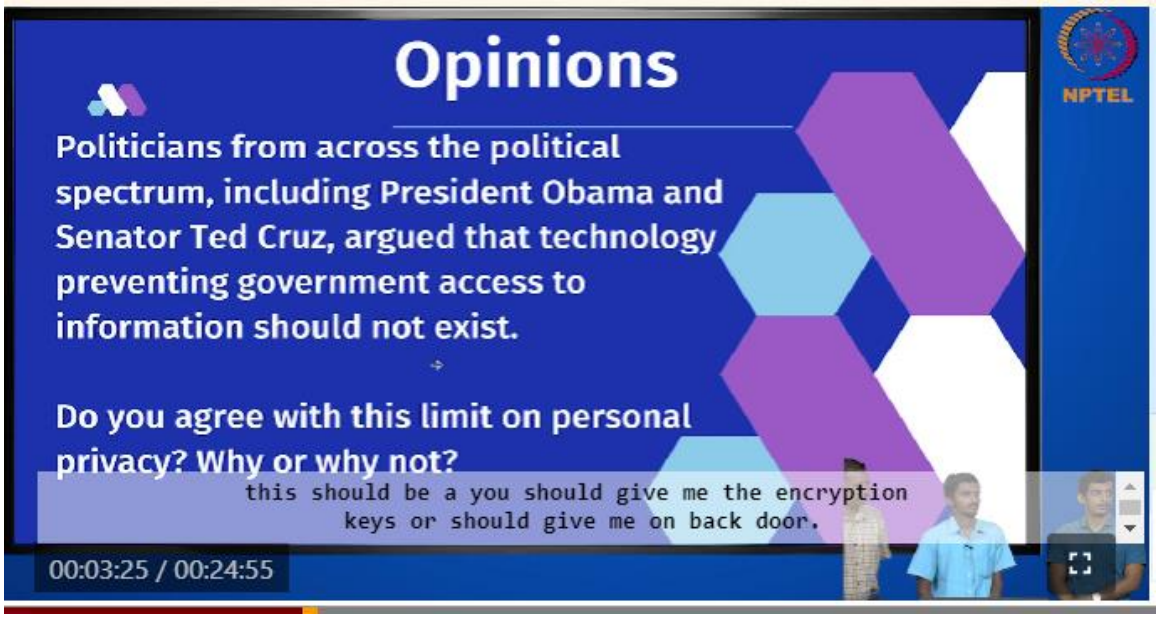
Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 14
Lecture: 41

And, and the reason for government mandating this back door access, we can why where you know why is government so forceful or why they are in such hurry or. So as we see in the criminal investigation they have, like in the modern times we can already know that compared to previous era, like we store data which, in which we store data in form of letters or hot copies in cabinet, cabinets, closets or if you want to protect it, we would have secret place in somewhere else. Like in this modern era of explosion of devices we are storing each and every day of our life in a digital device. So what in, like recently what they as you can, as you can see on screen like in the period of October 2014 to June 2015, the Manhattan district attorney's office could not access potential evidence from 74 of the 92 cases involved iPhone iOS 8 in which we just saw. It was the first iOS which had a default, a full disk encryption. So which it essentially prevented law enforcement officials to prevent, essentially carry out investigations.

So as we can see from the below, this is a quote said by former director Comey. So they had essentially argued that it hinders law enforcement's ability to solve or enforce, solve the problems. So which they argued that it is shielding criminals from getting convicted. It is, it is the one way of convicting or letting them go, like it the only way the digital device was the only key evidence in difference between conviction and letting them go.



So this is a question, like the politicians have argued that you know technology preventing the government access to information should not exist. So what they are seeking is essentially that the company should, whatever innovation or software, like they are providing, like they are asking for a default solution such that the back door, a back door should exist. So do you agree with this limit on personal privacy, why or why not? So my take on this would be that here actually there is also one another point of innovation. So once you say for example, if the company says, in the government says that this should be a you should give me the encryption keys or should give me on back door. So that will actually stifle innovation because as innovation happens the nature of back door might also change, but the government will not be able to.

So there is a mismatch between the government's capability of keeping up with the technology and these companies pursuing innovation. This might actually stifle innovation then. Yes, as you rightly said there are multiple stakeholders in generating or creating technology which was, which is used by all people. So it is difficult to coordinate in, coordinate the developments or the technical analysis of how the back door should be implemented. So it is difficult for the government as well as tech companies to follow this method.

