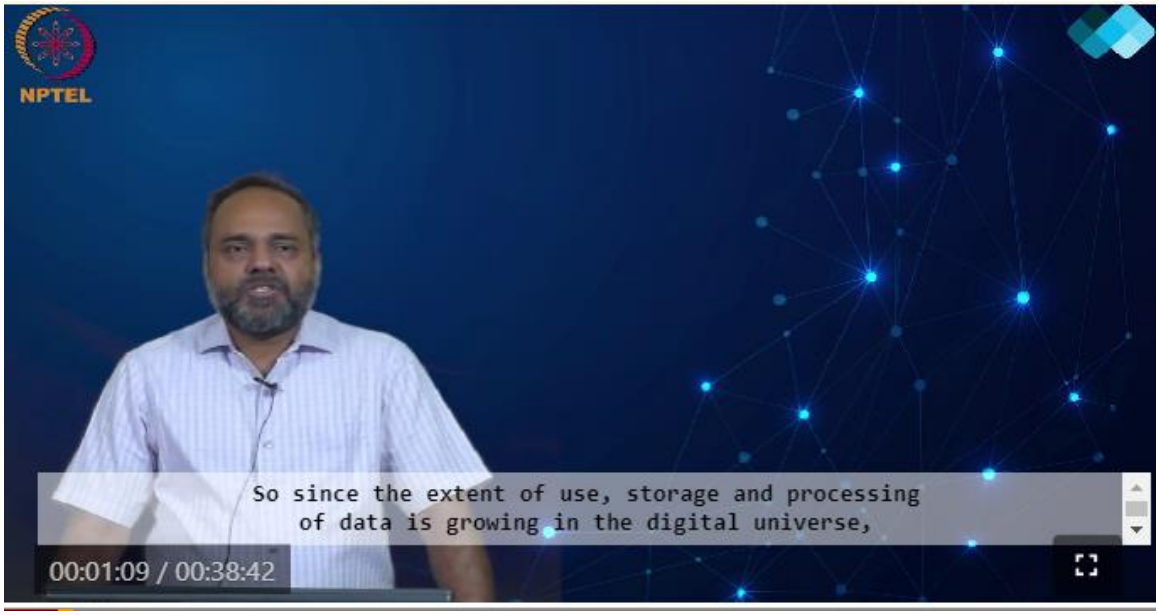
Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 14
Lecture: 40

jhGood morning and welcome back. Today is our last day and we had a long journey through Cyber Security and Privacy. We looked at fundamental concepts related to Cyber Security and Privacy, starting from the CIA triangle and what are management frameworks and standards available for cyber security management and also cyber security governance and we looked at some of the recent examples of managing cyber security and data protection, we found could also be a problem of governance or corporate governance. So since the extent of use, storage and processing of data is growing in the digital universe, it is all the more important to have systems to manage this dynamic complex challenge that organization face. So cyber security is not a static topic, the challenges are ever increasing and that is critical to run business. So these are some of the basic things we understood and as we move to privacy, we looked at privacy at different levels, privacy at an individual level, individuals concern for privacy and we also looked at it, not as a concern but also from an economic perspective.



What is the value of privacy for individuals and we found that valuation is difficult because it is context specific and people behave differently in different context. We

advocate privacy sometimes but we are not willing to pay much for it. So we seem to be having a very contradictory or paradoxical behavior with regard to privacy and that makes it difficult to assess privacy value in economic terms or quantify it. So we saw that there are concepts from behavioural economics that can be used to analyze individuals' privacy behaviour.

For example, if you are used to privacy, if you enjoy certain amount of privacy and then if there is a proposal to remove that privacy, then you have a higher degree of pain, loss aversion and also we saw the concept of endowment effect, the difficulty to part with privacy because somebody is asking we will stop giving you this privacy but you have to pay for it but you will be rewarded. So you see that you ask for a higher reward to part with privacy. So we also saw behaviour and economics are related and it is also linked to emotion. It is not just a rational behaviour because the pain and gain are not just rational but it is emotional also. We can be very irrational when we ask for money, when we are in pain.

So those are the aspects we saw with respect to economic behaviour, with respect to privacy at individual level. We also looked at how trading of data is common at aggregate level, you know how organizations actually value or not value privacy but try to do free trade of private data for strategic benefits, for profiling and for positioning of products, data pertaining to individuals. So private data is very valuable but at the same time we also saw the ethical challenges there when private data is traded but the individuals to which the data belong are not actually in the negotiation or in the picture and therefore that raises different set of challenges. So that we see the topic of privacy is pervasive. It cuts across individuals and organizations, it has personal concerns, it has economic and strategic value and today as we conclude we see a case that is like a capstone, it actually summarizes the entire concept of privacy and security and it is also linked to safety, privacy versus safety is the topic that we see.

