

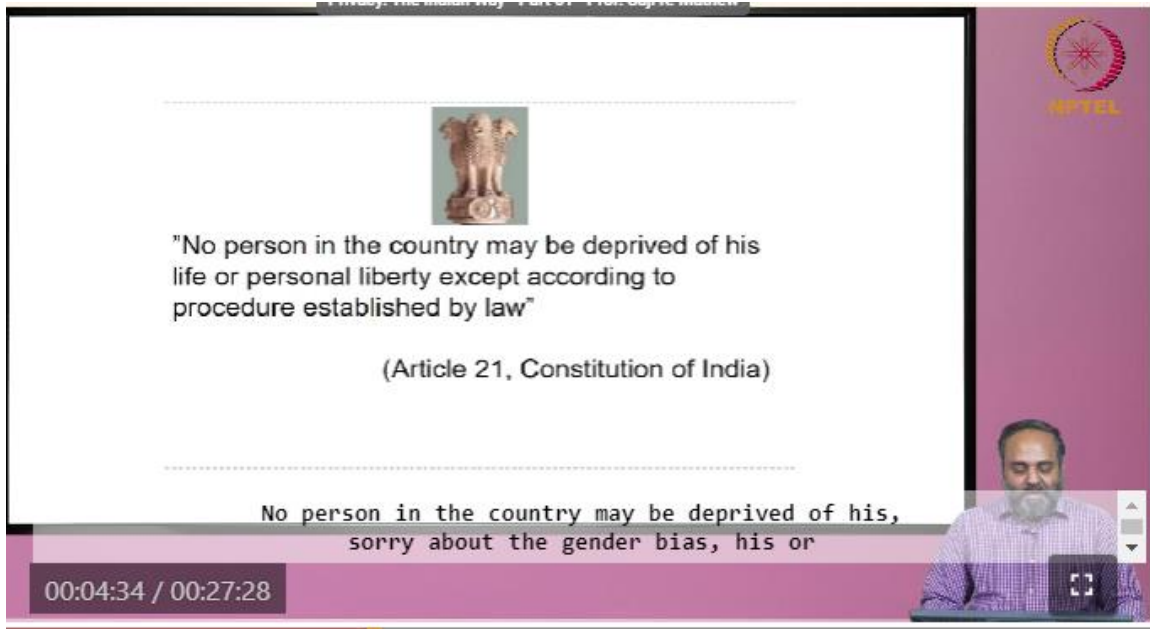
**Course Name: Cyber Security and Privacy**  
**Professor Name: Prof Saji K Mathew**  
**Department Name: Department of Management Studies**  
**Institute Name: Indian Institute Of Technology Madras, Chennai**  
**Week: 12**  
**Lecture: 34**

Okay, good afternoon and welcome back. So we have started discussing regulation, regulatory frameworks that prevail in different parts of the world. So that is something that we are exploring along with case studies which actually give us a sense of what are the issues in different parts of the world and how are they being addressed. So, we can now appreciate that data privacy is something that operates in multiple levels or there are different stakeholders when it comes to data. It is not you alone or it is not government alone, but there are many layers of, many layers through which data passes or there are many actors who are interested in data and particularly personal data and whenever personal data or personally identifiable data is involved, there is a data privacy issue and we discussed what is privacy and what are the concerns in privacy and why organizations should worry, why countries should worry or government should worry and so on. So we have seen that.

So today we move on and we land in India, to see how, what is the state of affairs in our country and since we are part of the Indian society and in the Indian culture, I believe all of you, we do not have foreign students in the class, otherwise we get to compare. So we have a sense of our own understanding of what is privacy and that has been evolving. It is not, it is quite dynamic and as the digital world has exploded, not just incrementally expanded but it has sort of exploded in the last 20 to 30 years and you can see its implications in the country and we can also see our administrative systems at different levels including the country level are sort of responding to that changes. That is the most interesting point that we will see, that we are not sleeping, We have to tap into the potential of digital world but we also need to take care of the concerns of privacy and we can see government is acting on it.

