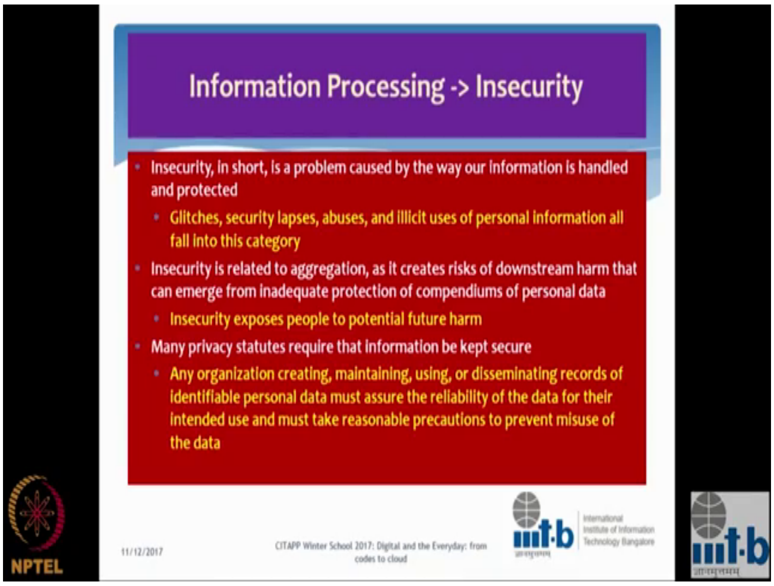
Digital And The Everyday: From Codes To Cloud

Prof. V Sridhar
Department of Multidisciplinary
International Institute of Information Technology, Bangalore

Lecture – 07
Data Protection & Privacy Regulation in the Digital Era Part 02

The third one which gentlemen here talked about it is insecurity, right. This is most of times privacy is associated with information security; which is also you know partly correct, right. What is insecurity?

(Refer Slide Time: 00:29)



Information Processing -> Insecurity

- Insecurity, in short, is a problem caused by the way our information is handled and protected
  - Glitches, security lapses, abuses, and illicit uses of personal information all fall into this category
- Insecurity is related to aggregation, as it creates risks of downstream harm that can emerge from inadequate protection of compendiums of personal data
  - Insecurity exposes people to potential future harm
- Many privacy statutes require that information be kept secure
  - Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

Everybody says that Aadhaar database is prone to hacking and therefore, we should not have a centralized database where all our biometric information is stored. Now if for example, this centralized information repository. CIR is hacked, is it a violation of privacy?

Student: Of course,

It is a violation of privacy.

Student: Yes

How serious it is?

Student: Very serious.

Very serious. So, who should take responsibility for this information repository to be secure as secure as possible?

Student: Completely (Refer Time: 01:01) every stake hold right.

Every stake holder; so, for example, we can have different mechanisms, right. We and I approach (Refer Time: 01:12) prakash also we talked about it; quite some time back. So, why we can not we have other biometric information in your cell phone. Not in the centralized database. So, centralized database, we know that it is prone to hacking. It is may be insecure, and if once hack then it can hack 1.3 billion Aadhaar cards, right. Why can not you put the owners on the user?

Student: Yes

Put it on mobile phone or some device you give a some device small device, right. Which will have all this biometric information. And you can authenticate on that itself. You know, you do not have to really depending upon the centralized repository in order to authenticate, right. Is it a suitable solution?

Student: Economic feasibility.

Economic feasibility and where should the where is the owners now?

Student: (Refer Time: 02:05)

The owners is not with the government owners is with you right. So, you have to take responsibility in order to make sure that your biometric information is safe, and secure sir.

Student: This is more prone to we had or more insecure.

More in secure. That is the reason why the Aadhaar has.

Student: All the state has it is own resources.

Right.

Student: they have put it more risk by (Refer Time: 02:22), but the individual who I may not be able to secure my data, if it is with me, what if it gets hacked you know there are millions of Aadhaar card get hacked like a if there is hacking being done. And what is the like you just lose your device and; that means, just like 10 people 20 people good data is being lost.

Student: So, you are just your privacy and my privacy. I mean, even if you are using 6-time privacy, privacy doing the like how you.

So, it is the owners right. So, for example, if all of us. So, should there be a provision in the Aadhaar act saying that if you what your if you cannot protect your biometric information, put it in Aadhaar database. If you can out it if you are able to secure your personal biometric information keep it in your hand know.

Student: Yes sir.

So, there should be a should there be a provision of Aadhaar acts such as this.

Student: Yes

However, Aadhaar act does not provide that, right. So, could there be a policy which says that it is up to you, if you want to put it on centralized database put it government will take responsibility to some extent in protecting it. But if it gets stolen, usa stolen along with millions of others, right. If you want to take the ownership take it in your hand. I will give you a biometric device you purchase it for 10,000 bucks and then put it your biometric information on that, right.

You do all the authentication locally, possible, right. But this requires policy intervention, right. And this is a (Refer Time: 03:42) is a clear distinction of what privacy is what we are talking about, right. This is information insecurity, like what you say you said, right. Your private information is being hacked I have to protect it. Now who will take the responsibility the states, or a firm or an individual like you and me, right. And the important thing is the information once stolen need not be used immediate. It can be used after a long time.

Student: Yes.

Right, and therefore, there is a temporal aspect to information insecurity, right. And this a violation of privacy. So, on a scale of 1 to 10, how would you rate? I have to again ask you; how would you rate the information in security as violation of privacy? Can this be sort of compared to for example, the secondary use and the aggregated information that we discussed. Is it possible to prevent information insecurity? Is it possible to prevent?

Student: Yeah.

Sir, is it possible to prevent the information in security? Is it so everybody including (Refer Time: 04:44) saying that biometric database is a 100 percent tampered proof. They are confidently saying know, CEO of uidii pronounces that it is 100 percent safe. So, is it possible that we can that, we can do that?

