Digital And The Everyday: From Codes To Cloud
Prof. V Sridhar
Department of Multidisciplinary
International Institute of Information Technology, Bangalore

Lecture – 08
Data Protection & Privacy Regulation in the Digital Era - Part 03

(Refer Slide Time: 00:20)

Important, yesterday, 2 days back, it was out. You know this case? Sir, do you know this case?

Student: I do not know how I think somebody has asked for the thumb impression of the Jayalalitha.

I live near very near Parappana Agrahara where Jayalalitha was in jail. So, Jayalalitha was in jail. She put her thumbprint before going to Parappana Agrahara jail, right.

Student: Madras High Court has denied.

No, I am just. So, she put her fingerprint, right. Then there seems to be you know the opposition is saying that there was an incident in which Jayalalitha was actually physically present. Jayalalitha's council is saying that no she was not there she was in the jail ok. Now how can you prove, right? So, you have a thump impression, but I have to match it with Jayalalitha's, how will you match it with Jayalalitha's? She is dead. She is

no more no, last year she passed away, right. so, High Court asked for release of biometric information from the other database of Jayalalitha. So, that they could match it then if it is proven, then she was in Parappana Agrahara jail. If she is not proven, then she might have been in another place, right. High Court asked for release of UIDII biometric information. UIDII came back and said that the biometric information cannot be released without.

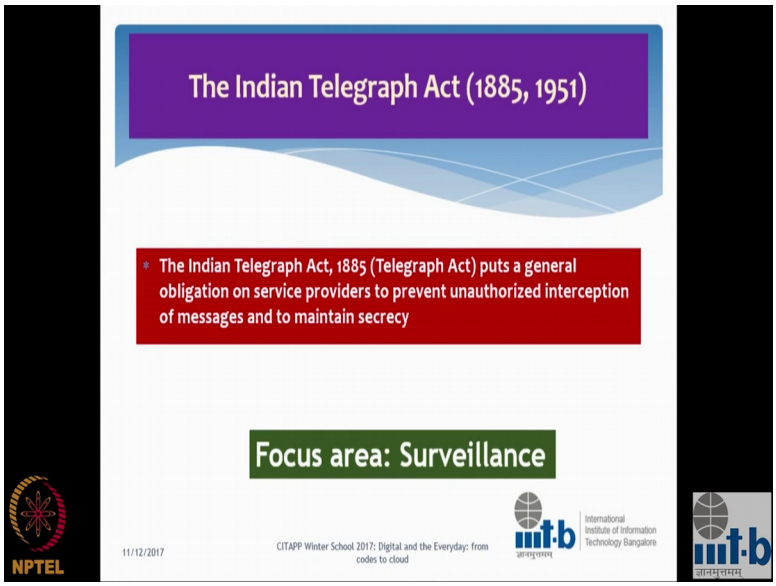
Student: Consent.

The owner's consent; owner's consent; you cannot get it anymore, right. So, Supreme Court; it went up to the Supreme Court. So, Supreme Court said it has put a stay on High Court questioning of this. You know no more information releases about Jayalalitha, especially on fingerprints and the state, the proceedings; very important right. Now, how will you account for this? Is this ok? There is something called as right to be erased, ok.

Student: (Refer Time: 02:14) forward.

And we will discuss about that in (Refer Time: 02:17). So, if for example: once, the person is no more, shoot that information be there and not be there, it is a big question mark which is hunting UIDII, right. Now, on one hand you cannot get the consent, on the other hand you cannot release without consent, right. So, how will you do with this? It is a big problem, right. So, how will you deal with all these things? It is a big question mark, right. So, we need laws, regulations and policies. So, snapshot it is not we have been having lot of loss right.