So we see many complex ideas or concepts there, as to organizations, business models which are related to privacy and government as an entity which thinks that they must have full control on privacy and no laws should actually prevent them from access to data or intercepting data and so on and so we see major incidents in the decade that you live in when there was espionage charges when the kind of data that government collected and it became public. So government as an entity which is the big brother, that image of the big brother is something that we can actually see because no laws applies to government. They can do anything to get data, aggregate it, analyze it and profile individuals. So we see it is a complex phenomenon and the elements of this, that is what we are going to see in today's two cases. So I am sure you are ready with the cases, there is lot of background information and it pertains basically to Apple which, a company which has risen to the top in terms of

market valuation and market capitalization.

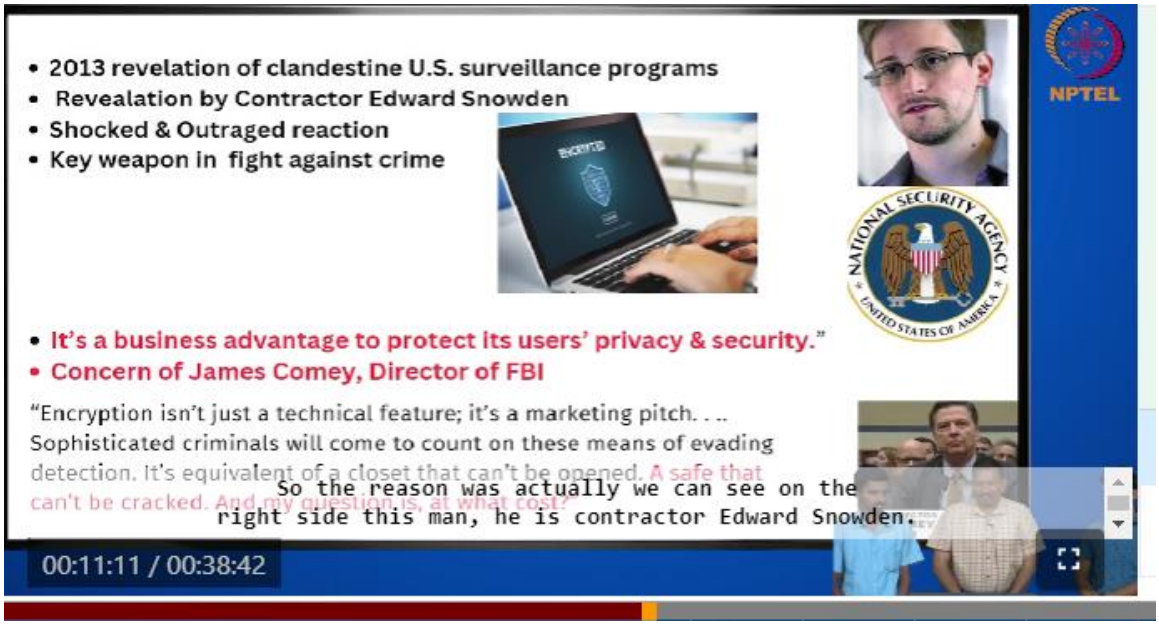
You see the company has grown phenomenally during these days and you see, we also get to analyze what is the company's business strategy and what drives certain positions that a company takes etc. So we look like the company is all out to protect your privacy like God or like what government should be doing, the company seems to be doing but the government seems to be taking the opposite view, you know privacy is not very important. So very interesting arguments and our role is to analyze as to why certain positions are being taken. So good, so I leave it to you. So my role is over.

So I invite the team to come, present the case and lead the discussion, case A and case B. Thank you. Good morning everyone, today our group number 4 comprising of myself Colonel Jagvir, Prasad Deshmukh and Sanjay, we are going to present the case study Apple - Privacy versus Safety, part A and then its sequential part B. So we all know about Apple. It is the largest multinational company of America with the headquarter located in California.