So let us move on, the first plan is to give you a summary of data privacy or a historical perspective of data privacy or privacy in the Indian context and then we would get into more details of how this has actually become an issue in the recent times. So maybe for several decades post-independence the government did not have to worry much, but currently it has become a national issue. So we will focus more on the current times after giving a perspective, so that is how we are going to go. So first things first, we belong to India. So when you live in India, India is sort of, you know the reference document what

defines India is the constitution, we have a constitution and that is binding for all states of India, all states and union territories.



The screenshot shows a video lecture interface. The main content area is a white slide with a purple border. At the top center is the State Emblem of India. Below it, the text reads: "No person in the country may be deprived of his life or personal liberty except according to procedure established by law" (Article 21, Constitution of India). A second line of text at the bottom of the slide reads: "No person in the country may be deprived of his, sorry about the gender bias, his or". In the bottom right corner, there is a small video window showing a man with a beard and glasses. The bottom left corner of the slide shows a timer: "00:04:34 / 00:27:28". The top right corner of the slide features the logo of NPTEL (National Programme on Technology Enhanced Learning).

So it applies and touches upon each of us and see what the constitution assures us or in more glorified language, this is enshrined, what is enshrined in the constitution of India, is a right to freedom. No person in the country may be deprived of his, sorry about the gender bias, his or her or her or his life or personal liberty except according to procedure established by law. So nobody, no individual, no institution, no government can deprive an individual of personal liberty. So, but there is an except or there is an exception even in article 21, except according to procedure established by law. So that is what article 21 is, but we must read the whole of article 21, just do not read the first part and leave the second part.

So the constitution is a well drafted or carefully drafted document that addresses the concerns of all stakeholders. So let us move on, so freedom, personal freedom is assured in the constitution. So now let us look, let us go back a bit in time and let us also advance or go forward from the time the constitution became effective, we all know that the Republic Day or 1950. So let us look at India before that, let us look India after that. So one of the landmark legislations in the, in the ancient India or India before independence goes back to 1885 and you must have read about this in newspapers in recent times also because we often refer to this legislation, enacted by the British in 1885 and that is known as the Indian Telegraph Act.

**Privacy in India: A quick glance**

- › British enacts the Indian Telegraph Act 1885
  - › Post the first war of independence (Indian mutiny), 1857-59
  - › Provided interceptive powers to government
- › Post independence, Indian Govt instituted Post and Telegraph (P&T), a department under its control
  - › Article 21 and the telegraph act continued together
- › Telegraph act amended in 1972 to include the threat of "incitement of offences"
  - › Wire tapping during emergency period legitimized by the amendment
- › In 2018 SC declares privacy as a fundamental right
  - › Context: Aadhar act and government as a major data fiduciary
- › Government proposes Personal Data Protection (PDP) Bill alongside GDPR; drops it in 2022
  - › Proposes Digital Personal Data Protection (DPDP, 2022) Bill

because there was this so called mutiny or the first independence war,

00:07:02 / 00:27:28

So telegraph was used by institutions particularly the British government for, for communication in the, in the 19th century. So in, particularly after British got established in India, you know the Plassey war in 1757 I believe, though they sort of, you know they actually conquered the land and they actually established their own systems and laws and so on and they found it essential to have a telegraph act because there was this so called mutiny or the first independence war, in between 1857 and 59 and the British government extensively used telegraph or tapped telegraph and they found it essential to have interceptive powers. So this is, particular act gives powers to intercept telegraph communication of any communication that happens in the country. So it gives access or interceptive right to government to rule the country. That is the, that is the essential message in the telegraph act.

Government can intercept messages and that is a right by law from 1885 onwards. And post-independence this law did not change but what Indian government did was, it brought the post and telegraph, the P&T department as some of you may be aware, you know. We used to go often to the post office in our, in my early life but no more but the P&T is, was like Indian Railways, was part of our, you know regular life and it was under, it has always been under government's control because government could actually have control on communications. So essentially that is the message. So it remains a department under the control of the government.