I feel that they actually, if you see this access thing what Sir had also brought out, this Apple, this has been going on for a very long time. Whatever I have read about it Sir, there is hardly any system or technology which has not got back doors incorporated into because such is the world of geopolitics. And if US is leading and it uses, frequently uses all these companies because one of the major revelations of the Edward Snowden case was that the US organizations which they have got branches of their NSA which actively involves itself in actual cyber warfare across states. They had infiltrated Huawei servers, they had deliberately done that, it was the only thing was he brought out all these things in the open that they have been doing it. Now, now it is a misnomer, personal privacy is a fallacy for the public, for us to fight it out on it.

I will give this, yes to some extent in the open domain, in the corporate domain we can live in that, under that assumption that we have some, you know privacy and at least in the open domain within the companies and the corporate it should not be shared. But in all other things, there is nothing which is and it every country does it including ours. Any person for, the moment he comes into media, the IB starts off its file dossier on it. So, it is a misnomer this privacy. So the only thing is for a normal day to day lives, how can we limit our information not spreading in, for that purpose yes, there should be some degree.

Otherwise geopolitics will always demand that privacy or, you know government access to information will always be there. And all these companies whatever they are saying in back door, they have to stay in that country in their country, they have to cooperate and in this thing, there is one particular thing where this, in this Snowden episode was the, there is an organization called the 5 I. The foundation was did in 1941. So, there are 5 country which are signatories to it and they are supposed to cooperate on all signals intelligence. That is why UK is part of it US and New Zealand, Australia, and Canada and they have been doing it for a long time.

The Stuxnet virus, which once Sir had also mentioned, in Iran, was actually developed by this TAO. It is part of NSA, Tailored Access Organization which indulges in deliberate cyber espionage. It has also done the same in our country also, but these are all hush - hush things. It is, the internet itself was developed from the defence, from the CIA side only and frequently in the dark web, they deliberately placed what Sir was mentioning one day was RAS, ransomware as a service. They deliberately placed those programs over there, the malware then all that.

So that it goes into each and every system of ours, whether it is One Plus or iPhone and all this. So it is a misnomer, but yes for the public perception, for normal day to day use like the supermarket case, which we were discussing yesterday in, at least in to some degree some semblance of security needs to be there, medical records and all, but otherwise in the larger world of the government. So believes that in the larger interest of the geopolitics of their particular interest countries, their personal privacy needs limitations. So that is their perspective and our perspective will have to live with it, that yes, we want at least to some degree in the day to day life. Yeah, actually rightly brought out by Colonel Vijay, now a days actually we can say that 100 percent privacy is a that cannot be ensured whether you can say right to privacy is a fundamental right or whatever and again most of these countries actually, they are those countries, they exploit this as a, you know warfare tool actually, which is more actually damage causing actually to the other country, but again the question and the main aspect is the users and the customer.

They should be made actually aware that these things are happening and they should not be kept in the dark. That is the main thing actually. I think there are two sides to it, one is in response to an incident, if government wants to or FBI wants to conduct an investigation and so key information is in a phone and what they argued is if a militant or a criminal died, so the password has died with that person, so password does not exist. So in that specific case, if law enforcement agency is not given access, say by Apple to decrypt the message, they are actually not able to do justice because they are protecting criminals in that case or you know this incident can happen again, so from a safety point of view, you know most of the safety argument for national safety or individual safety, it is also important to have access to the information in the phone, but what you are actually now showing is a very different phenomenon. It is not in response to an incident or it is not for investigation, but for monitoring.

Government seems to be continuously monitoring individual's personal data and collecting that data extensively from within the country and outside the country and profiling people. So that is not for criminal investigation, but it is for monitoring, in which case a backdoor is continuously opened, the government in that case is saying we need backdoor not for investigation but for monitoring. That actually makes the case very different in the sense, privacy should be there, but government should be completely watching what you see and when you say or use the term government, it looks like God or it is some extraterrestrial agent, but we also have to know that government consists of people, individuals and they belong to political parties. So there are interests that can actually be guided by individual interest or political interest and so on. So, we are entering

a territory which is very sensitive in that sense.

