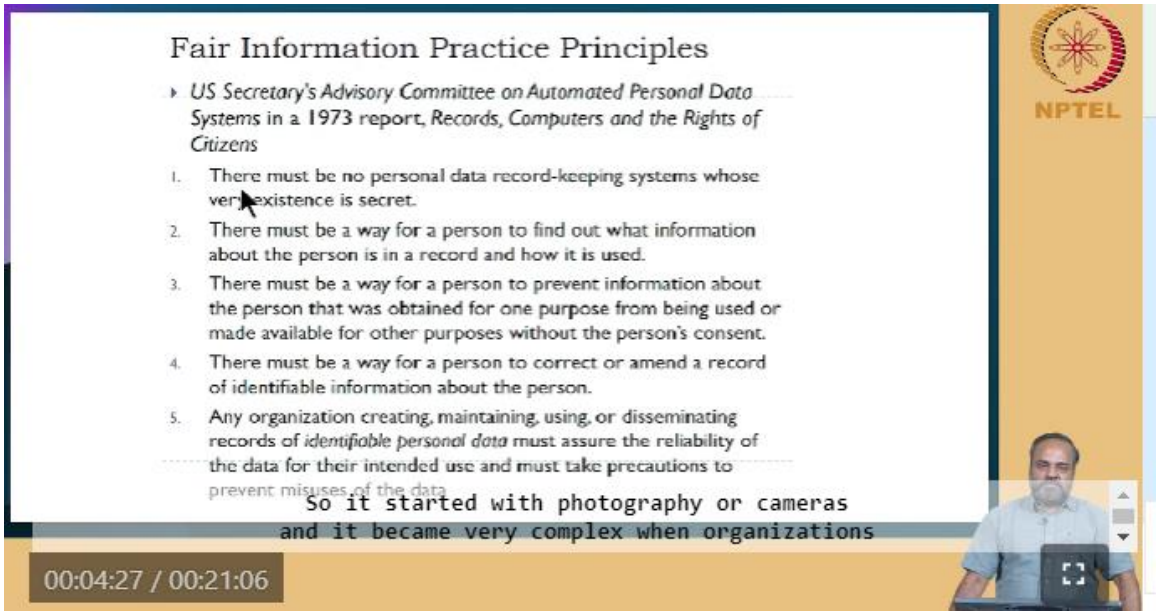
So Alan Westin is often known as the father of Privacy, father of Information Privacy. Till that time he consistently studied the topic of privacy and wrote several books and published several papers on Privacy. So Alan Westin is a name you cannot miss if you study Privacy. So his definition of privacy 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. So in other words, this is the definition of Information Privacy.

Information Privacy is an individual's control over one's information. I will decide what I disclose. I should have that right or I should have that autonomy. So Privacy,

Information Privacy as control over one's information is a fundamental definition of Information Privacy. Just like in the case of Privacy, we saw the definition is the right to be let alone.

So that involve your physical, your body also, your whole. As a whole what is privacy? The right to be let alone. But what is Information Privacy? The ability to decide for yourself, what you share or what you do not share. So that is the difference between Information Privacy and Privacy. Now the topic of Information Privacy became extremely important with the rise of technology.

So it started with photography or cameras and it became very complex when organizations including government and other organization, business organization started collecting and storing and analyzing individual's data in databases. And then there was increasing awareness about individual's information or employee's information and citizen's information to the extent that in the computer era, the US government actually instituted a committee, US Secretary's Advisory Committee on Automated Personal Data Systems. In 1973 they actually produced a report but this committee was constituted by the US government because they found time has come to make some sort of guiding principles or law about privacy because data is stored in the databases and there is a concern for privacy. This particular report provided five principles known as Fair Information Practice Principles, FIPP, FIPP it is called FIPP, Fair Information Practice Principles. It is known as the most fundamental foundation for Information Privacy because we will be reviewing various regulations of privacy, security and privacy in different regions of the world, Europe, India and maybe North America.