So what we can see is, article 21 we have already seen, it gives right to freedom and we also see telegraph act. So both this, both this, both these references or both these facts work together in our country. They go together. Government has certain rights. At the

same time, you also have your personal right.

And essentially what we can conclude here is, you know these are, this may be, you know sometimes in conflict. So let us move on and telegraph act got amended in 1972. Let me not name any individuals but there was a government in power in the 70s and it is a bit notorious in the history of India because it is known for, sort of government taking control on individuals freedom, particularly the emergency period and that is when this law was further amended to make it, to make wiretapping possible, especially on to what opposition leaders were talking to each other. The government could gain access and it was made legal. That is what you see in 72.

But the landmark judgment or the declaration came in 2018. There are events before, between that but in 2018 Supreme Court of India, the judiciary okay. So of course, you see the legislative and the executive, it is one government. So part of the same government. So they make laws for their convenience to rule but the Supreme Court actually intervenes and declared privacy as a fundamental right and I am sure all of you are aware of this and that was a landmark judgment.

And before that itself in certain judgments, I think in Madras High Court, there was a judgment which the judge almost said the article 21 in fact assures that privacy is a fundamental right, although it does not say it explicitly. So in 2018, the Supreme Court explicitly said privacy is a fundamental right and it also was in the context of the Aadhaar Act and the deployment of Aadhaar extensively in the country. So government was going extensively or almost exhaustively to collect biomedical data of citizens and store that personal data, personally identifiable data in a database in a digital form. So that is when this concern for privacy came up at a national level. So government actually became a data controller, a major data fiduciary of the country today is not organizations, but the government.

Having in its custody digital data pertaining to about 1.3 billion people, the largest database in the world. So that is the context in which the Supreme Court made this declaration, well you are in possession of individual data but it is somebody's fundamental right. It is the fundamental right of citizens that you are actually becoming a guardian of. So that is actually a very critical responsibility for the government.

So then subsequently you can see that when a GDPR was enacted in the European Union in 2018, you presented that already. You can see the Indian government has been very responsive, very positive thing that you can see is in 2016 if you read the background, in 2016 itself when GDPR was actually being discussed and was an open draft, Government of India also started working on a similar regulation for data privacy. And in 2016, 2014

I guess, if I am sorry a bit confused about when Justice Srikrishna Commission got the project from the Government of India to draft a regulation, a draft, a bill for a regulation in the country for data privacy. So Justice Srikrishna Commission, actually it is a commission. So it made extensive consultations with different stakeholders and of course, it also was very much aware of the GDPR development in the European Union.

So it actually presented its final draft in 2018, that is known as the Personal Data Protection bill, PDP. But of course what happens is when an independent committee works on a bill, you know it of course it is like a conceptual document, you know so it goes to the government and then the bill is prepared by the government. The particular draft was developed by the Justice Srikrishna Commission but the bill was, it was converted into a bill and of course, government made certain changes in the draft. And that is why it went for a long time in the parliament and it was not approved by the parliament. It was referred to a parliamentary committee and of course, a committee consists of people from opposition and the ruling party and they never agreed.

Finally the government dropped this PDP bill and it actually now has proposed something called DPDP, digital data protection, digital PDP. DPDP, sorry I have written it, there is a spelling error there DPDP, Digital Personal Data Protection, DPDP, it is called DPDP. DPDP 22 is a bill now and we have to watch it, keep watching and waiting what happens to it next. So that is a broad historical overview of the privacy journey of the country and we can see that of late we are very very responsive to what is happening around the world and we have a very, you may disagree with specific clauses of the bill, you know that that is where the debate is but we can be very proud that we are very much at par with the developed countries to have a separate bill or a separate law for personal data protection, PDP. Now let us move on, let me give you some more insights from recent times.