It was founded on 1st of April 1976 by three person Steve Jobs, Steve Wozniak and Ronald Wayne. And then Apple they offer various kind of products right from iPad, iPhone, Apple watches, ear pods and many cloud based services. So this case is actually all about, on one side we have right to privacy and we know that is a fundamental right, although that is not absolute right and on the other side we know all the surveillance government agencies and they look for SS basically on the name of national security and they look for front door entry and back door entry and we also know and we have studied that is the privacy paradox, we also look for privacy and on the other side we also want to share our information on the social media post and all. Then we have also studied the prospect theory and the endowment effect and the willingness to pay and the willingness to accept, that is all part of our individual behaviour characteristics. So as we can see actually this man is the Tim Cook, the CEO of Apple and on 9th of September 2015 he is addressing the media, that is public and Apple they have actually launched a newmodel iPhone 6S which is a upgraded version of iPhone 6 and it is having the enhanced security features the default encryption system and on the top we can see the statement by the CEO Tim Cook and that reflect the concern that, that is having about the fundamental right to privacy for the customers and the users and the down below actually we have got a statement by Cyrus who is a district attorney, the law enforcement agency and again he shows the concern about, you know the national security and bringing justice to the victim and their families and the concern for all these national security agencies and all.

So that is there. So again the question arises actually, why this debate? What was the reason for this and why was the reason for upgrading this default encryption system in

the new model? So the reason was actually we can see on the right side this man, he is contractor Edward Snowden. He was one of the contractor in National Security Agency, NSA and on actually on 5th June 2013, he revealed and leaked in the media about one of the clandestine US surveillance program by the name of PRISM. So he revealed in the media how this NSA, they were collecting all types of information data about the customer, about the users from the companies whether they were emails or the chats or other social media posts and the phone tapping. So obviously it led to all the customers, users and the company they were in a mood of, you know shocked, really shocked and at the same time many foreign leaders, they were outraged that how their phones were being tapped without their knowledge and their email, chats and official as well as personal data.



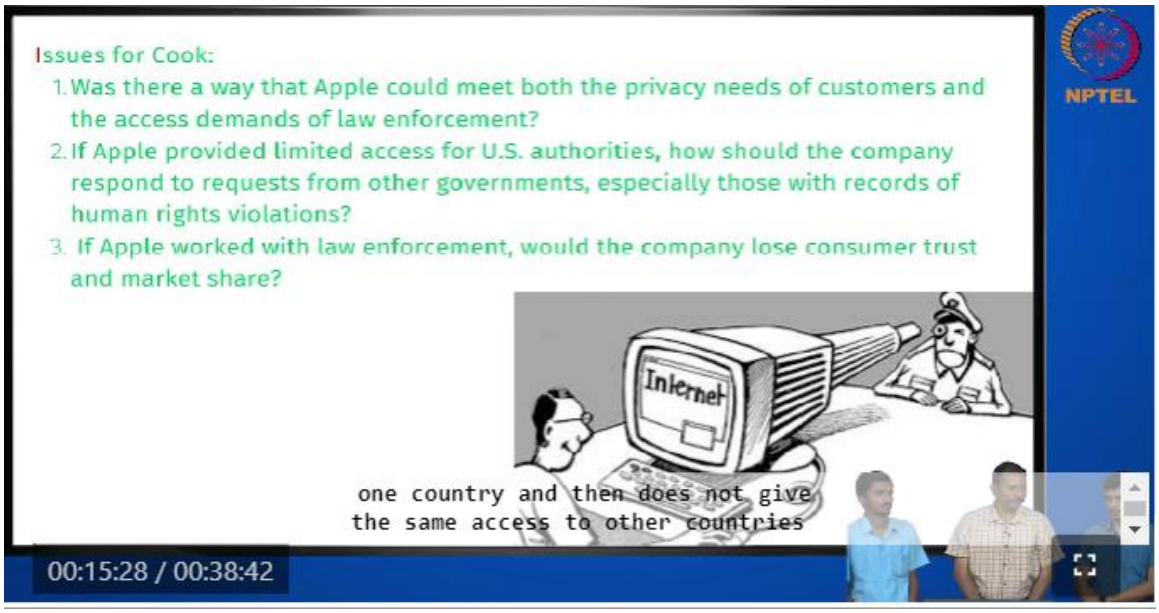
But again on the other side all these government agencies, they defended and justified this surveillance program. They said it is basically a key weapon in a fight against crime and that has to be done. So again on the down below we can see this man, director of FBI, Federal Bureau of Investigation, James Comey. So he gave a statement. He said basically all these companies, the internet companies and the telecom companies, they take it as a business strategic advantage to protect their users and the customers on the, for their privacy and security.

