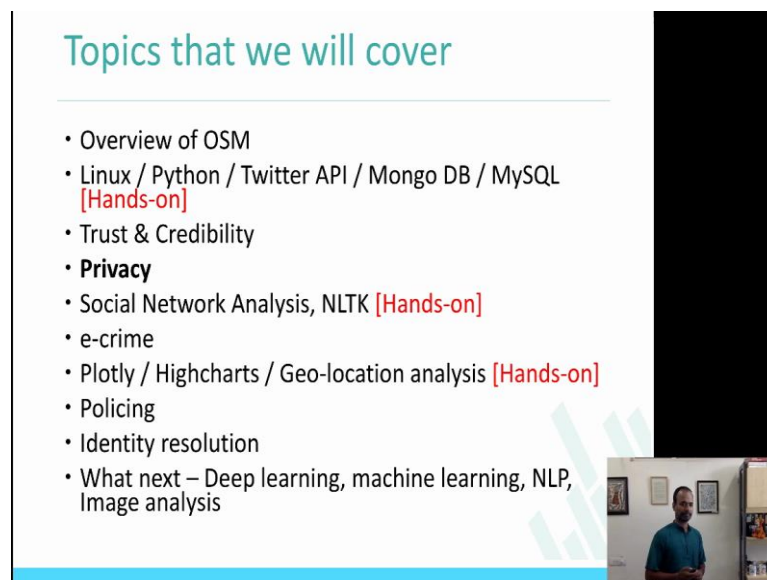


**Privacy and Security in Online Social Networks**  
**Prof. Ponnuram Kumaraguru (“PK”)**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Week – 4.1**  
**Lecture – 15**  
**Privacy and Picture on Online Social Media**

Welcome back to the course. I hope you are enjoying the course in terms of studying some new concepts, new ideas, and new solutions. This is the week 4 of the course Privacy and Security in Online Social Media, what I will do now is **continue** the topic on privacy that we were talking last time.

(Refer Slide Time: 00:32)

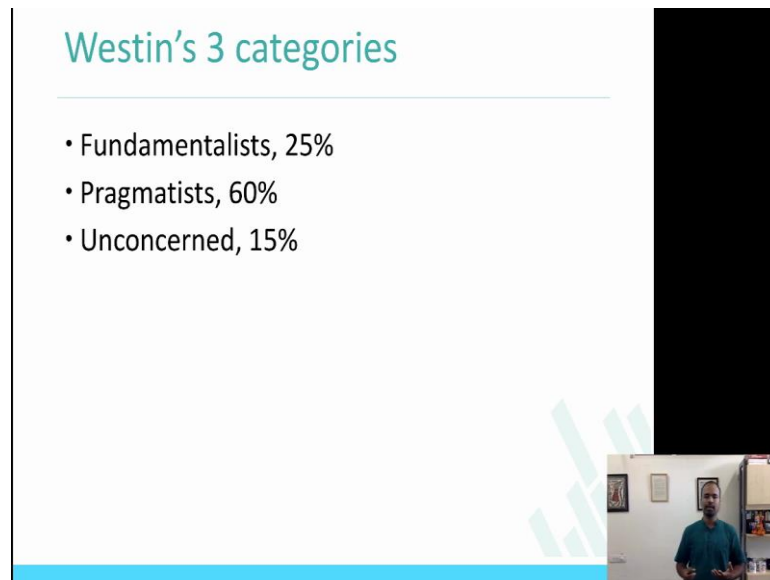


**Topics that we will cover**

- Overview of OSM
- Linux / Python / Twitter API / Mongo DB / MySQL [Hands-on]
- Trust & Credibility
- **Privacy**
- Social Network Analysis, NLTK [Hands-on]
- e-crime
- Plotly / Highcharts / Geo-location analysis [Hands-on]
- Policing
- Identity resolution
- What next – Deep learning, machine learning, NLP, Image analysis

Now, just **let to let you** know we are in the topic of privacy for now, we just covered the trust and credibility, and I assume by now you are all very well versed with little bit of Linux little bit of a Python, how to collect data from twitter, how to store the data, what kind of MySQL queries you should write and collecting data and all that.

(Refer Slide Time: 00:54)

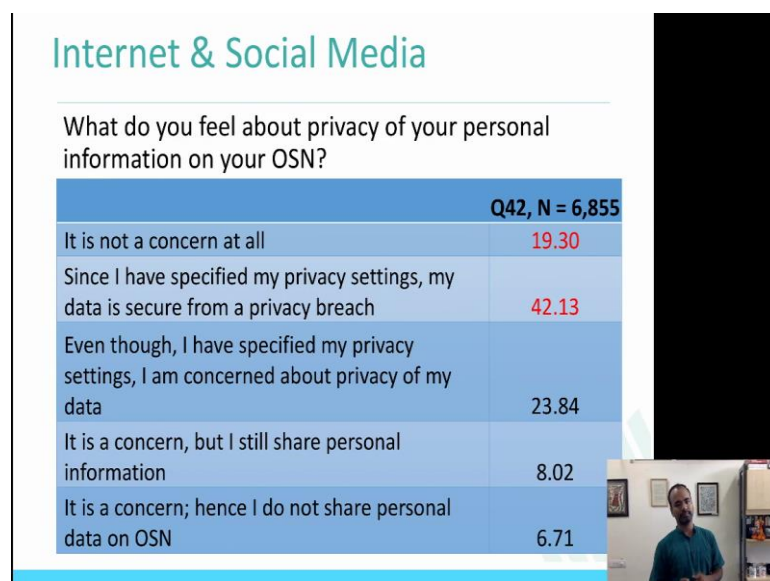


### Westin's 3 categories

- Fundamentalists, 25%
- Pragmatists, 60%
- Unconcerned, 15%

In the last week we saw about how Westin categorized **all** the US citizens into 3 categories; Fundamentalist, Pragmatists and Unconcerned. Fundamentalist is being 25 percent, pragmatists is being 60 percent and unconcerned being 15 percent. Fundamentalist are the people who actually do not give away any personal information. Pragmatists make decision about privacy keeping the situation in mind. Unconcerned are the set of people who gave away personal information and be part of **revealing** personal information is about 15 percent in the US.