Student: May at the time, at the time.

Ok.

Student: When we give all the.

So, here we have technology to assist us, right. So, this is using technology it is possible to find the solution, which is not 100 percent perfect, but it is 99.999 percent perfect, right. So, that we can keep the information secure, it is possible, right? Unlike in the case of aggregate or secondary use, where technologies actually maligned the purpose, here technology can assist the purpose in order to protect the informations security of the individuals right. So, on a scale of 1 to 10.

So, what about you sir?

Student: 8.

8. So, we have one for aggregation, and about 7 for secondary use, I think.

Student: Something like this.

Something like that.

(Refer Slide Time: 05:52)

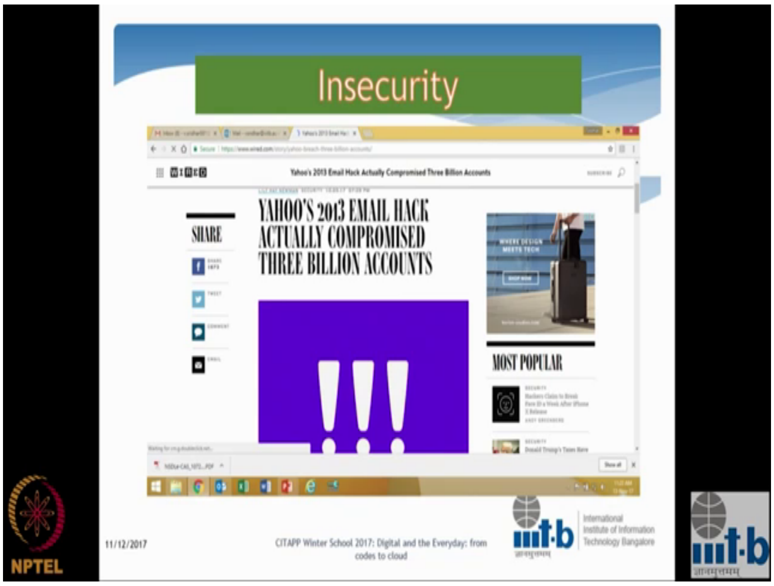
WELL THE GOOD NEWS IS THAT THE SYSTEM IS COMPLETELY SECURE. NO ONE CAN GET INTO IT
AND THE BAD NEWS?
IT'S BECAUSE IT'S CRASHED!
CARTOONSTOCK .com
Search ID: form1093
NPTEL

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

So, this is normal way of life. So, everything you protect finally, you crash yourself; and this we know right.

(Refer Slide Time: 06:02)


Insecurity

Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts

YAHOO'S 2013 EMAIL HACK ACTUALLY COMPROMISED THREE BILLION ACCOUNTS

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

Student: Yahoo.

Yahoo’s valuation. Just fold it to millions, just because of this particular hack which happened, right. Yahoo was about to be bought by (Refer Time: 06:16) and the it was a multi supposed to be the multibillion dollar deal, then after this hack it is come to millions, right. Nobody believes that yahoo can be as safe as anything else right. So, it is because of a information security. So, what is yahoo done. Have you used have you have you do you use yahoo mail.

Student: I used to use.

Do you use it on mobile as well as on the web site? On the (Refer Time: 06:39) do you use? Who uses mobile yahoo news and web app?

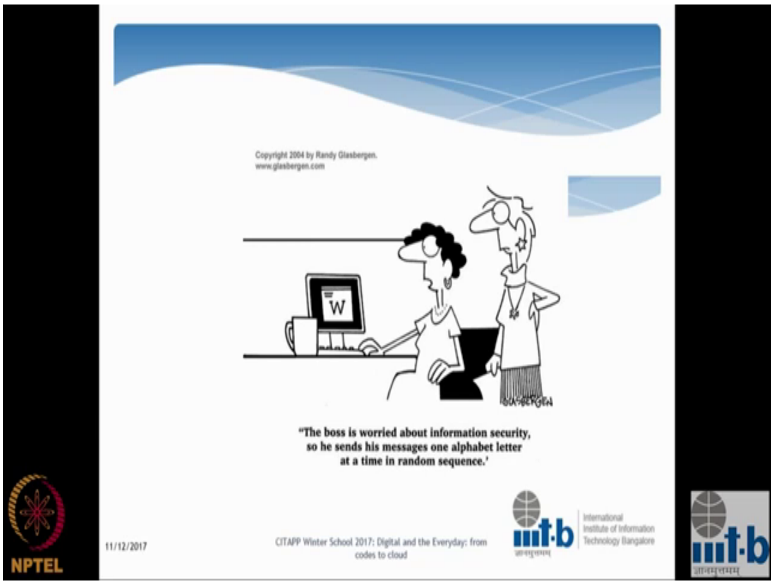
Student: 2 factor authentication.

2 factor authentication, what is the 2-factor authentication sir?

Student: So, when I just login normal web browser, transferred we to verify on the mobile.

So, they think that they have cut you make it more secure, right. If you do it from web app. They will ask you, you have to authenticate from your mobile app. So, in mobile app you will get an information saying that, I approve this person use to use it from the web app right. So, they have provided this 2-factor authentication mechanism, right. Now it is 100 percent sure whether this 2-factor authentication is 100 full proof. But they have taken some measure. So, technology can assist in improving the information in security.

(Refer Slide Time: 07:29)



Copyright 2004 by Randy Glasbergen.
www.glasbergen.com

"The boss is worried about information security, so he sends his messages one alphabet letter at a time in random sequence.'