So that is there. But again he said that when these encryption models are there, it is equivalent of a closet that can not be opened or safe that can not be cracked and he says at what cost. So here we can discuss actually a hypothetical situation. Suppose there is a victim of a crime, say murder and that victim dies and the government agency, they knows they can crack the case and all the proof and evidence there lies in the emails or in the mobile but again that can not be opened because it is encrypted. So how to give justice to

their family? So that is actually just one of a very general hypothetical situation.

So coming on to this case that is Operating System 9, the new version, model that was launched, it had actually two factor authentication. The upgraded encryption feature and the length of passcode. That was also increased from the earlier four digit to six digits. Again all these surveillance agencies they were obviously not happy. They were very very displeased because they are making it more difficult to crack and open the system that was there and they are concerned about the national security.

Now as a CEO, actually Tim Cook, he had three issues that we can see here. Firstly both the agency, that is the customers, users they had a right to privacy and on the other side all these law enforcement agencies they look for, you know the national security and cracking the cases. So how to find a balance midway so that both the requirements can be justified and both the requirement can be met because both are actually right. And secondly, the second issue was basically in case they give limited access to the US authorities. So obviously similar requests are going to come from other governments.



So how to handle that and especially the request from the notorious governments having records of the human rights violations, that is the second issue. And thirdly, in case the Apple, they works with the law enforcement agency, they cooperate with them, then would that mean that the company is going to lose the customer trust and faith and that may result in the, you know decline or market share falling down. So just to ponder about it, think about it. Anyone having any comments or views about it? See one thing regarding the second issue which you have pointed. So if Apple, I mean obviously if Apple provides

the access to one country, let us not say US, one country and then does not give the same access to other countries then means Apple is now deciding which country is a good country.

So a company is now deciding, is playing moral judge here. So that will not be acceptable. Yeah, basically because they are having business globally all over, all the countries, so obviously they cannot discriminate and then they will have to agree the comply with the demands of the other countries also. For that issue I would say that they would have to have only one policy for all countries. What about the third issue? But I think although Tim Cook is highlighting Apple's privacy policy and showing himself as an evangelist, as a great ideal that the company is trying to protect.

It looks like an ideological statement. But didn't the same company let Chinese government do audit on its data center which concerned with the data of Chinese individuals? So it had a, when Chinese government wanted access to the data apparently they have given access to it. So how can they say in the US, we will not allow backdoor because they have already done it in China. What do you think about it? Yes Sir, you have rightly in fact pointed out they cannot have different, you know policies for themselves and for the others, rightly brought out. So we will be going all three actually these issues as we progress the case.

So what happened actually this Edward Snowden, he was one of the contractor in NSA and on 5th of June 2013, he revealed all the government, revealed all the files and the secret files and how this government, NSA they were carrying out this, you know data collection on the name of national security and this program PRISM that was there. So NSA was collecting all sort of data records whether that was phone calls or data transmission not only within USA but also USA and other countries and all the telecom providers such as AT&T and Verizon and all and they also, you know compelled internet companies, in fact nine companies to share the data legally that was there. Then after that actually Yahoo and many other companies they went to court and they challenged NSA and the government agencies and not only NSA, in fact they had a joint operation with UK also by the name of MUSCULAR and they were sharing and carrying out a joint operation and we can see that all sorts of data was collected and then what happened actually there was mixed reaction from the public and from other agencies. Snowden, he was you know hailed as a hero by some fighting for their right to privacy and some called him and labeled him as a traitor also.

So that was there. Again the US government, they filed criminal charges against Snowden for the theft of the government property, the secret files and sharing them and also he was booked under the Espionage Act. That was there, that is spying against the government.

And then this guy Snowden, he actually tried with many countries and finally he was successful and none other than Russia. They provided him temporary asylum and actually today latest he has got actually the permanent residency from Russia as of now, that is there. So what happened after this Snowden effect, obviously the industry and the response.

They were all affected. The Cisco, they you know, they witnessed a lot of, you know drop in their customers in the sale in China, the Qualcomm and the HP, their sales declined and the Chinese media and the government, they actually accused Apple of sharing all their secret data with the US agencies, that was there. Brazil, they carried out some kind of localization of data that we studied in the class. So they shifted from Microsoft Outlook to a domestic company for their email and similar things. And again the American cloud company, cloud based company, they suffered a lot of losses because most of the other companies, they shifted from that. And then we are actually surprised that some of the non-US companies, they exploited the situation and it was a, you know business opportunity for them, as they offered to its customer the NSA resistant services and they also claimed that they will not be sharing data with other companies or the government.