And we will see that FIPP actually is sort of a guiding principle for all these regulations. So what does FIPP say? It said there must be no personal data record keeping systems whose very existence is secret. No company including government can collect and keep data about an individual in secret. If any agency collects my data and stores it, I should know. It cannot be secret.

That is principle one. Principle two, there must be a way for a person to find out what information about the person is in record and how it is used. I must, if my data is stored, collected and stored, I should have the right to access that information. Can you change, make changes in your Adhaar data? Can you access your Adhaar data? You can, you can. There is a procedure for making changes as well and correcting errors etc.

So this is principle two. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes, without the person's concept. So if Shaadi.com collects or you provide your information to Shaadi or a matrimonial site for the purpose of finding a partner or for marriage in our country, then it is a lot of private information that you actually share there. Now Shaadi has that in your database, in their database.

What do you think? Do they share that data with other agencies? You should read their privacy policy and decide whether you should go for these sites or not. They have, sometimes these companies have got perpetual rights to transmit your data anywhere. So we will go, that is why regulation is becoming stricter and stricter today. So if an agency is sharing the data that is collected about you to some other agency, it should be with your consent. That is the third principle.

There must be a way for a person to correct or ammend a record of identifiable information about the person. If I want to correct some things, there is an error, I should be able to do this. Nandan Nilekani when he developed the Adhaar idea, so he several times, I have listened to him saying that we collect only most basic data that is required, nothing more. So the basic principle is collect only that data which you need, nothing beyond. So and it has a purpose and the data should be used only for that purpose.

If you collect anything extra, the purpose should be clear. Just for the sake of it, you cannot collect data and store. It should be purpose driven. Fifth principle, any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. So now here the onus or the responsibility of securing private data is on the data collector.

A agency which collects data should be able to secure the data or data breach is a breach of law, is a breach of the privacy principle. So it is a company's responsibility to invest in security by going by this FIPP's principle which became regulation in many countries already. So these are the basic underlying principles of Information Privacy which first got outlined in the Fair Information Practice Principles. And in the domain of Information Privacy, you would often come across these three entities, reference to these three entities. This is very much there in GDPR, when you actually have an overview of GDPR in Europe.

Data Subject, Data Controller, Data Processor, there are three entities. Data subject is a person or an individual whose data is collected. That is the Data Subject. Data Controller is the agency which collects data. It also takes decisions about the data.

The Data Controller can process the data that is collected, can store the data, can also share that data with another entity, which is a Data Processor. Or the Data Processor and the Data Controller can be one entity also. So if say, ICICI bank has your banking data and it shares the data with an analytics company, Fractal Analytics. So the data is passing hands from Controller to Processor. So it becomes a third entity which has access to the private data of the Data Subject.

So we need to visualize these three entities across which private data actually gets transmitted, stored and processed. We have Personal Data Protection Act, which of course, got dropped in recently and it is, government is reworking this Act. But in the original document, they had similar concepts like Data Subject is called Data Principal, Data Controller is called Data Fiduciary and Data Processor is called Data Processor. Fiduciary is someone whom you entrust your data with. So before I hand over the session for the case, there is in research, in research literature there is a concept called Concern for Information Privacy.

So privacy can be a talk, you know you can keep talking about my right, your right, regulation, this and that. But In research, particularly in consumer research and also in economic analysis of privacy, you need to have measurable concepts. You should be able to measure what is the privacy or what is the concern for privacy. So that is where scholars developed a scale or a measure of privacy. And if you look at closely these measures which can be measured using a scale, a Likert scale or whatever.