11/12/2017

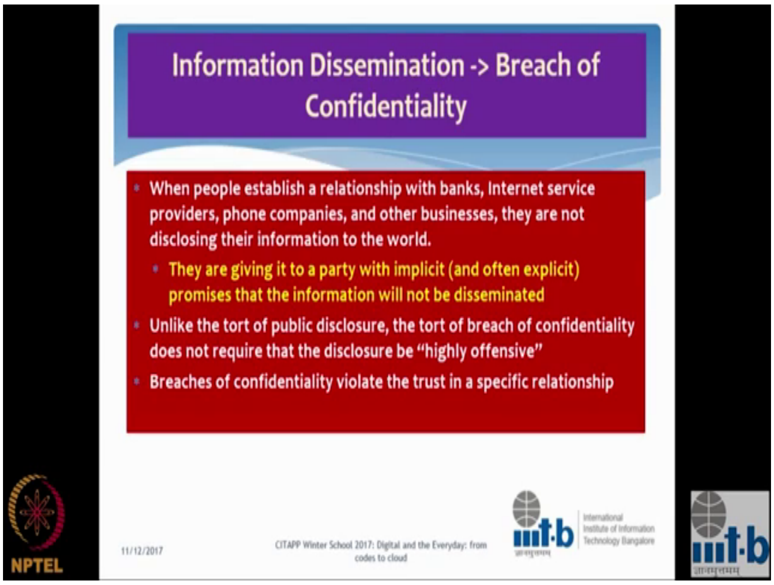
CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

But the problem is this. So, once we become very, very conscious of security, what will you do? We talk in random numbers, which nobody else can understand.

Student: Yes.

And most of the times this what happens. So, we remember all passwords, right. We remember all the password, because we have we have to have different passwords in order to protect our information, right. So, we remember all these passwords write it down and all, but finally, we forget our name. So, it is quite possible that this can kind of thing can happen right. So, in security is the problem right, but to some extent it can be counter way by for example, technology.

(Refer Slide Time: 08:14)



Information Dissemination -> Breach of Confidentiality

- When people establish a relationship with banks, Internet service providers, phone companies, and other businesses, they are not disclosing their information to the world.
  - They are giving it to a party with implicit (and often explicit) promises that the information will not be disseminated
- Unlike the tort of public disclosure, the tort of breach of confidentiality does not require that the disclosure be "highly offensive"
- Breaches of confidentiality violate the trust in a specific relationship

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

Breach of confidentially. What is this? We trust each other, when I give information to the doctor, right. This we a discuss a little bit about it in the health domain as well. So, we disclose lot of things to the doctor, right. Because we have trust in the doctor, that the doctor will not take it to somewhere else, or you know sell it to someone else, that information that yes collected health information is very private right. So, we disclose it to trusted parties. So, the same thing holds good with for example, if I buy something on amazon, right. I trust that amazon will use it for you know.

Student: General.

Beautiful you know, I mean they will not use it they will not a misuse it, right. I have trust in certain websites, organizations, individuals. But if for example, that information that they have collected is used for some other purposes. Or it is divulged posted outside. Then it leads to breach of confidentiality right. So, the trust that I had in video while confiding my information is lost, right. Is this violation of privacy?

Student: Yes.

So, there is a private information which I have confided to a trusted third party, right. And the trusted third party has violated this confidentially agreement. There is a breach of confidentiality, right. So, is this how serious it is compared to for example, secondary use.

Student: Same.

Secondary use is also the same thing, right. I confined it, and then it is used for some other purposes right. So, here I have confined and it is being made public, whatever private information that I had given is being made public yeah, yeah.

Student: also difference in which is being made public like for example, let us say (Refer Time: 10:10)

Good point, yeah.

Student: those were again breach of those were again breach of privacy, but which is most (Refer Time: 10:18) the breach of privacy there or the acts committed by these people.

Good point, that is the most important thing.

Student: But sir.

See any of these privacies have a positive side as well as a negative side. Suppose for example, wiki leaks case, right. That is also violation of privacy, violation of privacy of the state, right? The state was snooped, and it was leaked, right. And this guy who was there with I think FBI or.

Student: Snowden.

Snowden, yeah snowden he was he was working for the government. So, there was trust on him not to confide the data; which is there in the government data base, but he leak it, right. So, is this violation of privacy against his state.

Student: Yes.

Yes, but does it have like what he exactly said seems to have positive consequences, right. So, yeah.

Student: any search operation for that matter, right. By any intelligence agency (Refer Time: 11:09) all we must have PCIA. So, there are violations of privacy at one point. But they also I mean they claim to deliver the bigger picture claiming that we. So, the (Refer Time: 11:21) privacy is a crime, but we are exposing the crime committed by these people or I who I mean.

Correct, correct, correct so.

Student: So, it depends on what it is useful and then, (Refer Time:11:32) the information

So, how will I ascribe you know for example, a value you know I mean to action against.

Student: any example.

How will you how will we do that? Is it possible?

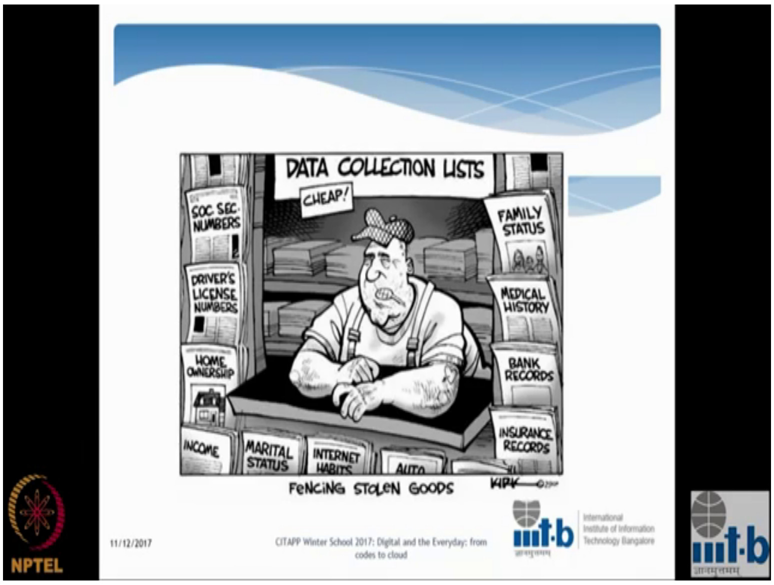
Student: (Refer Time: 11:49) 7.9.