(Refer Slide Time: 01:27)



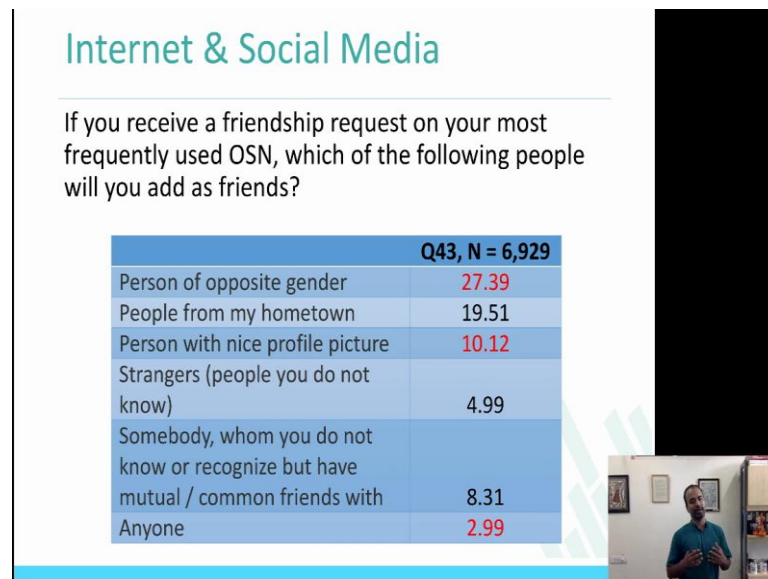
### Internet & Social Media

What do you feel about privacy of your personal information on your OSN?

	Q42, N = 6,855
It is not a concern at all	19.30
Since I have specified my privacy settings, my data is secure from a privacy breach	42.13
Even though, I have specified my privacy settings, I am concerned about privacy of my data	23.84
It is a concern, but I still share personal information	8.02
It is a concern; hence I do not share personal data on OSN	6.71

I kind of asked you couple of questions last time about some data that was collected among large set of population in India. So this is one of the questions that I asked which is what you feel about privacy of your personal information on your online social network, which is about Facebook. About 42 percent, the highest was about 42 percent **who** said that specified my privacy settings my data is secured from a privacy breach.

(Refer Slide Time: 02:00)



Another question that I asked you also is about if you receive a friendship request on your most frequently used online social network, which is Facebook in this case which of the following people will you add as friends. And the highest was actually person of opposite gender. I am pretty sure in the last couple of weeks going through the class that you are taking on the social network now, even **your own behavior may be** changing, **you may be** looking at some of **these requests** more closely, you may be devising **your** mechanism by which any friend request that you get, how you are going to accept it or how you are going to deny it.

(Refer Slide Time: 02:35)




<http://precog.iitd.edu.in/research/privacyindia/>

The slide features a white background with a teal URL. A small video inset in the bottom right corner shows a man in a teal shirt speaking. A black vertical bar is on the right side of the slide.

Now, the data is publicly available please feel free to actually play around with the data.

(Refer Slide Time: 02:40)



**Hard to define**

“Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”

Robert C. Post, *Three Concepts of Privacy*,  
89 Geo. L.J. 2087 (2001).

The slide has a white background with a teal title and quote. A small video inset in the bottom right corner shows the same man in a teal shirt speaking. A black vertical bar is on the right side of the slide.

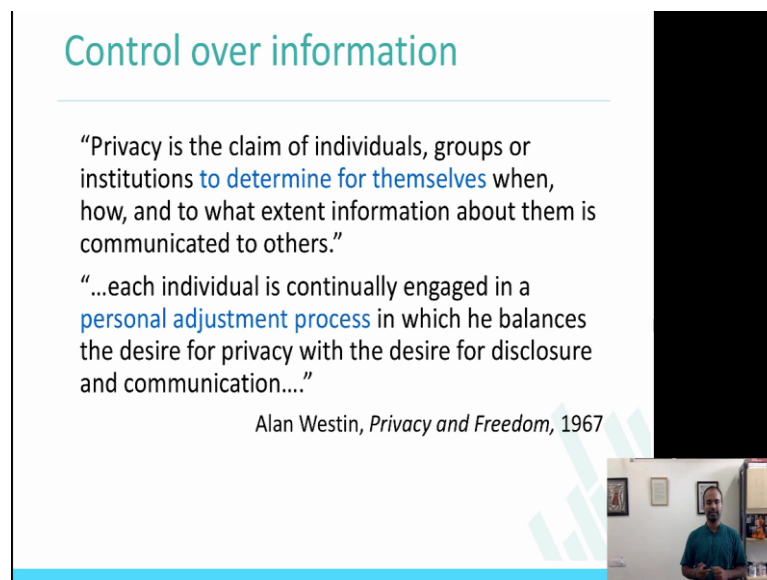
Last time I left you with the question saying; what are the kind of privacy issues that you have on Facebook, Twitter? How you define privacy? I think it is nice to see some of you posting information about various Facebook privacy issues or your own questions about Facebook privacy issues on the forum. We should actually make the forum more active because I think there are some very repeated questions **that** comes up, **we're trying** to answer as such as possible but when they are very repeated we can avoid actually

answering also. I strongly recommend you to ask, check the forum before posting the questions.

So, let us look at what privacy is a little bit and then give a little detail about some research that was goes down in terms of analyzing the privacy status on Facebook. One of the definitions that was given earlier about privacy was that “Privacy is a value so complex, so entangle in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.” So that was Robert talking about privacy in his book ‘Three Concepts of Privacy.’