Some of the survey results. Some of the surveys which were carried out in 2015 that reflects and shows that majority of the Americans, they were actually not confident about the security, about regarding their communication or landline or cell phones or the emails, that was there. And 25 percent of the respondents, they said that after this incident they had changed their technology, either mobiles or the other services and all. Then 74 percent believed that obviously they give more priority to their privacy and freedom in exchange for the national safety. And only the 55 percent of the users, they were actually happy lot. They were still satisfied with the security features and the safety features of their mobiles and emails and other things.

And again as we have already, you know discussed in the class also, the prospect theory and the endowment effect and willingness to pay and willingness to accept. So you know, we were actually, some of the people, they were too willingly to disclose all their data for the financial rewards or better improved services but they were still concerned how the government and that companies, they can exploit their data. And again there was, you know many differences between the behaviour pattern in Asian countries versus some of the European countries or even Canada. The Asian countries, they were too willing to trade their data for the improved services or the financial rewards whereas the German and Canadian, they were not that willing. So these are some of the graphical representation of the survey.

So we can see that basically, here we can see the dark shade that pertains to slightly or

not private and the latter is moderately or very private. So here is USA then European, China, India and Brazil and on this we can see various aspect financial, children health, call history, location, web visits, purchases, social network, name, age or sex and brand preferences. So under financial we can see basically, you know very very less percentage, they consider slightly or not private, where majority of them in USA, they consider it as moderately or very private. But similarly in case we compare it with India then the percentage of people, you know which are considered as slightly or not private is more as compared to USA. Similarly in case we see, you know the age or sex, like this age or sex in USA majority of them, you know they consider it slightly or not private whereas in India or the other country it varies.

Similarly the case of the web visits, there is a different kind of pattern among USA, China, India and Brazil, that is there. The other kind of survey that was basically how much do you care that only you and whosoever you authorize, should have access to this kind of information. Again we see the pictorial graphical representation. It basically have three classes.

That is very important. The darker shade and the middle one is somewhat important and the lighter is not too important. So in case of content of your email, basically the 68%, they think that it is very important whereas only 13%, they think it is somewhat important and 15% are, they think that it is not too important. Whereas once we come to, like this place you are located when you use internet, then only 54% are there which considered it a very important aspect and 16% are there, they think that it is somewhat lesser important and 26%, they think that is not too important, that is there. Again in case we comes to this, like something called a times of day, in the down times of day you are online, then only 33% are there, which they think it is very important, it should only be visible to yourself or whosoever is having that authorization to see and not to others, whereas 45% think that it is not that important. So what happened actually is still 50% of the respondent, they actually claimed they have been a victim of data breach at some point of time in their life.

But it was again surprising that most of the, you know respondent they think that it is only the responsibility of the government or the companies to basically ensure the safety and security of their data, that was there. And surprisingly 62% were still who never change, who did not change their password that regularly and 39% were there who did not use a password at all to protect their mobile devices. That was just some of the results of the survey. And down below also we can see actually this, you know some of this.

We summarize all these things. So what happened after that in December 2013, the senior executives of the many of the telecom companies and the internet companies, they