That is the whole exercise right. So, our for example, if the dissemination of information without the government consent is a violation according to some law, then that is the reason why snowden is being wanted by the us government, right. Because he violated this particular confidentiality, right. He has written agreement he confided. I mean, he said that he will do according to the government you know disclosure agreements. Then, but he didn't follow it, right

Student: Sir, that is what criminals is also technically.

Correct, correct. So, that is what I am saying. So, blanket saying that privacy is bad is not a correct. So, like exactly what you said the intrusion of privacy might have some positive consequences. And depending upon that we need to. So, we will discuss a little about you know how to do this (Refer Time: 12:39) how will the state do it, right. How will the regulator do it will discuss a little bit about that right?

(Refer Slide Time: 12:52)

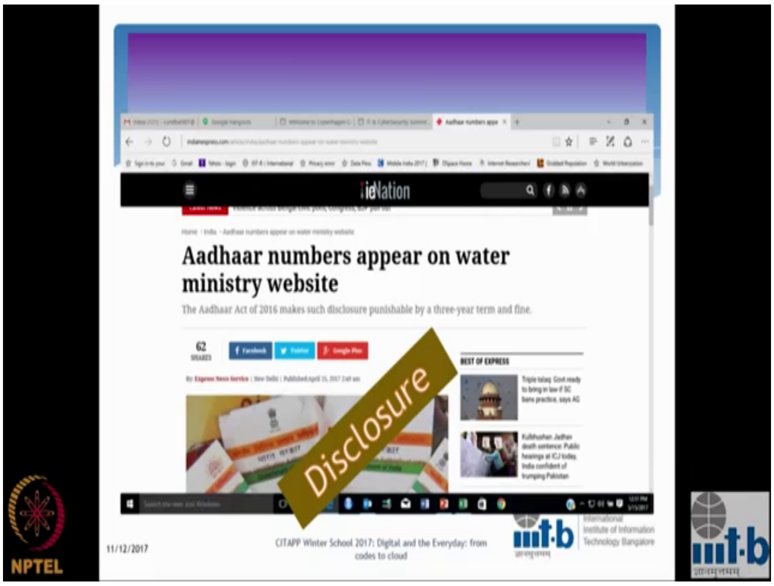


11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

So, for example this is a classic case right. So, the information that you give to insurance agencies or doctors, they can be put for public use. And it can be sold breach of confidentiality. It can happen and this is the violation of privacy.

(Refer Slide Time: 13:12)



Home › India › Aadhaar numbers appear on water ministry website

Aadhaar numbers appear on water ministry website

The Aadhaar Act of 2016 makes such disclosure punishable by a three-year term and fine.

62 SHARES

By: Express News Service | New Delhi | Published:April 25, 2017 2:49 am

BEST OF EXPRESS

Triple talaq: Govt ready to bring in law if SC bans practice, says AG

Kulbhushan Jadhav death sentence: Public hearings at ICJ today, India confident of trumping Pakistan

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

Excellent cases Aadhaar leakage; which is been happening day in and day out, right.

So, you give Aadhaar number for you know direct benefit transfer, and it gets leaked through government websites, right. So, you basically assume that the government is going to protect the confidentiality of the Aadhaar identification information that you have given. But unfortunately, it gets posted, right. May be due to information insecurity, but there is a breach of confidentiality between me and the government in this particular case right.

So, along with Aadhaar number my other details are posted and therefore, there is a confidential agreement is completely broken, right. So, these kind of things do happen, right. And we have to be watchful at that. So, on a scale of 1 to 10 again, if you take breach of confidentiality how would you rate it? How would you rate it?

Student: I think this is very serious.

Very serious.

Student: 8.

Worst then secondary use.

Student: No, not worse than secondary

Not worse then secondary use?

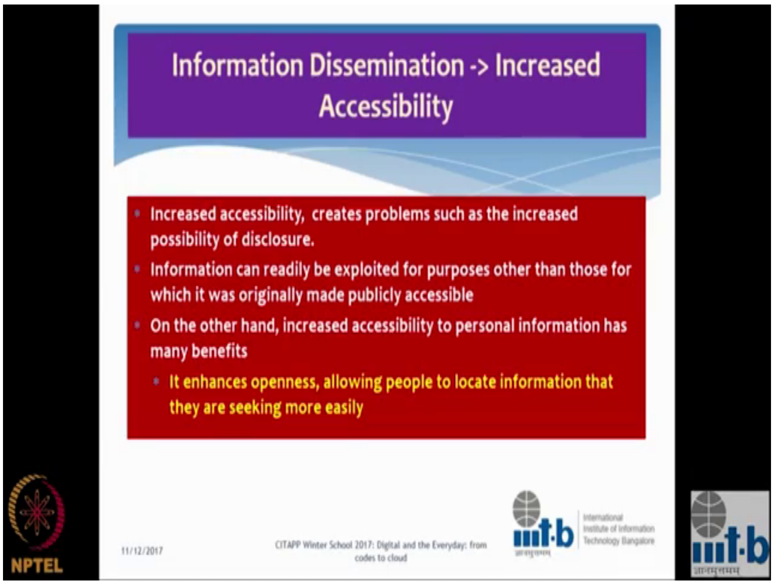
Student: because anyway government was providing if I am not wrong, then they were providing some facilities and move a (Refer Time: 14:14) beneficiary data then within the Aadhaar number means. So, that the so that the beneficiary can check whether I am in to that list or not that was the.

That was the purpose, that was purpose the intended purpose was that everybody can go and check whether your name is there or not.

Student: Yeah

But unfortunately, they get you know about other details of other Aadhaar holders, right. And public at large can also do that. So, this is you know another dimension of security.