(Refer Slide Time: 02:56)

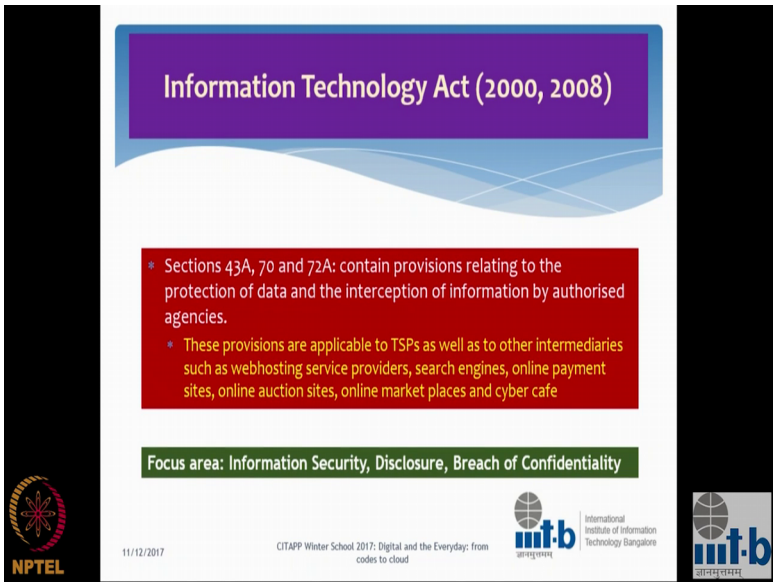


So, Indian Telegraph Act of 1885, also talks about privacy, right. So, it takes you know service providers, but here who is providing the electronic communication the electrical and electronic communication, they cannot you know without the authorization snoop in or intercept communication, right, this is there in the Telegraph Act. So, you for example, a telecom company such as Vodaphone or Airtel taps into your conversation, then it is against this particular class in the Telegraph Act and they can be booked for unsolicited surveillance.

We also have Information Technology Act of 2000, amended in 2008 has lot of clauses, but the important thing to notice that each law has its own focus, each act has its own focus, right. Telegraph Act is mainly intended for service providers it does not care about individuals, it only is worries about service providers, what service providers can collect, not collect, should they protect, should they not protect and most of this related to surveillance that is during the information collection stage they are not.

It is not worried about how it is passed on, it will be passed on and will be aggregated and things like that it is not worried about all these things at all it just worried about the surveillance part of it. So, we are just covering about I do not know one fourth of the whole information taxon and privacy taxonomy that we discussed, right.

(Refer Slide Time: 04:39)



Information Technology Act; it has clauses for breach of confidentiality security of information by the service providers disclosure without consent, these things are addressed, but it does not even talk about secondary use it does not talk about aggregation it does not talk about accessibility. So, all these things are not covered in the Information Technology Act just bare minimum, you have to keep the information secure nobody can actually access this information without your prior consent and things like that right.

So, only 2 or 3 clauses are covered in the Information Technology Act then we have Aadhaar Act. In fact, Aadhaar Act is very very good, I like it very much and it is actually targeted delivery of financial and other subsidies and services act, right, it is got nothing to do with your you know bank account or income tax you know pan; pan linking and things like that.

So, it is for targeted subsidy, right it is actually enacted under finance bill if you remember and then if you look at the act it mandates responsibility of the requesting entity that is whoever is collecting your biometric information or want to use authenticate your Aadhaar number to use that information primarily for authentication. So, according to this act anybody can authenticate, but there is only the answer should be yes or no right whether you are what you are or not the important thing about Aadhaar is that Aadhaar links your random number to your flesh and blood that is the most

important thing right no other instrument links your flesh and blood with a number your pan number that is why there is a reason, why we have many pan numbers you know.

All belong to the same individual, but cannot be linked to the flesh and blood right bank account you can have many accounts no problem right, but Aadhaar number you can only have one, it is a one to one relationship, right because it is linked to flesh and blood right that is why it is very very powerful right. So, Aadhaar Acts recognizes that right that this biometric information should be used only for authentication purposes and not for anything else and the requesting entity has to be very very careful right when it is using Aadhaar related information cannot be used for secondary use it cannot be used for aggregation all these things are discussed in the Aadhaar Act.