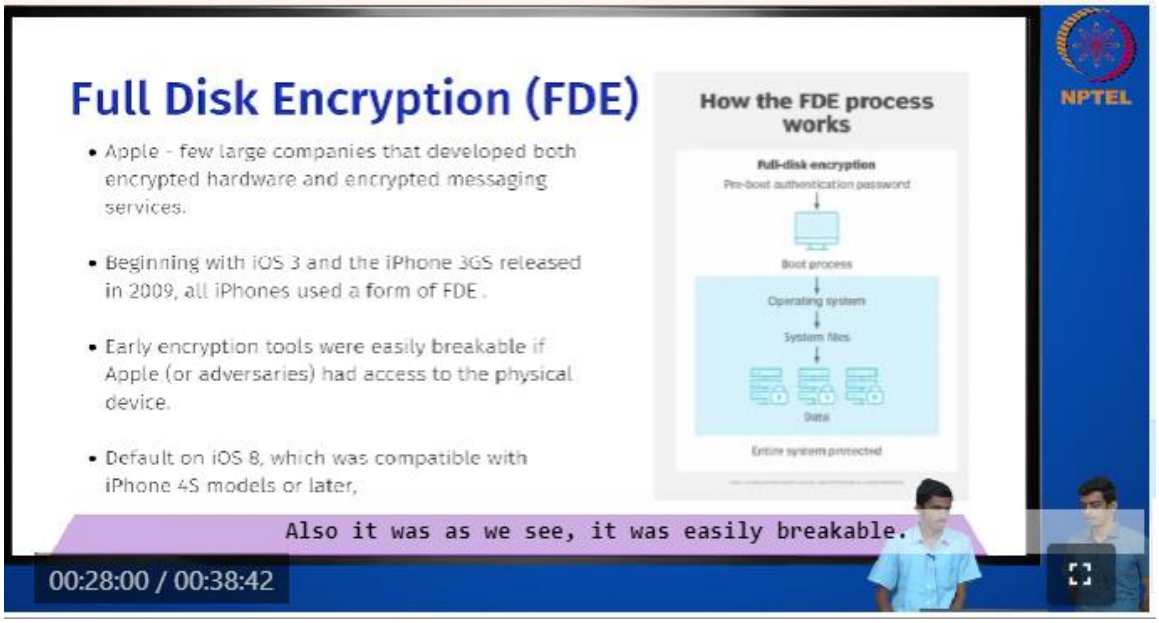
had a meeting with the then US President Barack Obama and they discussed with the consequences of this NSA surveillance program. And after that actually all these internet companies they started to invest more in their privacy controls and encryption models and all. And then Google, they planned to encrypt the traffic exchange between their data centers. IBM, they announced for building data center outside USA, shifting outside USA, so that the US government cannot carry out this monitoring and surveillance. And then Apple, they also planned to go out of USA, in Europe.

And many companies, you know they started sharing with the users, with the customer how the government and when the government is asking for the data and when they are sharing data, that disclosure and all. Now we will see the technical details about what Apple as a company did for encryption. So we already know that recent this websites we visit often are secured now. But in the previous days we just used HTTP, which was an unsecured protocol. So which means that anyone who can intercept in between can snoop through the data.

So after the encryption, we already know the symmetric encryption which is also not very secure in the, not very secure. So next came the public and private encryption which is basically, here we use two sets of keys to encrypt the data. We use a the public key to lock the data and the data gets transferred. So which means that nobody in between can decrypt the data and see it. So for decryption of data we use private key to decrypt which will be in the possession of the recipient.

So Apple is the one of the few companies that initially developed both encrypted hardware and software services. So as we can see beginning with iOS 3 and iPhone 3GS, they have implemented full disk encryption, short form is FDE, from all the way back in 2009. But the problem with this early encryption tools were if hackers or some adversaries or even government agencies can break, if they get physical access to the device. And also what Apple did was the, before iOS 8 it was not default like the user has to intervene and choose this option.

Also it was as we see, it was easily breakable. So from iOS 8 which was compatible with iOS iPhone 4S or later, it was made default. So all the users can enjoy, even non techie people can enjoy the privileges of full disk encryption, in case the data leaks. So after that Apple made a very drastic change in regards to encryption. It made end to end encryption in the form of 5 messages. It made Apple very popular due to its nature of the data not being visible to, even to Apple or any other third party in between.