But I think the privacy by definitions is actually thought. I mean, if you were to look at what privacy is for you, why are you sitting and listening to this lecture, versus privacy in your school, privacy at home, privacy at work is very different. It is very hard to define what privacy is for a particular individual across various situations, that is what this definition is actually trying to capture. Contradictory dimensions, so entangled and competing and contradictory dimensions.

(Refer Slide Time: 04:31)



**Control over information**

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

“...each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication...”

Alan Westin, *Privacy and Freedom*, 1967

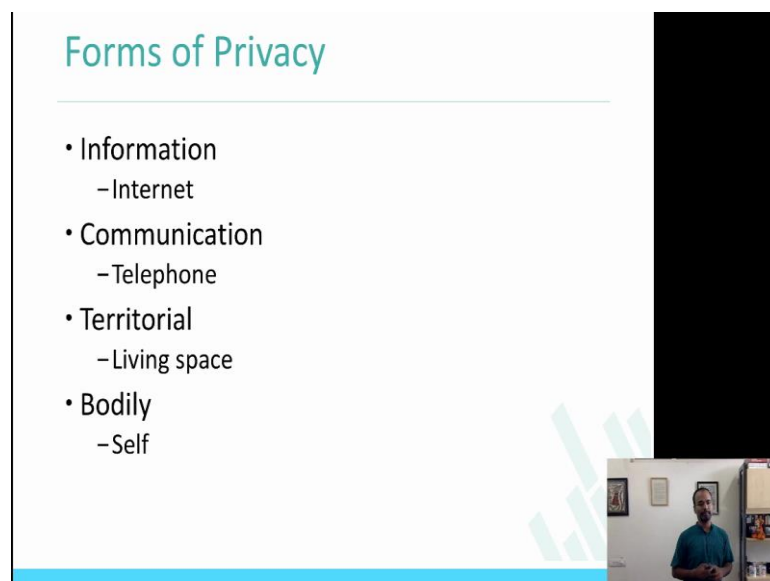
Fundamentally privacy is been always talked about control over information, here are two definitions of Alan Westin actually tried defining in his book in a ‘Privacy and Freedom’ in 1967. “Privacy is the claim of individuals, groups or institutions to

determine themselves when, how and what extent information about them is communicated to others.”

So it is basically about to determine for themselves, how much of my information I can actually share with others. “Each individual is continually engaged in personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication.” How much do I want to **reveal** about myself, how much do I want to actually anonymize information about myself, how much do I want to reveal about myself, is the way that the **word** privacy is defined and is the way by which you are controlling the information that you are actually spreading.

So, I am **sure** you kind of get the definition privacy which is very hard to define and also it is very difficult to actually come up with the list of privacy expectations for any individual in all given contexts. They strictly convey privacy is about control over information. It sometimes could be **actually** a group information also, given that idea is more or collective society we generally talk about a privacy of a group, instead of individual privacy, that the society is where its individualistic society where the privacy information of the individuals are more protected than the privacy information of the group.

(Refer Slide Time: 06:11)



**Forms of Privacy**

- Information
  - Internet
- Communication
  - Telephone
- Territorial
  - Living space
- Bodily
  - Self

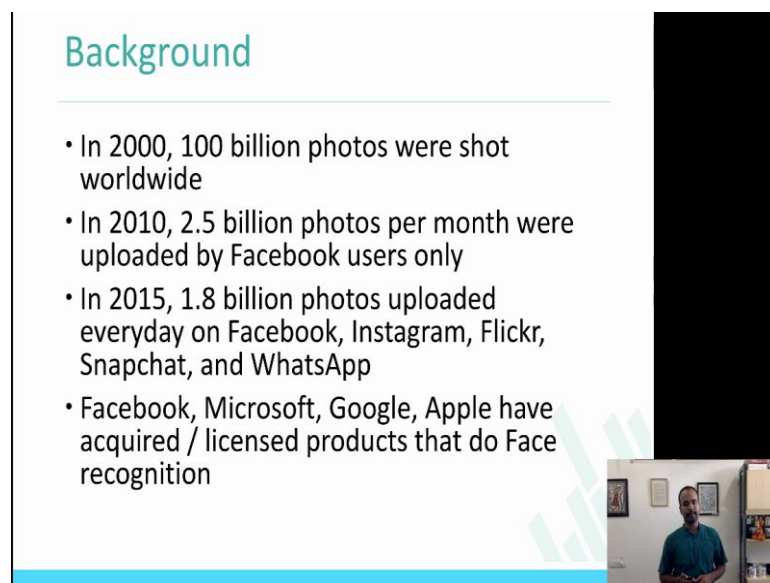
The slide features a light blue header and footer. A small video inset in the bottom right corner shows a man in a blue shirt standing in a room with a white wall and a bookshelf.

Some forms of privacy that people have come up with; information privacy, communication privacy, territorial privacy and bodily privacy. Majority of the times

when we talk about privacy particularly in courses like these it is always referred to as information privacy and particularly the internet privacy.

There is also communication privacy which is telephones and other forms of communication. Territorial privacy is about my living space, my home, my city, my country and, the topics around that. Bodily privacy is about self. So, information about my own physical presence is actually also discussed in the concept of privacy. For example, a CCTV camera is one example where bodily privacy can be actually attacked.

(Refer Slide Time: 07:04)



**Background**

- In 2000, 100 billion photos were shot worldwide
- In 2010, 2.5 billion photos per month were uploaded by Facebook users only
- In 2015, 1.8 billion photos uploaded everyday on Facebook, Instagram, Flickr, Snapchat, and WhatsApp
- Facebook, Microsoft, Google, Apple have acquired / licensed products that do Face recognition

Now let us look at some specific studies that are being done in terms of analyzing the privacy in online social networks. Here is the study that I will walk you through the reference to the study is at the end of the day of the slides, but we walk you through what they did, what they find, how revealing the information are, how good the study was and how the privacy is being actually studied in the context of Facebook and social networks and publicly available information.