So, it discourages secondary use, for example, whatever we have discussed right without once own content cannot be used for purposes other than for which it is intended for right and Aadhaar is mainly intended for cash transfer, direct subsidy, governments services and not for anything else. So, there are a lot of clauses which prevent that so, but the focus area is (Refer Time: 07:27) little bit broader compared to for example, the Information Technology Act or the Telegraph Act it covers areas such as confidentiality secondary use disclosure and so on and so on.

So, it is a little bit broader in scope, then we have this famous Puttaswamy versus Union of India judgment, Supreme Court Judgement, right which came out on twenty fourth august.

(Refer Slide Time: 07:50)

So, what does this say? This says that the privacy is a fundamental right of every citizen, it is a fundamental right, right. So, protecting the privacy is a right for the individual they very simple statement, but it is very powerful right. So, what does it say? It basically says that right to privacy is protected as an intrinsic part of the right to life and personal liberty a part of the freedoms guaranteed by part 3 of the constitution right except under a reasonable restriction you can defend your privacy and that is very important.

So, tomorrow for example, if you think that your Aadhaar linking is being used for secondary use or for aggregation purposes you can actually file a case am I right sir I can file a case saying that it is my fundamental right to protect privacy and I can take recourse under this particular judgment right. So, today, it is not it does not go into all the details right even it is server like 270 pages is something I have not written fully written you know red through it, but the focus area is the state cannot servile you is mostly on state surveillance, right.

So, you for example, your UIDII even nobody can force you right to disclose your UIDII information and that is one of the reasons why now government is very cautious about doing many more things, right, even Aadhaar linking with your with your bank account, pan cards been postponed 31st March and in fact, it is coming up for hearing in Supreme Court soon, right whether it is can be done or not and things like that are being questioned.

So, whenever government formulates any act or policy, then they have to be conscious of the fact that it can be contended by the individuals in the court of law right and therefore, it provides us with that mechanism right. So, even though it is very simple it provides you with all the ammunition to go to the court and you know protect your individual privacy that is one of the important things that this particular judgment has done. And of course, recently last year last week the justice B N Shri Krishna Committee Report is already out that is the draft data protection regulation.

(Refer Slide Time: 10:08)

So, this is supposed to give us combined view of all the things that we discussed I do not know I have not read it, it is about 273, I have still reminded of the 273 pages, how will I read it, right, but if you happened to read this right this is up in the mighty site the ministry of electronics and information technology website for a public consultation, you should all read it right and then its open for consultation and after that it will be drafted as a bill and then it has to be enacted in the parliament, but we have some you know good things that have that have come together I mean. So, far there was no protection of privacy in the country you cannot really protect your privacy.

After the Supreme Court you can protect your privacy and what under what it is still very nebulous there is no definition of privacy in the protest for me judgment it does not say what privacy is, but you can file a case and you can defend against your privacy

violation, but this one goes into the details of what constitutes a privacy and therefore, you can actually make forceful arguments right if there is of any violation and so on.

So, we have to sort of I have not gone through it, but important thing, what about other countries, right are we again lagging by 60 years, 70 years from other countries? Yes, we have lagged quite a bit, but the recent Supreme Court judgment is being you know pleased all over the world right this is the greatest you know privacy related legislation which is which is come.

(Refer Slide Time: 11:55)

So, the important thing is the other countries are looking at it an important thing which is happening is the general data protection regulation act of the European Union which is coming into force on 24th of May 2018, this is very strict ok, this protects the privacy of the individuals and more than that I have circled some important aspects of this GDPR.

The important aspect is right to erase it, very important, if I think that my personal data has to be erased and if I do a query to Google then they better delete it; delete it from all histories and all databases, all around the world, they have to be deleted and I have the right to be forgotten, right, the need to be forgotten is very very important, right and it is very very difficult to implement even with algorithms that (Refer Time: 12:48) of discussed because it might be there in thousand millions of places, but I have the right to erase that particular information that is a very important provision in the European GDPR, I have not yet red that Shri Krishna report, I do not know whether it is there or

not I have to see that, but if it is there then all these government as well as firms which are collecting information have to seriously look into it right because this clause is very very powerful.