(Refer Slide Time: 14:45)



Information Dissemination -> Increased Accessibility

- Increased accessibility, creates problems such as the increased possibility of disclosure.
- Information can readily be exploited for purposes other than those for which it was originally made publicly accessible
- On the other hand, increased accessibility to personal information has many benefits
  - It enhances openness, allowing people to locate information that they are seeking more easily

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

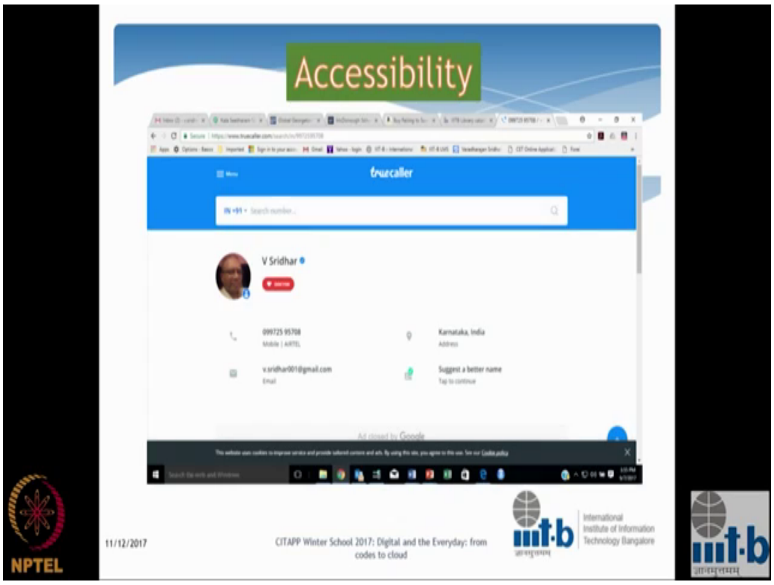
Increased accessibility, see the reason why for example, the privacy has become very important today is that the information is in digital form. And therefore, it is say accessible right. So, previously we used to write our address and all those things, and we side to you know will full submit to you know any government.

So, any government form if you take. It will contain all the information that you can provide, right. Including your mobile number address blood group things like that. What is the purpose of collecting this information nobody knows. But the form will contain ditto all the information that they can provide right.

Student: Yes sir

But at that time, it was in paper and pencil, and it is quite possible that it may not be used very effectively, but today it is all in the digital form. And that is one of the reasons why it is for example, increasingly becomes accessible, right. And increased accessibility is very evident using this true caller.

(Refer Slide Time: 15:41)



Accessibility

truecaller

V Sridhar

099725 95708
Mobile | AIRTEL

Karnataka, India
Address

v.sridhar001@gmail.com
Email

Suggest a better name
Tap to continue

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

Student: Yes

Help. So, true caller uses reverse look up. So, previously if you have, if you know the name, right. You can find out the mobile number.

Student: Yeah

But if you know the mobile number, can you find out the name.

Student: Yes

Yeah in previous times it is not possible. Because the yellow directory or the white telephone directory, which BSNL used to publish and all know.

Student: Yes.

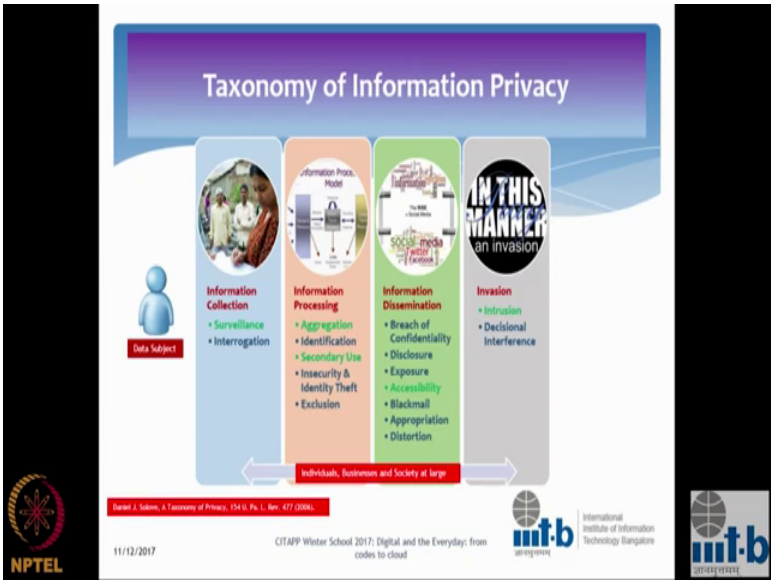
You get the alphabetical order of the name. Then you can find out the number, but reverse look up is very difficult, right. Today true caller does that, right. And not only gives information about me my photograph also it gives, right without anybody consent. So, you can get to know about your friends your their photograph everything, why? Because the reverse lookup has become so easy, right.

Accessibility of information (Refer Time: 16:30) digital form. So, given for example, your mobile umber using the algorithms that process shisha talked about, you can quickly search and come up with this particular name and number right. So, very funny, very funny sometimes it can be really funny.

There is a director called Jewel Singh in IBM. Her name is Jewel Singh I got a true caller when she called, right. There I didn't have that number. So, I use true caller to look it up and says that this is jewelry person and all. He is actually see is working at IBM as a consultant. But algorithms can do all these tricks, right. Jewel must be a jewelry shop right.

So, accessibility so, information can readily be exploited for purposes other than those that are intended, for and that is because it is in digital form right. So, that is one of the important things about digitization of information, becomes easily accessible. It is possible using algorithms to actually manipulate that information, right. And then create some cohesive whole.