Some background about pictures that were uploaded on social networks itself. In the year 2000, 100 billion photos were shot worldwide. In 2010, 2.5 billion photos per month were uploaded by Facebook users only. Whereas, if you remember the first lecture 1 where I actually showed you a infographic about what among the information is uploaded on social networks in 1 minute, we actually saw that 1.8 billion photos were

uploaded everyday on Facebook, Instagram, Flickr Snapchat, and Whatsapp together. So **there** is a lot of information, lot of pictures that are actually uploaded on social networks.

Companies like Facebook, Microsoft, Google, Apple have actually acquired a lot of face recognition companies in the last few years, to study, to understand, to use these technologies to identify faces on pictures that are **being** uploaded on the all social networks or online services. It has become very, very important to apply these kind techniques like, machine learning, deep learning and concepts around that into these images to study what is happening on online social networks, I actually recently **wrote** also a blog about the importance of images on online social networks. I'll actually shared it on the forum just after this lecture.

(Refer Slide Time: 09:07).



**Many things are colluding**

- Increasing public self-disclosures through online social networks
  - Photos
- Improving accuracy in Face recognition
- Cloud, ubiquitous computing
- Re-identification techniques are getting better

If you really look at what is going on currently in terms of these pictures that were uploaded and the privacy about individuals, increasing public self disclosures through online social networks happen, which is I take a pictures, I take a selfie standing near one of the very important spots let us take in Delhi I upload this picture you know that I am in Delhi, or let us take a picture next to Taj Mahal and upload it on my Facebook account you know that I am actually traveling to Taj Mahal now.

**There used** to be actually a **site called please rob me dot com** I do not think so the website is active now. This website what did they did was its called please **rob me** dot com, what we interestingly did was let us take it if I have a twitter account and I created



it from Delhi and posting about **weather** in Chennai or Hyderabad or California they would actually pick this tweet and post it on **please rob me dot com** saying that this account was originally created from Delhi and whereas now this post is actually talking about **weather** in California, so probably you are not at home and therefore your homes should be locked.

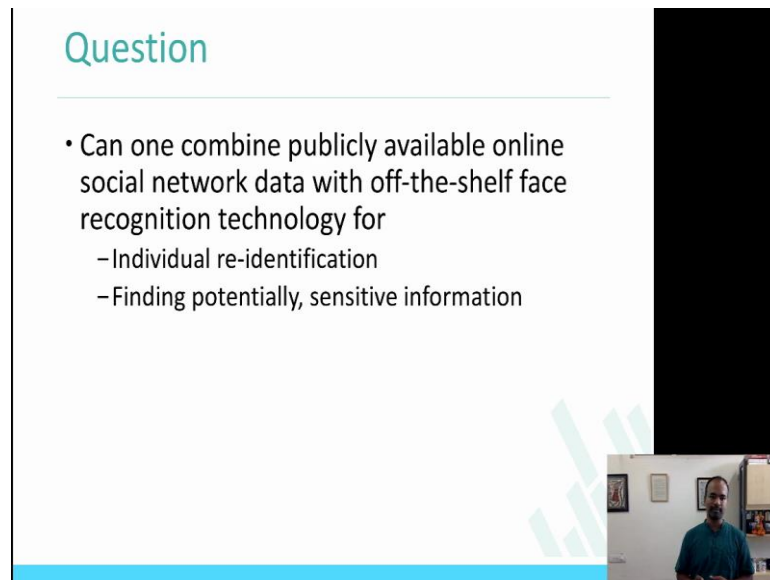
It got **flacked** a lot, but I think it is an interesting idea that they actually picked up to make use of the information that the users of social network are disclosing by themselves about their location. As a self-disclosure through online social networks and there are many many **issues that are** going all around because of self-disclosure of information on Twitter, Facebook, Instagram and other networks.

**Parallely** in one side this increase in public information is going on. In parallel there is also increase in face recognition accuracy. In earlier the accuracy which lower now the techniques, technologies that are actually improved. In particular if you look at networks like Facebook it is actually pretty high it is because they search **space** that they have to search for a particular face in the picture that you are uploading is actually **only** your friends, majority of the times **you're** going to be taking pictures with the friends to whom you are already are connected with or probably they are in a one, and one and half hour or two hours away from here.

So, that is **happening** on one side. And also this is whole idea of cloud, storing information on the cloud, easily able to compute, computing cost is becoming lower and lower for doing any of these analysis. On the fourth dimension, **problem is that** identification of this users, who they are, what kind of information they are valuing is also getting better. Meaning, the concepts like **k-anonymity came in** 15 or 20 years before, but certain many further and advance techniques that have been developed to identify users, to identify faces, to identify information about users, to re-identify people on social network, people on other networks.

Those are four different things that are **eluding**; one, increasing self-disclosure, improving the accuracy of face recognition techniques, the whole idea of cloud and ubiquitous computing, and the techniques for re-identification of users is actually getting better and better.