Their second important thing is international data transfer. So, as you know the information technology service industry the keynote speaker talked about all those things we deal with information all the time right our IT companies like Infosys, Wipro, all the BPO companies, they handle personal information all the time, the important provision in the EUGDPR is that it gets the privacy of the individuals gets carried across countries.

Student: Data sovereignty.

Aata sovereignty is pro. So, for example, the EU related data, if it is handled by the data aggregator in India then we are subject to the same provisions of privacy compared to for example, in Europe, right which means that we our companies have to comply with the EUGDPR and make sure that privacy variations do not occur the important thing, see we can have all these policies regulations, but there has to be enforcement that is one where India lacks quite a bit there can be lot of regulations lot of rules our rules and laws are always perfect, but the problem is with enforcement right important clause.

Here companies tend to lose 2 percent to four percent am I right sir of their gross revenue if there is a violation under EUGDPR and that can be millions of dollars for companies its even billions right Google has to be really really worried right before twenty fourth march if there is a case against Google and Google is found to be violating EUGDPR, then it has to pay up to four percent of their profit how about 70 billion dollars, right.

So, it is a serious violation. So, the enforcement the most important thing is EUGDPR is the first global regulation where enforcement is given preference, which means that if you do not add here, then there is a serious penalty. And therefore, the companies will weigh what is the benefit that I am getting by manipulating user beta; what is the penalty that I will pay if I am proven wrong and therefore, they will make appropriate decisions right.

So, EUGDPR is the first major step in global regulation. So, again there are focus areas in EUGDPR, if you look at EUGDPR mostly it is about exclusion, if I want to be excluded, then I have the right to be exclude, right to be forgotten is very given

prominence in the EUGDPR, it is not touched at all the Information Technology Act or Aadhaar Act or any of those things that is one of the reasons why; for example, Aadhaar Act is not able to decide on Jayalalitha, you know because Jayalalitha did not say that I have the right to be forgotten, right. So, we have to carry it long.

Student: (Refer Time: 16:03).

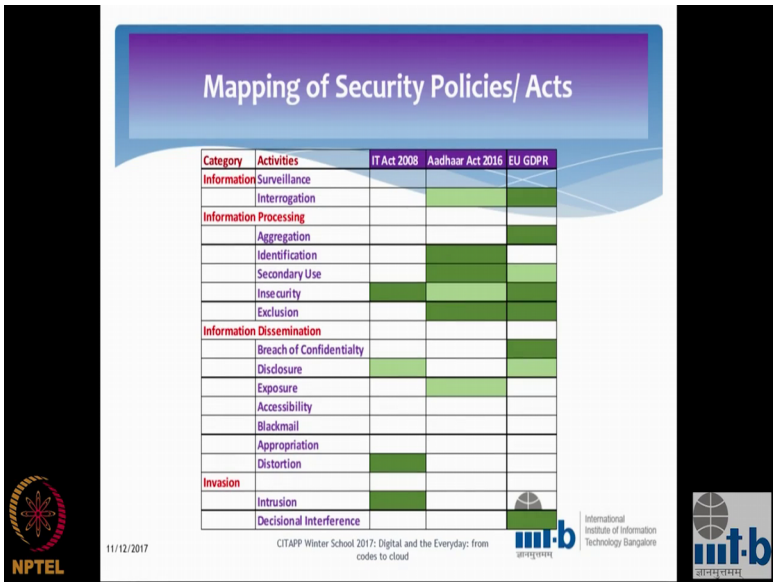
So, that is a there is a problem disclosure confidentiality all these are given prominence surveillance is not given prominence in EUGDPR, because EUGDPR is mostly about private information right and the organizations which deal with private information. So, what we have discussed is there are laws and regulations and these vary in terms of focus and I did not you know ideally, we would like to have a law or our data new data protection regulation bill should cover all the other aspects of privacy that the whole taxonomy has to be covered and there has to be a clear way by which I cannot clay it when my privacy is violated you know which bucket it falls in. So, that it is easier for the judgments to take place otherwise judgments will take long time and therefore, it is.