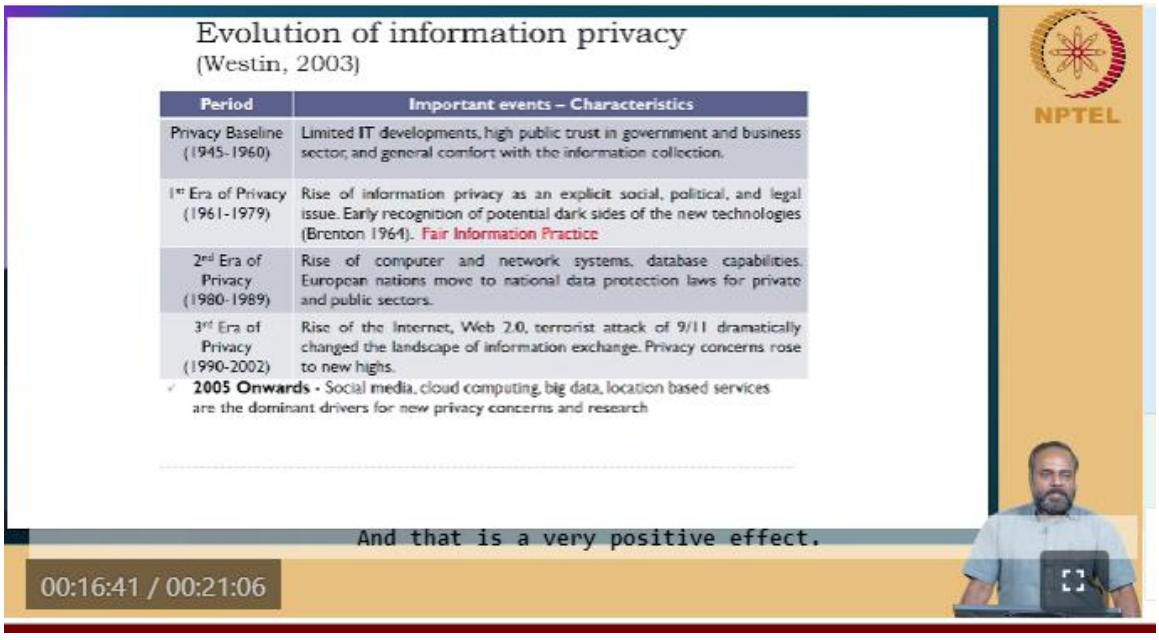
So they look at four dimensions. You can see there are four dimensions to Information Privacy. One is concern on collection, second is concern on unauthorized access, third is concern on errors and fourth is concern on secondary use. These are quite intuitive. When you talk about your privacy, actually what are the concerns, what is, you know, where all

you have concern.

One is about collection. Why are they collecting?, What is the purpose?, etc. You know something that is related to the collection of, collection itself. Second is unauthorized access, having collected would someone else, who is accessing my data, my health data, my, you know my family data and so on. So that is unauthorized access as a concern. Errors, you know I was in GATE examination the previous week and one student was not able to log in for giving the, taking the GATE exam.

And we found that the reason is the password is linked to the date of birth and the student has entered a wrong date of birth in the GATE database. So the GATE created a database based on the wrong date of birth, which we could see what is the date of birth in the system. But the student is trying with the actual date of birth. Then of course we checked it with the, you know ID card and all.

So it was only an error. But in this case, we allowed the student to write the exam because it is an error. But the student's concern now is I need to correct that error. So concern to correct errors pertaining to private data. And secondary use, will the entity pass my data to somebody else? And then what happens? This is an important concern in the Information Privacy space. So keep those four dimensions, which can be measured using scales, but that is what you mean when you talk about Information Privacy or concern for Information Privacy.