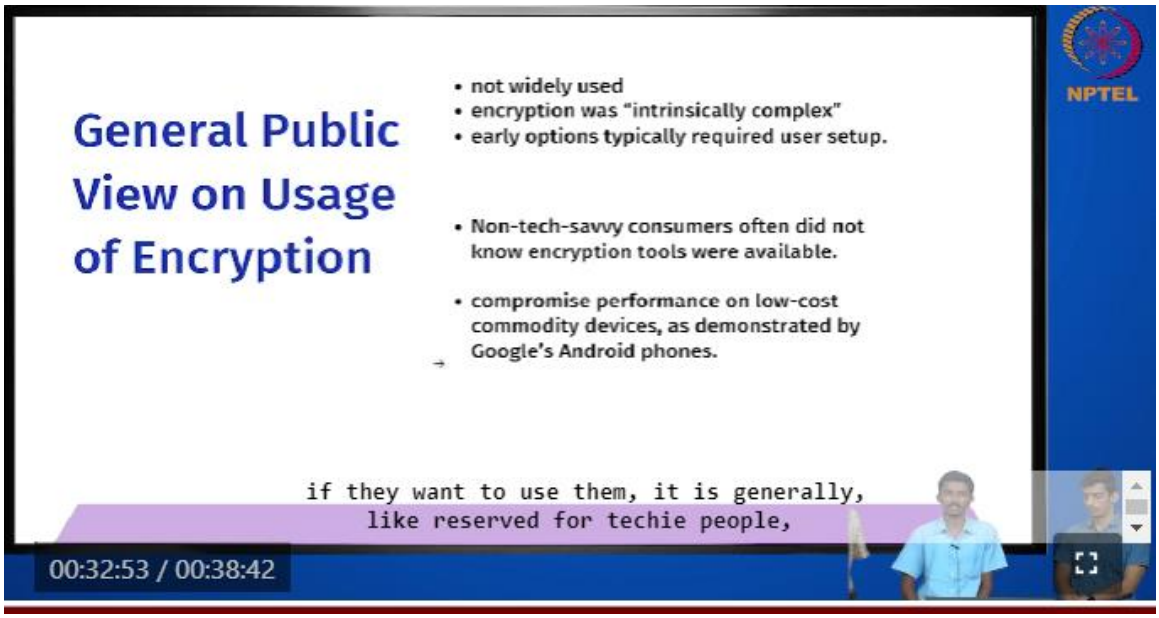


So in this encryption scheme, what it does is the keys were generated and stored on both is end user of devices which is the sender and the recipient. So even the Apple cannot have the master key. So even if Apple, if Apple wants to decrypt it, it cannot do so by technical means. So these are the things I just said and the master, like the internal encryption what it does is, when the user creates pass code what it does is the pass code is combined with a unique key. So it will be, so it will be made unique to each user and each device.

So it would not be common, like Apple cannot have a master key which will unlock any iPhone model. So the like, we can say this is as a not a problem, but this is a inherent feature like the hacker could attempt to find a bug in the encryption algorithm, but the encryption algorithms are already, you know very robust and very reliable and secure. So what it essentially made is, it absolved Apple of its liability in the, like if government agencies wanted Apple to, even if somehow government agencies force Apple to do, like decrypt the device it cannot do so, because they do not have any means of decrypting the device which was explained by Tim Cook. So these are the data's which Apple and iPhone as, and operating system can see. As we can see, the iPhone can access email, calendars or contacts from outside providers and it also sees, like health data and usage access which will be health data and what the next category, we can see the categories of data which is, which Apple can see, but it is made anonymous.

So it will be more private, so that people would not worry of searching sensitive or personal things and the next thing we can see that similar to, like the revenue generating

streams like iTunes or Apple music which will increase the personalization and recommendations which will generate their revenue. The last one, it is although, it is technically Apple can read it, but it promises not to read which are, which are emails, calendars, contacts, photos, bookmarks and passwords and backups and after Apple's introduction of internal encryptions and default privacy protections, Google made the decision of encrypting their Gmail services in 2010 and it is email service and in 2011 even it extended to Google searches and in 2013 it also extended to cloud storage and it also made the introduction of FDE in Android 2 with the start of Android Lollipop, but the problem with Google's implementation was, generally Android is, Android's consist of various demography categories of devices which include low hard, low capability hardware. So which made the penalty, like it impacted, the low performance, impacted the devices with low performance hardware. So Google what it did, it added the encryption feature in its operating system by default, but it gave the user a choice.