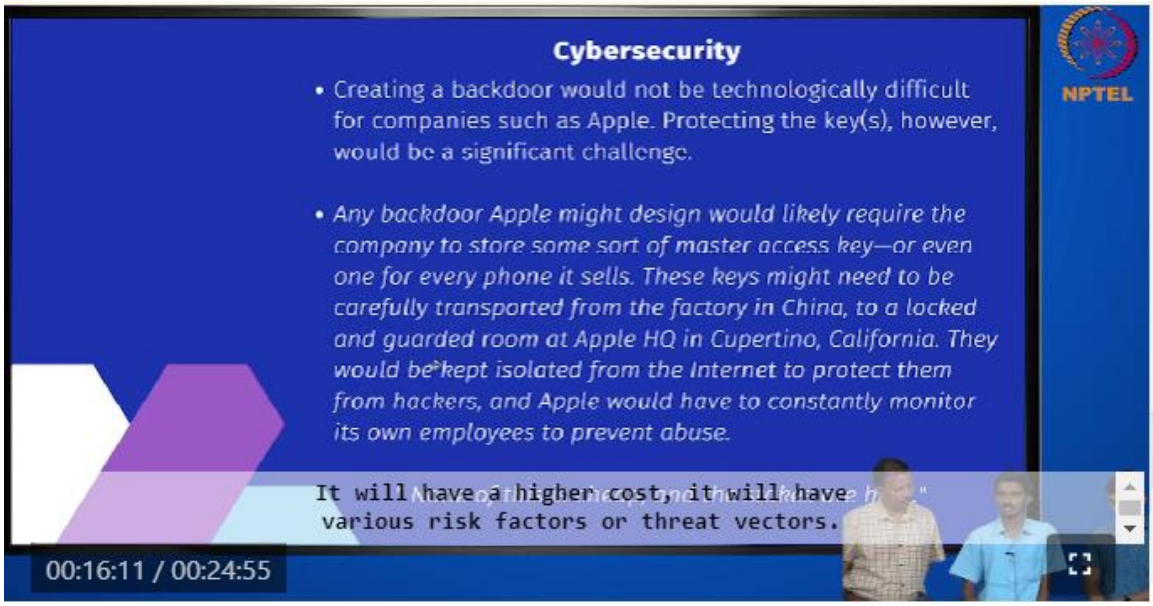
So as a continuation of that, like since Apple did not give access or you know comply with the law enforcement, what they argue is that, you know you can have data's, various data's already, which already you have within various organizations like telecom companies. We just saw like AT&T, Verizon, like they had the access, like they had collected various meta data's related to phones or backup computers on the cloud. So as Sir just mentioned, so in serious threatening cases or you know, the only key like the evidence, smoking gun evidence. So what happens when a victim dies, like it essentially, it is unsolvable case, like there is no further justice or investigation possible. So in US what makes this difference is that, you know in US law enforcement cannot make a person witness to himself, like they cannot force a person to self-incriminate him.

So there are also key disclosure laws like, it cannot come force a person to disclose their password voluntarily. So only if they are voluntary, they can do so. Also this is only present in US, if you compare to other countries like UK, Australia they could legally comply, legally force a person to divulge with their password or encryption key. Similarly, in India if we look at section 69 or of IT Act 2000, it was amended in 2008. So it included a clause such that if you do not provide or comply with law enforcement officials, to decrypt your device, you could be sentenced up to 7 years in prison.

So the other argument was regarding national security. So as we just saw, like in major significant evidences now reside in a phone or any digital device. So as I mentioned before, it is the difference between an offender getting convicted or acquitted. So also since the inception of internet, encryption of Apple and its technology, like various terrorist organizations are using this to essentially hide themselves between, hide themselves behind the technology. So what they are, like here in this case, they have recruited and people so, it was in enabling them to kill people.

So in this case, like due to end to end encryption, it was not possible even for governments or any method to intercept the data so, to prevent any attacks. So next we will see an implication of a backdoor. So if Apple or any other tech company, this you know, it designs a backdoor from the start by design. So what it essentially makes it, it just now it is not only providing a backdoor for the government. So as we saw Sir just mentioned before mentioned, like there are repressive regimes which will use that power to monitor citizens or monitor dissidents.

So who they, who will not agree with their ideologies. So it may use them to prosecute them and do harm. So we have to understand, also there is a presence of hackers. So they will also try so, if they are, if they have knowledge about presence of backdoor they will obviously, try to gain access or exploit that backdoor to gain their financial or any other active intention. So another argument for the government in relation to backdoor is regarding cyber security.