(Refer Slide Time: 17:46)



Taxonomy of Information Privacy

Data Subject

Information Collection
- Surveillance
- Interrogation

Information Processing
- Aggregation
- Identification
- Secondary Use
- Insecurity & Identity Theft
- Exclusion

Information Dissemination
- Breach of Confidentiality
- Disclosure
- Exposure
- Accessibility
- Blackmail
- Appropriation
- Distortion

Invasion
- Intrusion
- Decisional Interference

Individuals, Businesses and Society at large

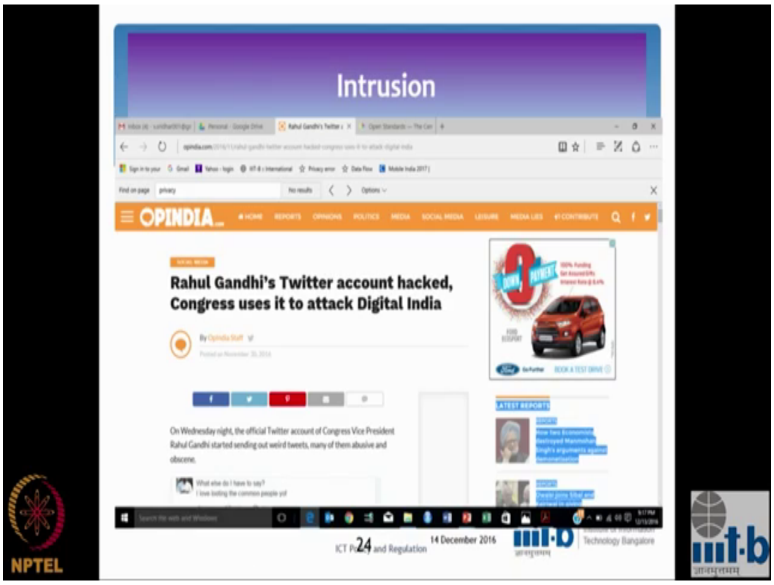
Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

So, this is very important to identify on a particular violation where it fits in, right. Once you are able to sort of narrow it down to your particular aspect of violation, then it is possible for you to identify the cost and benefits of violation, then attribute was in a scale of 1 to 10. And then take punishment, right. And this have to in acted through laws and regulations right. So, we will discuss a little bit about that. Intrusion this happened you know Rahul Gandhi's twitter account was hack.

(Refer Slide Time: 18:20)



Intrusion

Rahul Gandhi's Twitter account hacked, Congress uses it to attack Digital India

On Wednesday night, the official Twitter account of Congress Vice President Rahul Gandhi started sending out weird tweets, many of them abusive and obscene.

And congress uses it; is this violation of privacy?

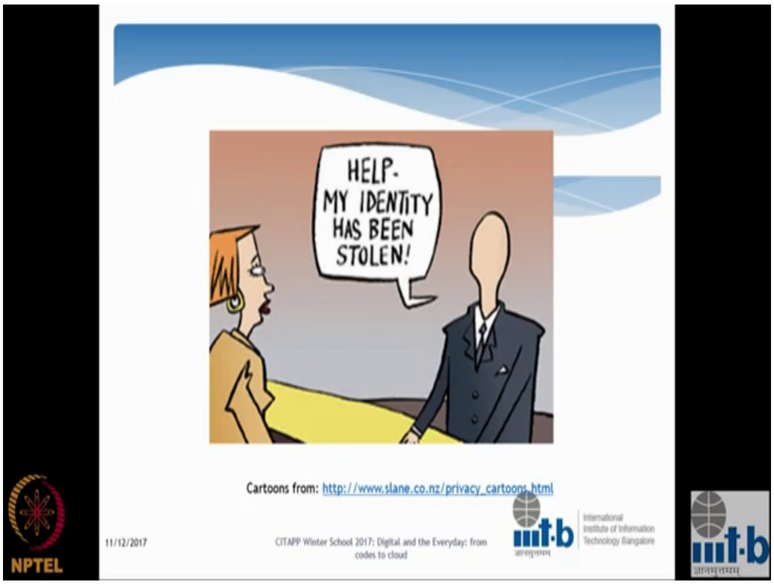
Student: Yes.

Intrusion, right?

Student: Yes

In intrusion into someone's domain; so, there are various dimensions. So, how firms and government should handle this? So, we have discussed some major aspects of the information privacy violations. Who should handle it? Individuals like you and firm's organizations, or government should do it, and how do they do it, right. These is an excellent example.

(Refer Slide Time: 18:57)



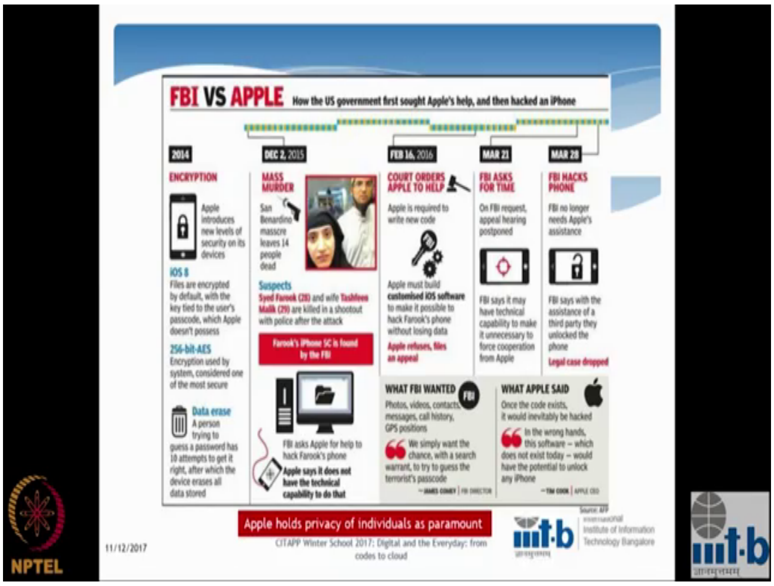
Cartoons from: http://www.slane.co.nz/privacy_cartoons.html

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

Identity is stolen; so, you go to UIDII, and make a complaint. And my biometric information is stolen; what can UIDII can say, right. They have to some provisions in order to restore my identity; so, classic case.