(Refer Slide Time: 12:33)



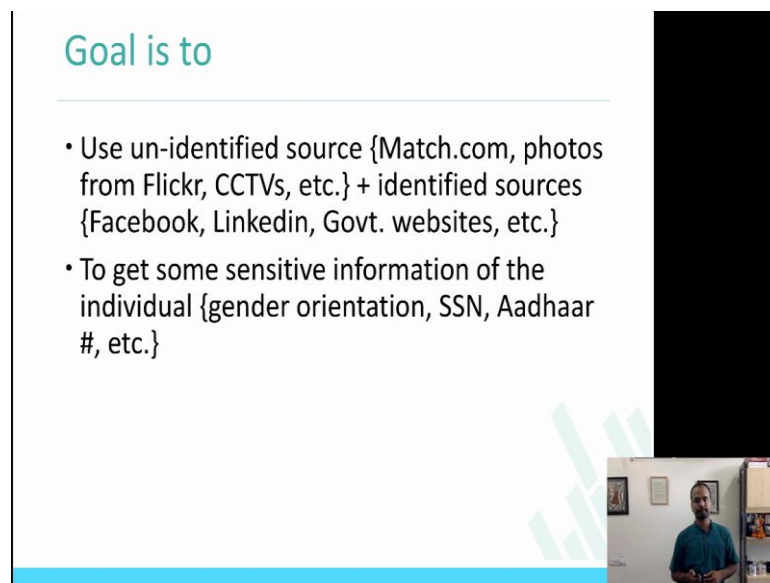
**Question**

- Can one combine publicly available online social network data with off-the-shelf face recognition technology for
  - Individual re-identification
  - Finding potentially, sensitive information

The one important question and one interesting question that people could ask is, can one combine publicly available online social network data with the off the shelf face recognition technology which is something that is already available, and be able to re-identifying individuals and finding potentially sensitive information. So that is the question that we were talking about in the **next deck of** slides which is, can we take some publicly available information which is that the things that I had upload on Facebook, the things that I had upload on Twitter.

Can you use that and connect it with the off the shelf face recognition technology which is some tools like **tensorflow** that I will also mention later in the slides. Use these techniques to identify just basis and be able to actually re-identify the person and or also find out sensitive information about the users themselves. That is the question that we will be talking about right now.

(Refer Slide Time: 13:35)



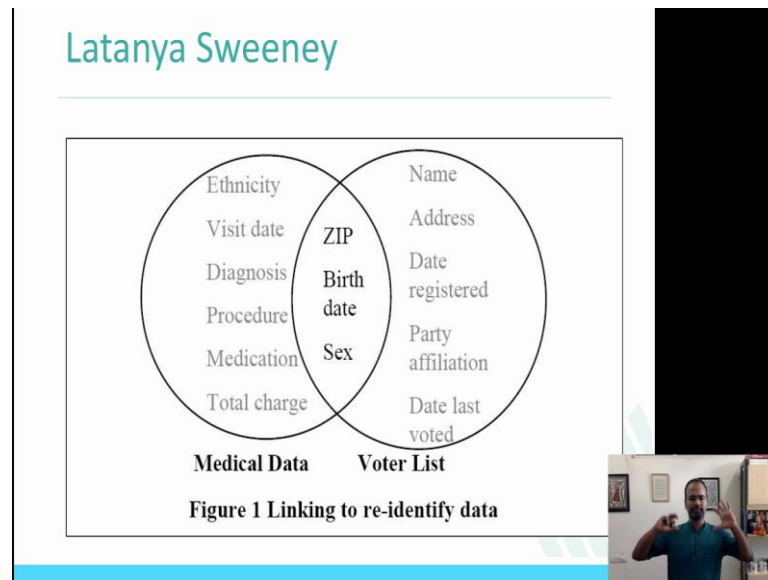
**Goal is to**

- Use un-identified source {Match.com, photos from Flickr, CCTVs, etc.} + identified sources {Facebook, LinkedIn, Govt. websites, etc.}
- To get some sensitive information of the individual {gender orientation, SSN, Aadhaar #, etc.}

Here is a goal. Goal is to use un-identified sources which is any websites that **you can think of**, match dot com, shaadi dot com, photos from Flickr, CCTV **feeds** and things like that, which is impossible to identify or its very **hard**, the user themselves are not disclosing who they are in these websites. It could be either they have **pseudonyms** and names that you cannot identify or re-identify to that particular person. Can we actually take these sources, shaadi dot com and pictures from Flickr and Facebook, connected to identify sources which are on Facebook, I would actually **reveal** that I am so and so on.

On LinkedIn I will put this as I am so and so, on government website and other services that are available. Which is un-identified sources like, shaadi dot com, identified sources which is **where** I am disclosing that I am so and so, and I upload a picture my account is **actually ponnurangam.kumaraguru**, can we actually put these two together to get some sensitive information of the individual. For example, gender orientation like example Social Security Number, like example **Adhaar card** number and the information like that. It can be pretty nasty if you can actually put this together and the get some personal information. So that is what we will be studying in our next slots.

(Refer Slide Time: 15:00)



Just to give you some very broad old view of some **phenomenal work** that was done in this topic **Latanya Sweeney**, who did this word called **k-anonymity**, where she actually picked up the medical data and connected to the voter list which is publicly available. If you look at the medical data she has ethnicity, visit date, diagnosis, procedure, medication and the total charges that was paid by the patient. Name, address, date registered, party of affiliation, date last voted. Taking this information which is from voters list and from the medical data putting it together she had found actually zip code, birth date and gender was actually common among both of them.

She was able to identify if you give the system that she **built** birth day and gender she was able to re-identify a lot of **US** citizens **uniquely**. So that is the idea that **built on** to create something called as k anonymity, but the problem she highlighted was that bringing these two different sets of data which is independent medical data and voter data, you could actually re-identify users **uniquely**.

(Refer Slide Time: 16:18)



## Experiment 1

- Online – Online
- Mined publicly available images from FB to re-identify profiles on one of the most popular dating sites in the US
- Used <http://www.pittpatt.com/> for face recognizing
  - Pittpatt acquired by Google
  - Face detection
  - Face recognition
- Use Tensorflow now

The slide features a light blue header with the title 'Experiment 1'. Below the title is a horizontal line. The main content is a bulleted list. A video inset in the bottom right corner shows a man in a blue shirt speaking. The slide has a light blue footer bar.