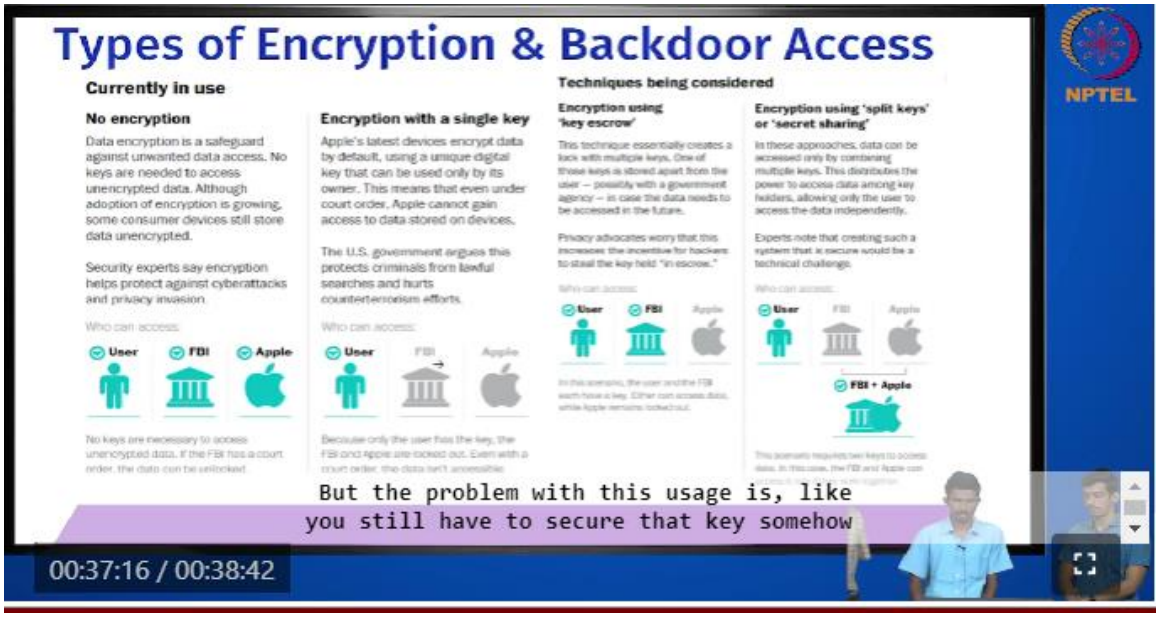
It did, it did not make it as a default, like default option. The users have to enable them by their own choice. So in general even though encryption tools exist, and various methods available, it is in, you know in general public, like very few people are aware of encryption tools and they, even if they want to use them, it is generally, like reserved for techie people, like who those who know how it works or what its limitations are. So it is not user friendly as one would expect them to be and also as I said using this on low commodity devices which will have a performance penalty. So it is generally avoided by most people. So in the case of government looking for backdoors, we can see as already discussed by Sir, many countries all around the world have reason with tech, big tech companies to have some sort of back door access, to enable them to solve criminal

investigation or other terrorism, to prevent counter terrorism activities.

So in US they, what they wanted was they wanted a technology that was embedded in the product itself which would enable them to get back door access anytime. So due to that people were, you know people were very reluctant and very private about their data but what government did, government argued was that they had previous laws which already set a precedence which they argued that it was already existing why cannot be amended, why cannot we have a back door instead which is a CALEA Act, it was enacted in 1994. It is a communication assistance for law enforcement which basically granted them powers to intercept or wire tap any communication between any people and also recently it has been amended to such that it also includes the VOIP, voice over internet protocol calls too. And UK, they are similar in stance, like the PM David Cameron said that if we are using in extreme situations like in case of any terrorist attacks, we are already using means to access or intercept communication. So why cannot we do that and also, like what is the need for full privacy when there is lives involved.

So in China they made, they mandated back door access in 2015 to see, like combat counter terrorism but then in contrast all these countries we can observe that EU block countries have different stance of, on encryption or looking for back door access. In case, in this case we, they have even promoted and supported the use of companies or firms and they in even in their government services to, for to use encryption and to use encryption. So government, there is, like these are the types of encryption and back door access like the first, the first two columns you see that these are the types of encryption currently in use. So, in one case we cannot, like we have an option of using no encryption at all but the problem with that is, anyone can access the data, from bad guys like even we can deliberately accidentally leak our own data's.

So, it is not protected by default. So it is, even if government agencies or any firms or users can access we can see that all the three stakeholders can access the data. So, in the case of end encryption we just saw, like if Apple encrypts with a single key, the issue is that the other, the third parties other than the users are locked out of it. So only the user have access to the data's which they possess. So it does not align with the views of the government which they, which they argue that it protects the criminals. So, in case of back door access what governments wanted was that they wanted encryption in the form of two techniques.



The first one is called key escrow. So what they are doing is that, they are essentially creating a set of multiple keys. So, one key is held by them. So whenever they want access, they can use that key to unlock or decrypt the data. But the problem with this usage is, like you still have to secure that key somehow because if the key gets stolen or leaked, the entire data, entire data that were encrypted by the key will be compromised. And in this case we can see that since the Apple is providing the key to them like Apple is also locked out and it is used by generally the hostile government agencies now defaultly user has access to it.

And the second option was encryption using split keys or secret sharing. In this case we are, what you are doing is essentially creating a lock which has multiple keys, multiple keys, but the issue is that we have to use both the keys to unlock the device. So, the presence of multiple keys to sequentially unlock, sequentially unlock the lock. So this provides a greater degree of protection. So that even if one key leaks the, still the data is somewhat secure, but the issue with this creating this with collaboration of various government entities, firms and various devices it will be a problem or a challenge. So this is Star Wars reference, you are able to understand.