(Refer Slide Time: 19:17)



FBI VS APPLE How the US government first sought Apple's help, and then hacked an iPhone

2014 ENCRYPTION

Apple introduces new levels of security on its devices

iOS 8
Files are encrypted by default, with the key tied to the user's passcode, which Apple doesn't possess

256-bit-AES
Encryption used by system, considered one of the most secure

Data erase
A person trying to guess a password has 10 attempts to get it right, after which the device erases all data stored

DEC 2, 2015 MASS MURDER

San Benardino masscre leaves 14 people dead

Suspects
Syed Farook (28) and wife Tashfeen Malik (29) are killed in a shootout with police after the attack

Farook's iPhone 5C is found by the FBI

FBI asks Apple for help to hack Farook's phone

Apple says it does not have the technical capability to do that

FEB 16, 2016 COURT ORDERS APPLE TO HELP

Apple is required to write new code

Apple must build customised iOS software to make it possible to hack Farook's phone without losing data

Apple refuses, files an appeal

MAR 21 FBI ASKS FOR TIME

On FBI request, appeal hearing postponed

FBI says it may have technical capability to make it unnecessary to force cooperation from Apple

MAR 28 FBI HACKS PHONE

FBI no longer needs Apple's assistance

FBI says with the assistance of a third party they unlocked the phone

Legal case dropped

WHAT FBI WANTED

Photos, videos, contacts, messages, call history, GPS positions

“We simply want the chance, with a search warrant, to try to guess the terrorist's passcode

—JAMES COMEY | FBI DIRECTOR

WHAT APPLE SAID

Once the code exists, it would inevitably be hacked

“In the wrong hands, this software – which does not exist today – would have the potential to unlock any iPhone

—TIM COOK | APPLE CEO

Source: AFP

Apple holds privacy of individuals as paramount

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

How firms handle. This is the apple case probably you know (Refer Time: 19:21) that. So, the san I always cannot pronounce this properly it is a north of.

Student: (Refer Time: 19:26) San Bernardino.

Bernardino, San Bernardino right; so, there was crime which was committed. And the criminals had apple iPhone, alright.

Student: (Refer Time: 19:40)

So, they were shot after the particular incident, but; however, the government the FBI wanted to interrogate. Basically they wanted to find out what information was stored in there apple iPhone. Actually, apply iPhone was connected to apple iCloud. So, all the information had moved to I cloud. But you needed authentication in order to get access to this particular data which was held on the phone of the criminals; criminals were dead, right.

And therefore, they thought that if they get that particular information which was stored in the iCloud on that particular identity, then they will be able to figure out some more connections and networks. And you know probably able to prevent such crimes in the future and so on.

So FBI due diligently asked Steve Cook, apple CEO to divulge the access code for the iPhone as well as the iCloud. Immediate response from the CEO was that we protect privacy of individuals.

Student: (Refer Time: 20:41)

Right and therefore, we cannot give you the code. Sorry, that is the procession that apple has taken, despite the fact that one the criminals or no more, right; the second it is in the national interest. So, Steve Cook made a decision like this despite these 2 compelling reasons, that it will not give access to the code right. So, FBI went on it is own, hired third party crackers, managed to crack that and they managed get this information. But they were not able to force apple to divulge the code, right. And this is position an organization has taken, right. Like apple has taken in order to protect the privacy of the individuals.

So, can is it good? Morally correct? According to CEO Steve Cook, I am mean it is correct because it protected the individuals of their uses, right. They confided in me that I would protect their information and therefore, I cannot breach that confidentiality. So, whatever it means I am going to protect the privacy of the individuals; the confidential information, right. The breach of confidentiality is not lost here, right. Is it a correct decision, right?

Student: May not be.

Is it a decision?

Student: It may not be positive or that may be same people who have that when product comes. So, some other if there are (Refer Time: 22:14) been like suppose my data is being producted by apple.

Correct.

Student: I.

The important thing correct is yeah, yeah.

Student: So, I I agree we have (Refer Time: 22:21) not share data, but there are people who have attacked by these people query come and attack them because.

Exactly that is the argument Steve Cook gave, right. Suppose if you divulge you the code, right. Now it is quite possible that it can be leaked or whatever it is. And that same code cracking mechanism can be used by someone else to crack all the other users. That is what you are saying you know.

Student: Yes.

Or is that.

Student: Different.

Different?

Student: Yeah.

So.

Student: Sir.

This is one possibility right. So, I give you a code cracking methodology, right. And somebody else can use this code cracking methodology to actually hack into my phone and my iCloud right. So, you are making all the other users information insecure by divulging this.

Student: But why?

Right?

Student: Apple has to give with code cracking mechanisms, like you can just leave the code (Refer Time: 23:09) code always remember.

Possible then we can find out you know that what is the mechanism by which the code was generated algorithms. It is too is given by algorithm. So, you can actually find out an algorithm which generated this particular code.

Student: If party is not giving third parties can use algorithms to crack it.

Correct, correct.

Student: Yeah that is the.

So, either the algorithm either you know the algorithm, or you know the pass code, if you know the pass code, you can do reverse engineer, and actually create the algorithm, am I correct or not?

Student: No.