Are you familiar with this person? K.S. Puttaswamy, nobody may actually care such an old man he is, I guess he must be 97 now, and he is a retired High Court Judge of Karnataka and in 2012 he filed a public interest litigation in Supreme Court and that is when the Aadhaar debate was very active, okay and actually if you have to remember a single person for data privacy, as a father of data privacy in India, I will call Justice Puttaswamy because it is against his, against his writ petition that the Supreme Court judged privacy as a fundamental right, you know it just Supreme Court just does not make a statement but it is actually Puttaswamy's writ petition that actually Supreme Court considered and finally in 2018 made the landmark judgment that privacy is a fundamental right. So Puttaswamy was concerned when he looked at what Aadhaar is doing. So every individual needs to go to a data collection center, provide the biomedical identities, you know including your iris, your retina, your all your fingerprints, you know everything about you is taken by government and as someone who is privacy aware looked at it, well

government is getting too much powers and what the government would do tomorrow with this kind of data is a matter of concern.

So and also the other important aspect is that, making governments, for getting government services, making Aadhaar mandatory, was another concern. For example, if I am concerned about my privacy, I do not trust government. I do not want to give away all my personally identifiable data to the government. Then what happens is, I am deprived of a lot of government services, including the PDP, my ration or my right to vote. So a lot of services became possible only if you have an Aadhaar card.

That is what he challenged. This is not fair because it is my private data. I do not want to give this much, this extent of private data to the government, okay and so that is when, sorry so I said probably 2018. So I was wrong. The Supreme Court in, on August 24, 2017 said the right to privacy is a fundamental right, you know. This particular judgment is there in the open, you can read the whole long judgment but the essentially, the key part of the judgment is the right to privacy is a fundamental right.

The right to be

- ▶ The right to privacy is a **fundamental right**. It is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices.  
The Supreme Court, August 24, 2017
- ▶ Then how can the government ask me to share my biometric data to receive government benefits?

It is a right which protects the inner sphere of an individual from interference from both state

00:18:41 / 00:27:28

The slide is part of a video lecture. On the right side, there is a logo for NPTEL (National Programme on Technology Enhanced Learning) and a small video window showing a man speaking. The slide content is on a white background with a black border.

It is a right which protects the inner sphere of an individual from interference from both state and non-state actors and allows the individuals to make autonomous life choices. So autonomy, we discussed this. So Supreme Court upheld the right to be autonomous, the right to be oneself, the right to decide, the right to choose for oneself where one can be or you know, with whom to share data, with whom not to share data etc. okay. So the point is, if privacy is a fundamental right, then how can the government ask you or me to share my biometric data to receive government, to government benefits or government

services? I want my privacy to be protected.

So government is intruding into my private space by asking for personal data, particularly biometric data. So what do you think about it? Isn't it a sort of conflict, if I choose not to disclose my data? It says I am autonomous. Now I say don't disclose this data. If fundamental if privacy is fundamental right, government should not deny services to me.

That is my choice, correct. Should not deny? P3 odd cases, in case you don't want to do anything about it, like absolute privacy, no benefits also required, there are people like that also. I know that is a point. If you are, if the government says for getting benefits you should share data, all your data, then that is not fair. That is the question because on the one hand I have the right to decide whether to share my data or not, I am autonomous, on the other hand government says that, that is fine you have a fundamental right but you will not get the services if you actually exercise your fundamental right. You cannot vote, you cannot get your ration and so on.

Some kind of balance will have to be maintained. So you see the need for, somewhere there has to be, it is a grey area. Okay, okay, okay, that's a different topic. Celebrities actually don't want privacy, okay, yeah.

Okay, okay. Information should be classified and protected. One thing is like why is the government asking for the biometric data? What is the end use of the data should also be seen. For example, the Aadhaar. So after implementation of the Aadhaar system, a lot of fraudulent data was removed from the system, lot of, where especially for rationing of ration goods. So a lot of fraudulent entries were there, which lot of people were siphoning off. Instead of the benefits reaching the actual beneficiaries, it was siphoned off and only by using the Aadhaar data where was the government able to identify that this is a fraudulent data and this is the actual beneficiary.