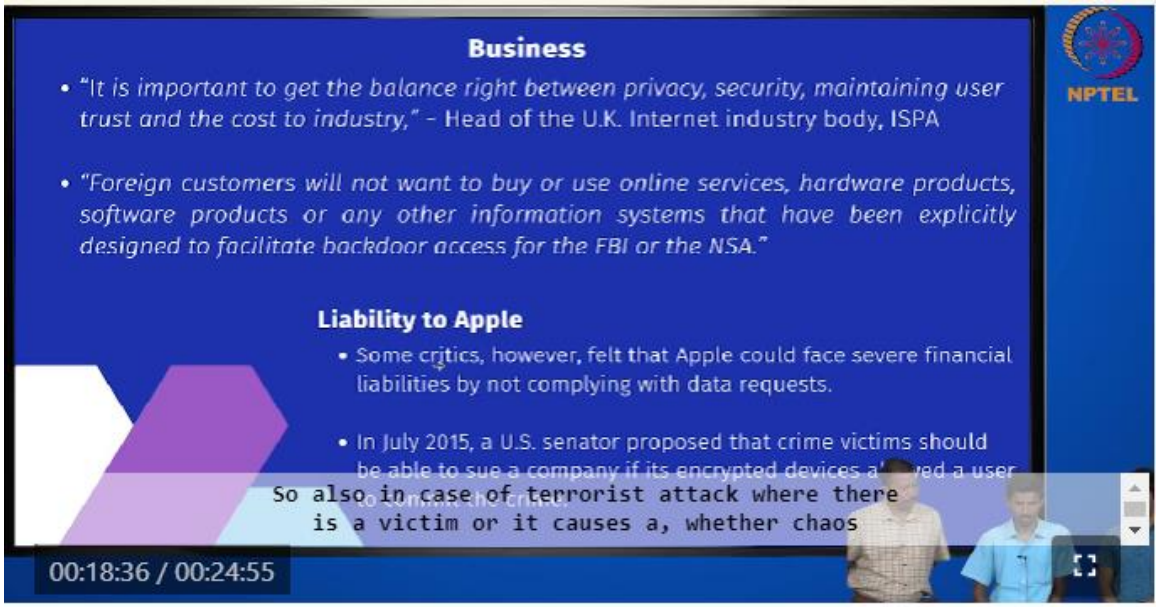


So even though Apple as a company or any company which develops its own product, it does, it is not significant, not say not, significant like. It has, it would not be difficult to create a backdoor, but as previously mentioned protecting that key, this, it will be very difficult. It will have a higher cost, it will have various risk factors or threat vectors. So as you can see, like if we have some sort of master key, like it has to be stored very safe, like it has, like it has to be transferred, it has to be stored and it has to be accessed. So it has various threat vectors within, from which we have to protect.

Also this comes at a very high cost and if you are continuing this for a long time, you would have amassed such a huge data, like one incident is enough to leak all the data. So the stakes are also very high. So the concern is, if any of the, like we said, if any of the private escrowing keys are ever compromised, then all the data which were created by that key is permanently compromised. Also this was an incident, it was lawful interception of backdoor in Greece's national switches, telephone switches that let someone, they did not actually find it, but they, what they did is, they listened to the Greek parliament and

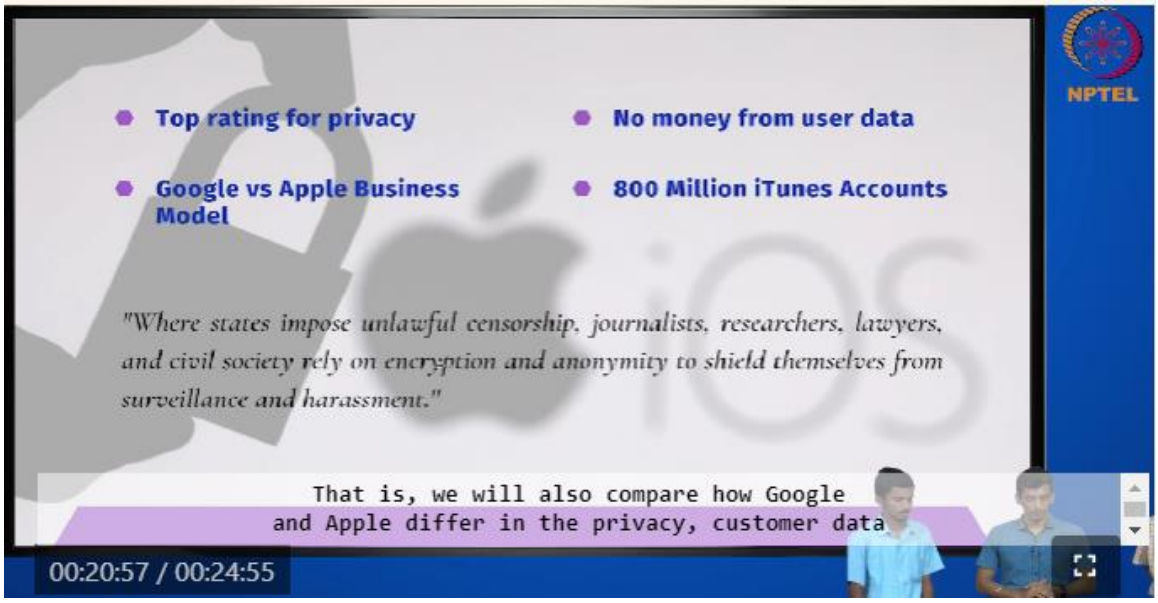
to the prime minister's conversation during a sensitive part of the Olympic bid. So you can understand the impact of creating a intentional backbone even to the governments.