In experiment one, they actually connected the online data to the online data. They interestingly mined publicly available images from Facebook and they going to re-identify profiles just on one of the most popular dating sites in the US. They used this tool called pittpatt dot com, which was face recognizing tool. Well, after the study was done the tool was actually acquired by Google it is doing face detection and face recognition. You could actually use Tensorflow now. Tensorflow is a open source library for machine learning techniques. Please consider exploring tensorflow little bit and how it works and what are the libraries that are available inside tensor flow.

(Refer Slide Time: 17:06)



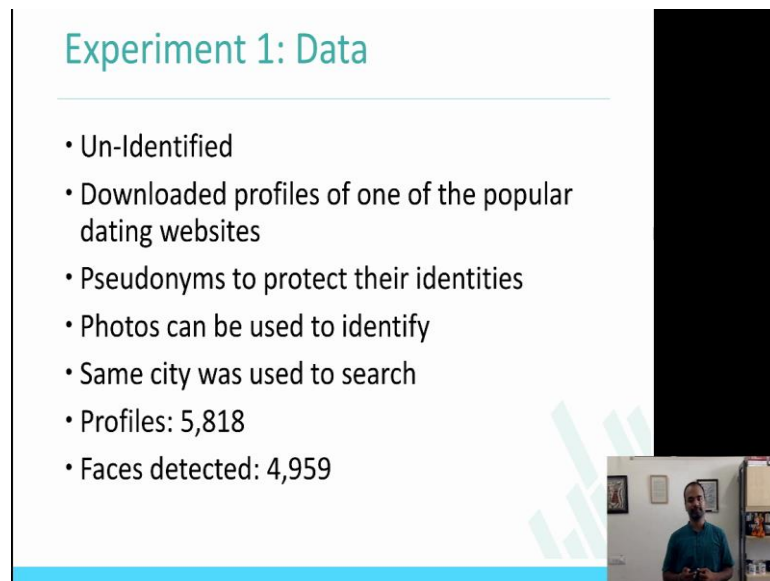
## Experiment 1: Data

- Identified
- Downloaded FB profiles from one city in USA
- Profiles: 277,978
- Images: 274,540
- Faces detected: 110,984

The slide features a light blue header with the title 'Experiment 1: Data'. Below the title is a horizontal line. The main content is a bulleted list of statistics. A video inset in the bottom right corner shows the same man in a blue shirt speaking. The slide has a light blue footer bar.

The data that they used was first as I said; they took the identified data, they downloaded the Facebook profiles from one city in the US which is possible in the way that you know about Facebook data collection now you could actually collect data from a particular city. Profiles that they collected were about 270,000, images that were collected around 274,000. The faces that are detected were about 110,000 faces. This is the data that they had for the identified data set, which is where you could actually say these are the names; these are profiles that are connected to these pictures.

(Refer Slide Time: 17:50)



**Experiment 1: Data**

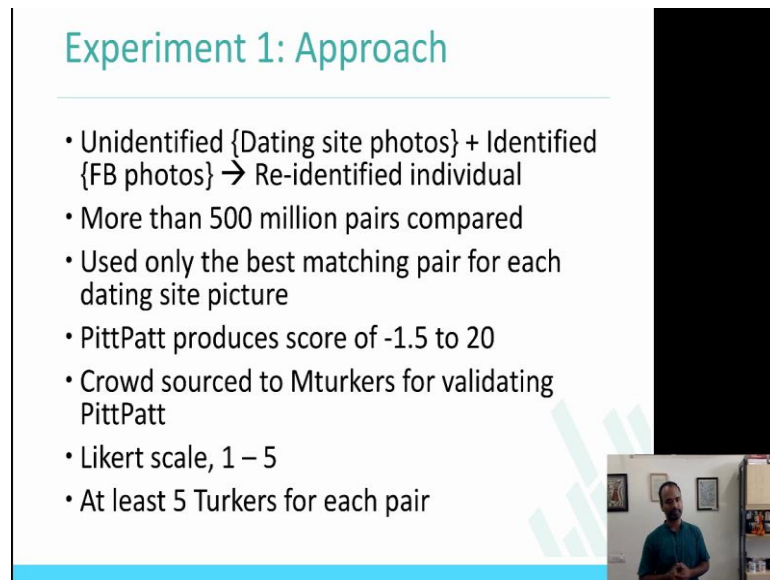
- Un-Identified
- Downloaded profiles of one of the popular dating websites
- Pseudonyms to protect their identities
- Photos can be used to identify
- Same city was used to search
- Profiles: 5,818
- Faces detected: 4,959

The slide features a light blue header with the title 'Experiment 1: Data'. Below the title is a list of seven bullet points. To the right of the text is a vertical black bar. At the bottom right of the slide, there is a small video inset showing a man in a blue shirt speaking. The slide has a light blue footer bar.

Un-identified data, they downloaded the pictures of one of the popular dating websites. So first identified, take a back; the first is the identified data, now we are talking about un-identified data, which is like the CCTV camera, publicly available information or from **match dot com**, shaadi dot com. They downloaded the profiles and the pseudonyms of their, to protect their identities, of course the names were not going to be **revealed**, the accounts may actually have pseudonyms also.

The photos that were downloaded from these websites where actually used to identify the profile. To make the connection appropriate they actually use the same city for the search, they download data from Facebook and the city from this un-identified data set. The profiles that were collected here were about close to 6000 and the faces that were detected were about closed to 5000. So that is identified and that is un-identified data.