So, I have tried to map for example, the security policies and acts along these different dimensions you see that there is lot of whites right these whites are not covered. So, it is very very important for us to cover another important thing that that you know Aadhaar Act to some extent covers exclusion right exclusion means either to be excluded or to be included. In fact, Aadhaar Act you can get then Aadhaar number I mean it in fact as a provision for homeless to get Aadhaar Act Aadhaar number that is the inclusion, right.

For example, it is a basically Aadhaar provides you residency, right, if you have residency proof, then you can get the Aadhaar number because Aadhaar you know basically enables you to be you know authenticates you as a resident of the place where you live in right, if you if a person does not have home then he cannot give address right it is not possible to get the Aadhaar number, but Aadhaar Act has a provision for inclusion of people who do not have homes, right.

So, which means it is a landmark act which you know does not exclude anyone right that is the most important thing. So, like this, you know different acts have their own preference.

(Refer Slide Time: 18:07)



I have created and you know the greens and the dark ones or where the it stress is on and so on and so on, there are lots of white spaces that we need to fill up in our regulations in policy going forward the important thing right should. So, there are a lot of ways to deal with this one is through regulation government intervention, right, can it be solved by markets can it be solved by markets like every market right you have the information market there is a new term called I commerce which is coming up right information commerce.

(Refer Slide Time: 18:23)

So, each and every individual can assign property rights to individual information right. So, my name my Aadhaar number mobile number address some things I will trade with Google and for that I will get some money like this can information markets exist there is a lot of research which is going on at this point of time. So, we might come to the stage where we will be willing to sell our information right forgetting some benefits its possible in which case the markets might actually self regulate if I do not want to get the benefit of the market, then I will not sell my information if I am able to get it, then I will sell that information, right. So, it is possible that a market might actually develop for personal inform in personally identifiable information, right.

Student: But.

Yeah.

Student: Why would that happen when then right now able to access all the information in access.

So, so along with that there will be restrictions you know for example, you can define; what should go or should not go. So, those mechanisms have to evolve.

Student: People are already (Refer Time: 19:50).

Correct, it is ok. So, for example, I mean we all know that information has some timeline.

Student: Not only that.

It is ok; I mean the past information may not be very useful as the current information. Therefore, I can create an information market based upon current relation right now.

Student: And also these kind of policies.

Student: European one or the new definition wise you cannot use it.

Student: So, after that?

Student: Right.

Student: Then, this there will be a possibility of.

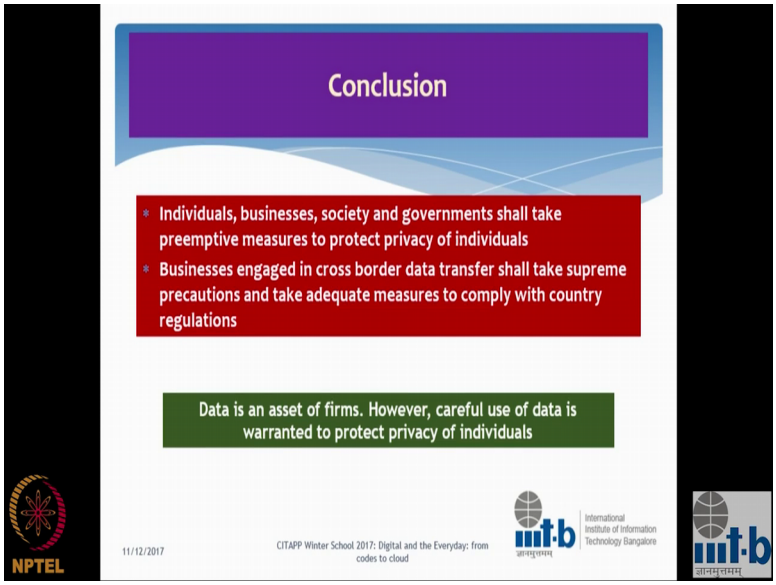
Student: Positive reaction.