So especially in Assam, there is a huge case where over 22000 crores of corruption was unearthed by using the Aadhaar which is in two years of implementation. So the end use should also be seen. So and it is not as if in though, we are implementing it now such social security systems based on a unique identifier already there in the West. So there of course, the citizens are more active and force their governments to protect their data much more but so for this particular question the right, the end use should also be seen, that's what I am saying. So essentially we are reaching the point that government.

Yeah I just want to answer is the government taking any ultimate guarantee that the data will not be compromised. There is no guarantee from the government. Well, that is what the PDP is trying to do. That is what the regulation, that is why we see this conflict or you

know, really conflict. You know two parallel lines and that is where you need regulation you know, to protect the both the interests, to ensure that it does not skew towards one but bring some sort of balance.

That is what always regulation does. So it is quite obvious that the country requires a regulation when these parallel lines exist. But there is one important aspect. Yeah. Where is the concern of the upwardly mobile and the educated only, the lesser educated are not so much bothered and that is what the majority of the country in our, in our country is, that the majority.

Yeah that has been the case for several. They want the benefits. Yeah. They said privacy you can keep. We talked about it that is a privacy paradox and you know unaware of privacy etc. But what you see is the migration towards the urban and education growing, western access growing so people are becoming more and more aware.

Otherwise this debate was not there in our country, we talked about it. So currently with digital, in the digital space when people are increasingly becoming privacy conscious, upholding privacy as a fundamental right was very important. So you can see in article 21 itself, we just saw that statement, no person in the country may be deprived of his life or personal liberty except according to the procedure established by law. So an invasion of privacy or personal liberty must meet threefold requirements. So it is very clearly specified that if the government, for example has to access or intercept private communication, there should be three requirements- legality which postulates the existence of law, need defined in terms of legitimate state aim and proportionality which ensures a rational extent of data collection.



Nothing absolute

- ▶ "no person in the country may be deprived of his life or personal liberty **except according to procedure established by law**" (Article 21)
- ▶ An invasion of life or personal liberty must meet the three-fold requirement of (i) **legality**, which postulates the existence of law; (ii) **need**, defined in terms of a legitimate state aim; and (iii) **proportionality** which ensures a rational nexus between the objects and the means adopted to achieve them;

about ten agencies can actually tap into private communication based on the 1885 British law.

00:25:44 / 00:27:28

So for example, in India if any government agency including the Income Tax, I think Income Tax is exempt, but see the Narcotics Control Bureau. We discussed a small piece of case in one session. So they were able to access the private communication between two individuals. But for any agency to do that in the country, there is an agency called Enforcement Directorate. So the ED's permission is generally required, I think Income Tax is exempted from that, that is what you know, it is not confirmed but that is what I believe.

But many agencies, about ten agencies can actually tap into private communication based on the 1885 British law. Government has actually the right to access that in the Indian Telegraph Act. So what you see here is privacy is a fundamental right but it is not an absolute right. Privacy is not an absolute right. You cannot say, always in all conditions your privacy should be protected.

Suppose you are a criminal, so you commit a crime and then you say, I will not disclose who I am, it is just not possible. So it depends on the context but I am just including a clip, not the detailed judgment. That is very recent. It also, a Supreme Court judge also said, no absolute power for state to snoop into sacred private space of individuals. You can see that even for the state to snoop or to intercept there are conditions.

That is what is given in the second clause, legality, need and proportionality. So there is no absolute power for government as well. So privacy is not an absolute right and government also does not have absolute power to intercept. So there are many grey areas

there in terms of interpretation, that is where actually the whole debate comes. What, in what situation, what context can government tap, wiretap and to what extent and can that be made public etc. are still grey areas.