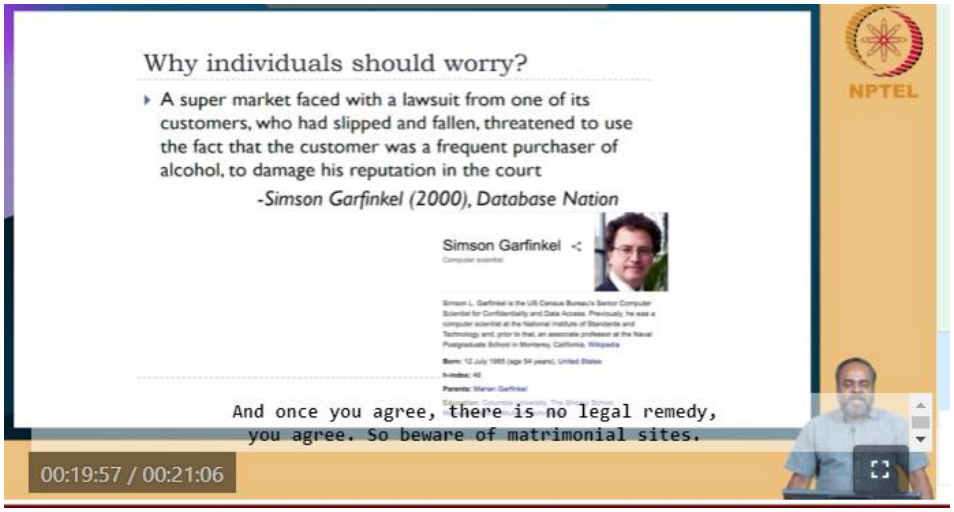
Collection, unauthorized acces, errors and secondary use. This is to give some sort of historic milestones about evolution of Information Privacy from the 60s to 2005 and beyond. So as I said, Alan Westin did not live in the social media era, but you know the privacy concerns are growing and growing where you can see countries are regulating the flow of information. And Supreme Court had to intervene in our country and say, privacy is a fundamental right. So you see the discussion on privacy is, has become a public debate.

And the primary reason for this to happen in our times is, there is, we call it information era, we live in the information era. The biggest change that has happened in the last few decades in the human evolution is the Information Revolution. And that is a very positive effect. You know the digital technologies has made life much convenient, much easier. And we flow today, but the dark side of that is that information about you is flowing.

So and that is a huge concern, misuse of information. Information is, you know, plenty and is available and can be stored efficiently, can be transmitted efficiently but that also has a dark side. Why should organizations worry? You look at the several cases of data breach and the liabilities that have happened in the recent past. Tomorrow in the next class, we have a discussion of a data breach of 2017.

And that is not very far in history. So you see that this is a major concern for organizations. And therefore, Information Privacy should really be taken seriously by organizations or the leadership of organizations. And you see that change happening, in addition to a CISO's post, you now have, you now have a information, there is an office of, a special office for Information Privacy. You will see those changes when we discuss certain specific cases. Why should individuals worry? Organizations should worry because they have liability.

Individuals should worry because it is my private data, I can be harmed. And I can be embarrassed. Embarrassment is a pain, it is actually a pain. And therefore, that can harm you, that can harm your career, that can harm your personal life, your family life, your existence



So this affects individuals. So when I joined research, PhD program, this is one book I read and there was not much focus on privacy in those days. But I enjoyed reading Database Nations, Simson Garfinkel's Database Nations, where in the United States the individual's information was available to credit bureaus. Credit bureaus collect and process and give information about individuals, their spending habits, their preferences, etc to merchants or online merchants or you know. So this is something, profiling of individuals is something that is happening. But at the same time, well this is positive for merchants, but this can harm individuals.

So Simson highlighted several cases where individual's privacy was affected. But when it, when they went to court, the decision was in favor of the business, not in favor of the individuals. Why so? So that is something that we should enquire. You know of course, there is something called privacy, terms and conditions of privacy, which we all generally agree. And once you agree, there is no legal remedy, you agree.

So beware of matrimonial sites. So let us discuss a very interesting case today. So before that, yeah, so I belong to this generation. So the best thing is that we shared a lot, but nobody knows. But if you guys put it, everybody knows. There is a record about what you do in the digital space.

And many of those social media organization, of course, now regulation is changing, do not actually delete your information, they retire you, but they do not delete. But we do not have to worry. So, so we have the case on We Google You, right, so which pertains to the case of privacy, which includes an organization and individuals. So let us try understand with this, with this case, the issue of privacy in more detail.