Student: New matter.

Right; so people are thinking along these lines because all the time you put the owners and the government to do something government may not have ware with all right government may not have the you know expertise to do that right is it possible that it can be solved by markets that is another view economists are saying that informational is like any other good. So, there has to be a market and therefore, let us use economics to create markets for information, right.

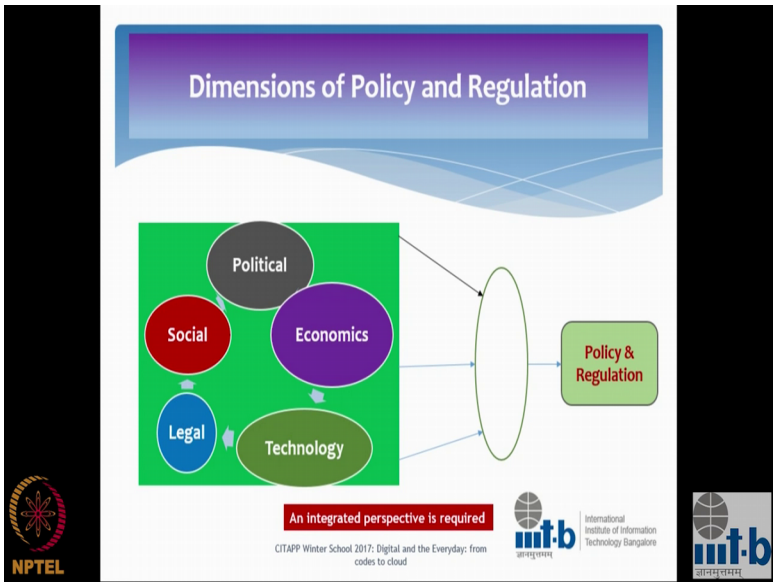
So, those are all some new aspects which are coming up.

(Refer Slide Time: 20:50)



So, this is a data is an asset and therefore, careful use of data is warranted to protect privacy of individuals and so on. So, we touched a little bit; for example, there are a lot of aspects to privacy right.

(Refer Slide Time: 21:00)



So, we discussed about for example, the technology there are legal angles social political and economic angles to privacy and these have to sort of converge in order to create a holistic privacy regulation, but as we know most of these regulations and policies that we craft they cover only certain aspects, but a holistic dimension you know holistic view is required.

So, that is about my talk and you have preferences here.

(Refer Slide Time: 21:30)

So, we might have to look at it if you have any questions you can ask me any questions ten more minutes.

Student: I got.

On time.

Student: Thank you.

So, any questions on privacy and regulation, Shushubi?

Student: Sir, so you talked about the vital product tax.

Yeah.

Student: Tax; so, sir, definitely there can be a tends to erase data from different kinds of databases around product, but many lots of models have been trained right with all these peoples like. So, how already (Refer Time: 22:10) propose like with such data this you cannot really pick one person from a model which is being very.

so, it is very unclear Shushubi. So, to be very unclear you know for example, EUGDPR has this particular provision right, now how the governments are going to do it you know what kind of mechanisms should be implemented is very open, but it is possible I mean the way in which we created we should be able to destroy it, you know, there is a way by which we created it. So, we do reverse engineering we should be able to destroy it.

Student: Sir, what.

So?

Student: (Refer Time: 22:44) process of destroying it is like a kind of (Refer Time: 22:45) track something track train (Refer Time: 22:48) only in that essentially only that only one particular data might not be lost, but several other data as well data points as well.

Correct, so, it is not very clear how the firms will you know accommodate, we have to say if basically solve the first question which comes up right somebody says that I want the data to be erased we have to then take this use case and see how the companies are going to do it right. So, for example, now there is no provision in the Aadhaar Act; for

example, to delete biometric information the person is no more is not automatically deleted there is no validity period for Aadhaar, am I correct, there is no validity period.