(Refer Slide Time: 18:51)



### Experiment 1: Approach

- Unidentified {Dating site photos} + Identified {FB photos} → Re-identified individual
- More than 500 million pairs compared
- Used only the best matching pair for each dating site picture
- PittPatt produces score of -1.5 to 20
- Crowd sourced to Mturkers for validating PittPatt
- Likert scale, 1 – 5
- At least 5 Turkers for each pair

The slide features a light blue header with the title 'Experiment 1: Approach'. Below the title is a list of seven bullet points. To the right of the text is a vertical black bar. At the bottom right of the slide, there is a small video inset showing a man in a blue shirt speaking in a room with a whiteboard and a refrigerator in the background.

The approach that was taken was un-identified data, dating website, identified data, Facebook profiles and the re-identification was to be done. More than 500 million pairs were actually compared, because if each picture and each of the profile, each of the data set were compared with each of the pictures in the other data set, from the un-identified to the identified and the reverse also. What they did was, they did only used the best matching pair for each of dating site picture, and pittpatt and I am sure in tensorflow also it gives you in specific values, it actually produces values in some range they use the best value that they could get in terms of comparing two pictures.

And to confirm, to get ground truth when this pictures are just the same data sometimes if the techniques that are machine learning techniques are not going to be fool proof and they are not going to make 100 percent right prediction. Therefore, they are actually showed these pictures to Mturkers, the users who are part of mechanical turk which is a crowdsourced mechanism where you can actually put a small task of like this identifying where these two pictures are same people and you could actually pay them small money for doing the task.

And there were asked to rate the pictures on the likert scale of 1 to 7, at least 5 Turkers for each pair. Again please try and look at what are Mechanical Turkers, mechanical turk is a crowdsourced mechanism. For example, if I were do a task in identifying whether a given email is phishing or not I would actually it show to the Mturkers, I would create

the task on mechanical turk and get users to actually look at the image and say whether it is phishing or not. Look at the profile and Twitter to say whether it is fake or not, they would actually go to the profile, they would click on the link in go to the profile in Twitter look at the profile and then make a judgment whether it is legitimate or not.

So it is the very popular and there are many many services like this, crowd flower which is mechanism in which many of these services come together, it is also very popular crowd flower is one - c r o w d f l o w e r, is one of the popular services like this - Mechanical turk which is from Amazon is also very popular. They took these two pictures showed to users, mechanical turkers asking to actually compare the images and make the decision. So, at least 5 Turkers for each pair because **then we'll** see more confidence, more and more people say that, more and more people take a image and say that this is the chair and there is high confidence that is going to be a **chair**.

(Refer Slide Time: 21:37)

**Experiment 1: Results**

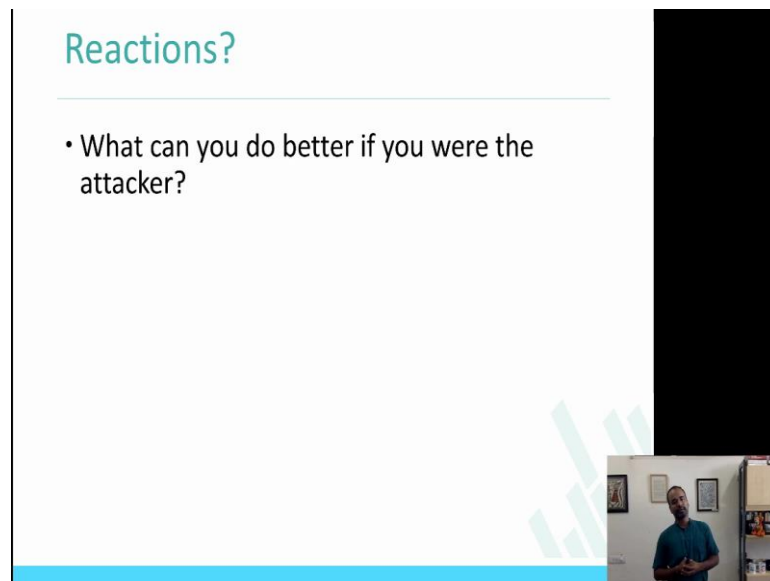
- Highly likely matches: 6.3%
- Highly likely + Likely matches: 10.5%
- 1 on 10 from the dating site can be identified

What they were able to find out was highly likely, which on the likert scale, is highly likely matches where about 6.3 percent that images that they took from this un-identified and identified and randomly they compared using the pittpatt tool and showed in the mechanical turkers. The comparison highly matches were about 6.3 percent and highly likely and likely matches were about 10.5 percent. Which basically says that 1 on 10 from the dating site can be identified, because the dating site **is an un-identified** data set, whereas Facebook is my identified.



So every time I see one of the pictures in the 10 pictures that I see, I will be able to actually clearly exactly identify who this person is, because I have the Facebook data, this is done of the same city and therefore it should be probably correct and mechanical turkers actually confirmed that. So, you can see that 10 percent of the times the users can be actually identified.

(Refer Slide Time: 22:40)

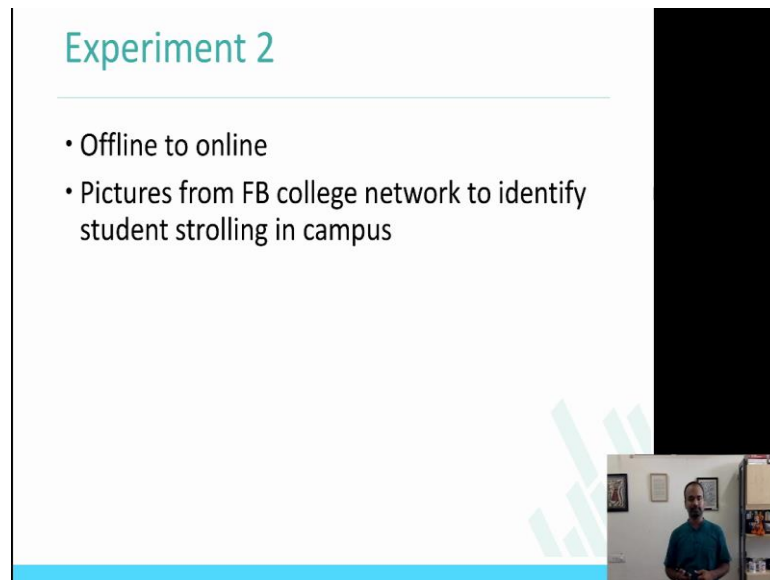


Reactions?