So from the business perspective it is, you know difficult to, for technology companies to coordinate with themselves and create a standard use. So even if, like in the case it mentions that after the incident of Snowden, like companies have even had the choice of creating a, like alternate products which one had a deliberate backbone and other another thing, it was catered to without a backbone. So as a business perspective it also made, even if they complied it, even if they complied it would made decisions in the companies very difficult to coordinate these activities and it will obviously raise cost. So as we mentioned previously, it will, like the foreign customers will obviously not want to use their services or try to go for alternate services which will advertise their features as privacy protected. So also in case of terrorist attack where there is a victim or it causes a, whether chaos in the country, it also could been, like the Apple could be sued in court.



So that it, even though after repeated warnings, it did not comply. So it makes them a lie, makes them and makes them reason through which the terrorist attack happened. So in July 2015, the US senator proposed that the crime victims should be able to sue a company, if the encrypted devices allowed the user to commit a crime. So next we will see the various incidents and the rules and regarding what Apple did in relation to privacy. So hello everyone, we just now saw how many incidents have unfolded which created a trend among of privacy, among the tech giants and Apple as you can see, it is one of the advertisement of Apple and they have used privacy as one of the USP and they have used it for their marketing purpose as well.

Apple received, there were many incidents which showed why Apple is focusing on privacy. One of the reason, some positive factors were there at Apple received top rating in 2015 by an independent organization which fights for digital privacy and it is a very surprising fact that only 9 tech giants were received these ratings out of 24. And also there were, many experts said that the reason why Apple is more focused on privacy or less data tracking is that their business models. Apple in previous case yesterday, we saw that how ShopSense uses data by customer to earn the money or how their profits were there most from the customer data. Apple does not rely on customer data for its profit.



We will understand their business model also. That is, we will also compare how Google and Apple differ in the privacy, customer data and business models. So if you look at the business model of Apple, the major revenue is come, comes from the iPhones

manufacturing and selling them and rest were from services and other devices like iPads and Macs and another thing is that, it is a, it has a global audience and global customers, like it is spread across America, Europe, Greater China and rest of the Asia. And as you can see none of here, none of the revenue is generated from data analytics or user, by selling the user data or it does not rely on the user data, but does that mean that Apple does not store any data. For example, there are around 400 millions iTunes accounts which means that the iTunes accounts are used for all the purchases on the app stores.

So it also means that Apple has a credit card data of around 400 millions customer and with that it also, while registering for the Apple id you also have to give your name or the demographic info. So Apple does have user data, but it does not use it for generating of the revenue. Contrary to it, we look at the Google or Alphabets business model. If you look over here, that then major of the chunk of the revenue comes from marketing and same for the Youtube ads and all the other networks. So we can see that how Google is reliable, reliant on the user data it generates.

So that is why companies like Apple do not need to, do not track their data or user data and that is why it received top ratings from all these firms. Moving on to next case here, Apple as we saw it is a, it has a global customer base and in 2014, it had more sale in China than its US counterparts and that is the reason due to many lawsuits and regulations, Apple had to store, create or store their user data of Chinese citizens in the, in the China itself. They agreed to store the data in third largest data center in China. The reason was that Chinese government did not allow Apple to transfer its citizens data outside of the China. In 2015, China accused Apple that it might be using backdoors and not, it might be your tracking its citizens, by your US government.

So China, so Chinese government asked a security audit from the Apple. Initially Apple was very, Apple did not agree for it, since they, the officials might also seek a backdoor from it but some, many people have said that in the end Apple did agree to China for the audit and they might have also shared the code, it create a lot of criticism for Apple but in the end, Tim Cook released a press release and said that we have never compromised with the privacy and have never allowed for backdoor entry for any government. So there are many instances, not only with China it and with also the US government where privacy was compromised for safety or for law and regulations.