Student: (Refer Time: 23:26).

Yeah.

Student: In your last slide, you have mentioned about (Refer Time: 23:30) data set in your view which department of the government should be taking this up.

So, that is a this is a very important question see as ministry of electronics information technology has put out this draft regulation bill telecom regulatory authority of India has already released a consultation paper and it is going to come up with its own recommendation of what the telecom service providers should do with respect to data protection privacy right one of the reasons is that the chairman of the telecom regulatory authority of India was with UIDAI earlier. So, he strongly believes that it has to come under the department of telecommunication right because telecommunication internet and all those things are linked together right. So, it is a very I really.

Student: Sir, it comes under home ministry.

Correct. So, in my view because it is related to digitization it has to have a combined view of the department of telecommunication and ministry of electronics and information technology right and you know it is not possible to prescribe actual solutions privacy violation in each and every case. So, I believe in exposed regulation ex anti can be only for basic things ex anti means you have a regulation which everybody has to abide by right, but that can be very restrictive right it can prevent innovation for example, I cannot say that you should not use secondary use you should not data should not be used for secondary use then in which case all the information markets will collapse; Google will collapse right and you might have to pay ten rupees for each search which you do not want no we want free search, right.

So, ex anti regulation should be sort of minimal right and then I believe in exposed right. So, whenever a case comes up then it has to be analyzed on the merits and demerits and then the decision should be made. Right now, it can be handled by courts of law or it can be handled by competition commission of India if it is relating to firms and the abuse of

the market power by the firms or it can be by the individual sector regulator for example, if it is telecommunication TRAI can take it to TDSAT, the telecom dispute settlement apply attribute.

So, it can be distributed it need not go to higher Supreme Court all the time no. So, we need to have a mechanism by which it can be sectorly decided right if there is a financial breach then same you should make the call right the telecom valuation, then TRAI should take the call if it is competition competition commission of India should. So, I believe in it should be exposed you know ex anti may be very very restrictive because it is very ticy.

Student: Sir, regarding the Aadhaar. So, if you are going to take means if you are going for a new SIM card or something. So, you have to do the Aadhaar verification first time. So, the person like the shop keeper can access the information right he can view the information like if I input the biometrics you can see my personal information.

Student: So.

See the I mean this is not very clear you know the requesting entity see the requesting entity initially when the whole u UIDII was designed it is only for authentication purposes which means the requesting entity can ask whether it is in the database or not yes or no the answer should be yes or no not giving all this date of birth blood group and all. So, today it has been relaxed because if you do KYC for a mobile company the mobile company needs not only yes or no, but also needs address.

Student: Yes.

Right and therefore, they started providing APIs by which you can have access the application program interface by which this requesting entity can access the information relating to address and so on. So, some information they let it private not the date of birth, but address information right. So, they are able to get that right now it is if it is used only for KYC by the TELCO, but if that TELCO sells it to another one like insurance agency or retail store you know you get a mobile SIM from RGO and you get a coupon from reliance footprint its secondary use no. So, if that is used then it is a violation so, but.

Student: Quite restrictive.

They are all quite restrictive, I mean the sense that.

Student: Restrictive.

Not all.

Student: We can see the email ids and alright.

Correct; that is because that is because of the requirements for which it is used you know see if you have direct I mean the Aadhaar Act is not is not a you know act which covers all the sectors, it is only for financial services provided by the government government subsidy services, right. So, if it is only for that then you do not require these kind of information, right, you need to be authenticated whether you are a correct person or not, but unfortunately if it is used for KYC by a mobile company, then you need some more information and therefore, the APIs have been you know are allowing all these information to be sent and so on.

So, it is still in the court, you know, I mean we have to see whether it is.

Student: (Refer Time: 28:32) if I am selling SIM or like five or six SIM cards. So, I can access the all information correct that is what is correct.

Correct.

Student: So, even I can sell it.

Even otherwise, you are access you know.