So, it is possible. Once you create this generic algorithm, then give me Apple phone number or IMEI number. I will be able to give you the code, which possible. Technology wise it is possible as procession is as told, right. So, by divulging I am actually risking my all the other uses and therefore, I will not do it that is the logic which Steve cook gave (Refer Time: 23:54)

Student: Sir

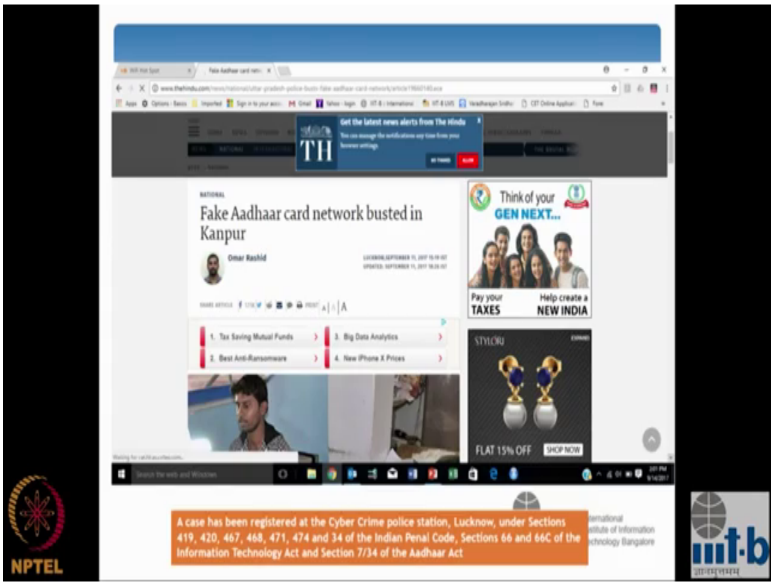
What did you say?

Student: When I was saying that the Steve cooks Steve cook’s decision is not a (Refer Time: 24:00) is may be like people who attack them people who have like, they will also have attack their users. Whose information if is information, if it had been given up to that is save another crimes.

Possible, possible that is that is why FBI wanted it, right. T there is a reason why FBI wanted it; but the position taken by the firm is very different, right. The procession irrespective of the national interest, right; I want to protect my users, privacy. That is the procedure that you know the origination has taken it, right. That is good or bad it is an national interest or not whether it is totally beneficial or loss I mean that is, but it is a policy of apply right.

So, this is one of the ways by which the companies attack the privacy problems, right. If you have confidential information, then it is possible that companies can take this position.

(Refer Slide Time: 24:52)



Get the latest news alerts from The Hindu

NATIONAL

Fake Aadhaar card network busted in Kanpur

Omar Rashid

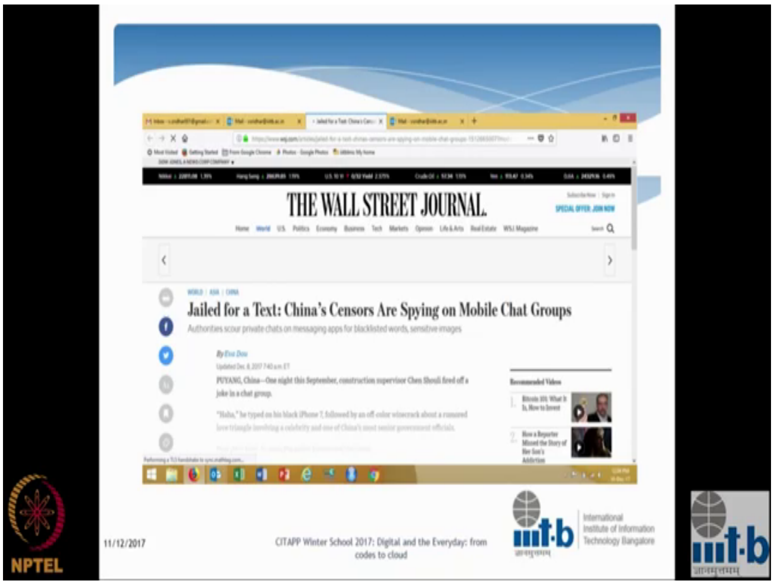
1. Tax Saving Mutual Funds
2. Best Anti-Ransomware
3. Big Data Analytics
4. New iPhone X Prices

A case has been registered at the Cyber Crime police station, Lucknow, under Sections 419, 420, 467, 468, 471, 474 and 34 of the Indian Penal Code, Sections 66 and 66C of the Information Technology Act and Section 7/34 of the Aadhaar Act

TH
Think of your GEN NEXT...
Pay your TAXES
Help create a NEW INDIA
STYLORI
FLAT 15% OFF
SHOP NOW
NPTEL
International Institute of Information Technology Bangalore
iiit-b

Lot of Aadhaar cards where generated, fake Aadhaar cards. They faked the ID’s they faked. Biometric you know thumb prints and things like that, and Kanpur and government busted it, right. I mean one possibility is that the government can take a very active role in cybercrime, and then actually it protects privacy the individuals whenever this kind of events happen right, but we need to have capability to do that, right. We need to build the capabilities in order to do this forensics.

(Refer Slide Time: 25:27)



THE WALL STREET JOURNAL.

WORLD | ASIA | CHINA

Jailed for a Text: China's Censors Are Spying on Mobile Chat Groups

Authorities scour private chats on messaging apps for blacklisted words, sensitive images

By Eva Dou

Updated Dec. 8, 2017 7:40 a.m. ET

PUYANG, China—One night this September, construction supervisor Chen Shouli fired off a joke in a chat group.

"Haha," he typed on his black iPhone 7, followed by an off-color wisecrack about a rumored love triangle involving a celebrity and one of China's most senior government officials.

Recommended Videos

1. Bitcoin 101: What It Is, How to Invest

2. How a Reporter Missed the Story of Her Son's Addiction

11/12/2017

CITAPP Winter School 2017: Digital and the Everyday: from codes to cloud

This is just yesterdays released. So, government can be surveilling, right. And it can be used for both positive as well as for negative consequences. So, somebody posted a text which says that you know something about a Chinese you know marrying or something like that of a western you know girlfriend or someone, and he was jailed. Because this was detected from the text speeches that where going out in WeChat. So, government can take these kind of measures right.

So, government can say that it owns all the data and therefore, it can take whatever for example, in the case of Aadhaar; that is why Aadhaar has become such a very big issue. Because government controls that biometric information database that is using; it is very sensitive, right. And what if government starts making use of it in ways other than what it is intended for right. So, we need to be a little bit careful about that, we will come and have a look it.