Student: So, like how.

Even otherwise in the KYC what you asked to fill up all and you can take a copy and do it know.

Student: Only after.

So, there is no violation, I mean see the important thing is whether we are doing the same thing as we were doing it before or much less or you know, it is a compare. So, even

before you had all the information the mobile that retail shop had all the information because you need to fill up that form.

Student: No, but sir if government used to say that it will not equip.

Correct. So, the because mobile companies have started using for KYC which required more than the approval the application programming interface allowed to access this address information and so on right, so.

Student: And they will not value the biometric information not the;

No, biometric information is a ruled out I mean this biometric information.

Student: So, they will see whether it is bank or pan automatically it goes out invariably.

So, you know that case no like dog getting Aadhaar number and all.

Student: (Refer Time: 29:38) sir.

So, you can spoof biometric information and you can actually there are cameras high resolution cameras that can actually mimic you know you I mean the photographs can be captured in such a way that you can mimic the Aadhaar person and then get a you know.

Student: If it is a function latex fingerprinting.

Latex fingerprinting correct. So, you can do latex fingerprinting. So, you can spoof the machines, but technology can evolve in order to minimize the spoofs right.

Student: Some more question some like in interface software skills.

Yeah.

Student: There are some guidelines of that. So, companies that can have so that, correct.

Student: (Refer Time: 30:18) product (Refer Time: 30:19) enterprise security here the same (Refer Time: 30:32) to make sure the software is not (Refer Time: 30:24). So, similarly you have such thing on the app within app space and minimum safe guard you make sure whatever the app you publish is in is in ready to comprise with customer data anything a variable of that internationally you know (Refer Time: 30:40).

See I, So, it is a good I do not know you might want to ask to Mr. Srikanth when he comes here, but in general the minimum checks are being done when you up upload the app to play store or the android I store right. So, they do the sanity check to make sure that there is no vulnerability in the application right the vulnerability that can actually breach the user information.

Student: The apple will does not give a set of guidelines or anything.

It it is there definitely it is there definitely and you you know passing the check on I store is you know relatively difficult, I mean you have to pass all the sanity checks before you it gets approved to be there on the I store Google's check is a little bit loose because it is an open source platform and things like that, but they also do sanity check right, but I do not know about the standards which you know what standards they use might want to ask Shobha, do you have any idea?

Student: No sir.

The standards for mobile security mobile app security, but it is only at the store level that it is done any other questions we have we are almost done.

Student: Sir.

Any questions.

Student: Sir, (Refer Time: 31:49) you mentioned (Refer Time: 31:51), right.

Yeah.

Student: So, is there any (Refer Time: 31:52) in first (Refer Time: 31:54) very advantages for everybody, but at the sudden drawbacks of the;

See the drawback with markets is that markets can become imperfect if it is a comparative market, it is a perfect market, then in you know Adam Smith said that invisible hand will take care of everything you do not have to do anything right who is from economics (Refer Time: 32:14) Cormel.

Student: (Refer Time: 32:15).

Right, so Adam Smith said, but there can be imperfection in the market the imperfection can be due to monopoly power; for example, Google can dictate because it has 901 percent of the search queries right or it can be because of externalities you know for example, the information asymmetry is a positive externality to the firm because it can give leverage this. So, if there is an externality positive or negative externality then it can create in perfectness in the market, right.

Student: Yes sir.

So, if there is imperfectness then the market will not work then government had to intervene or regulation has to intervene. So, we do not know really you know for example, how whether the; I commerce market is going to be perfectly competitive market or not right. So, we need to see it, for example, search market is not comparative it is that is why you has put a penalty on Google right because it manipulates search results and why because it is monopoly power abuse of monopoly power.

So, it is not a perfect market. So, we need to see how for example, the I commerce is going to evolve, but my guess is that there will be more suppliers more you know in general anything to do with information has no great barriers to entry that is why we have millions and millions of apps in the app store. So, if those are there then invisible hand will take care of it will close it.

Thank you.