- What can you do better if you were the attacker?

One question to you and I hope this question since there will be some discussion in forum also is that; what can you do better if you were the attacker? And if you were make use of this information and do something to increase the rate of the efficiency or use this information to do something against the user what kind of things would you do Because as an attacker you making one this percentage to be more right, because it is 10 percent you're getting a hit rate of only 10 percent, or 1 and 10 pictures. Whereas, if you were to have a better attack or threat mechanism you could actually do things by which you can increase this percentage to more, so more and more pictures are actually re-identified and therefore it can be actually used maliciously.

(Refer Slide Time: 23:01)



**Experiment 2**

- Offline to online
- Pictures from FB college network to identify student strolling in campus

A small video inset in the bottom right corner shows a man with a beard wearing a blue t-shirt, standing in what appears to be a kitchen or office setting.


Experiment 2 as I said there are 3 things. So the second one what they did was they connected the offline and the online. First one, they compare online versus online which is the dating website and Facebook, now what they did was they did the offline and the online.

Pictures from Facebook, one of the Facebook college network **data was collected** to identify students who are in campus and it was actually compared to the offline pictures also. What **was** stated when the students were actually participating in the **study**. So this is the experiment number 2; all connecting to the same questions which is can we actually take images, pictures from these social networks like Facebook and re-**identify** people who connected to networks, to data where users cannot **get** in from, CCTV source in.

(Refer Slide Time: 24:21)

## Experiment 2: Data

- Webcam to take 3 pics per participant
- Collected over 2 days
- Facebook data for the university
  - Profiles: 25,051
  - Images: 26,262
  - Faces detected: 114,745




So, what they did was they actually put a booth in the university, took 3 pictures of the participant, they basically were standing and collecting data of the college students in this university took 3 pictures for participant, collected data over 3 days. They collected about 25 percent profiles, images were about 26,262 and the face is detected were about 114000, so Facebook data for that university. So, the data that were collected from Facebook which is online is about 25000, profiles were about 25000, pictures were about 26000, faces were about 114000 thousand.

(Refer Slide Time: 24:59)

## Experiment 2: Process

- Pictures taken of individuals walking in campus
- Asked to fill online survey
- Pictures matched from cloud while they are filling survey
- Last page of the survey with options of their pictures
- Asked to select the pics which matched closely, produced by the recognizer

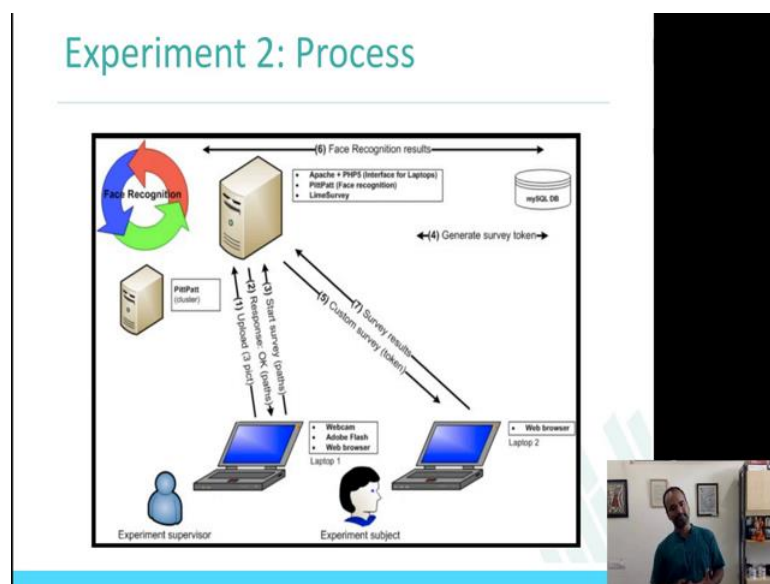


Just to summarize or just to look at the whole experimental set up itself is that, pictures taken of individuals walking in campus, asked them to fill the survey. Next slide I also have a image to actually show you what was the process of the study. But now pictures were taken of the individuals walking on the campus, they were asked to fill an online survey. Pictures matched from cloud while they are filling the survey, because what they did was they ask that you want to participate in the study, ok I will take you 3 pictures, when they took the pictures then they asked into fill on online survey.

While they were actually filling the online survey, technique the system that they are acted would go compare this pictures what they are took to the Facebook pictures that they are already collected from the university itself and bring back the comparison and showed to them. Last page of the survey with options of that pictures, so by the time they actually fill the survey they were actually shown the pictures, saying what this is the picture that we got from Facebook, do you actually agree to it. Asked to select the pics which matched closely, produce by the recognizer.

So, that is the process of the study, please understand how the study was done, collected pictures were taken individually walking in campus, they were asked to fill the survey, while filling the survey the data the system was comparing the pictures on Facebook, pictures were brought back to the survey showed to the user and saying tell us if these pictures are right about you.

(Refer Slide Time: 26:28)



Same thing is captured here in the process format in the background, which is upload pictures of the users, pictures are taken which is 1 and then responses coming from the server, start survey which is 3 and then 4 is generated survey token, so that through this survey token you will actually be able to say that comparing the images and bringing it back, which is 5 is looking at custom survey tokens send to the user who can actually fill the survey. And then by the time of 6 is happening which is face recognition results are being produced and then survey results both the images that are actually used which is given to 7.

So that is the process of the study, not a very difficult, not a very complicated study but it is actually collecting some very interesting data.

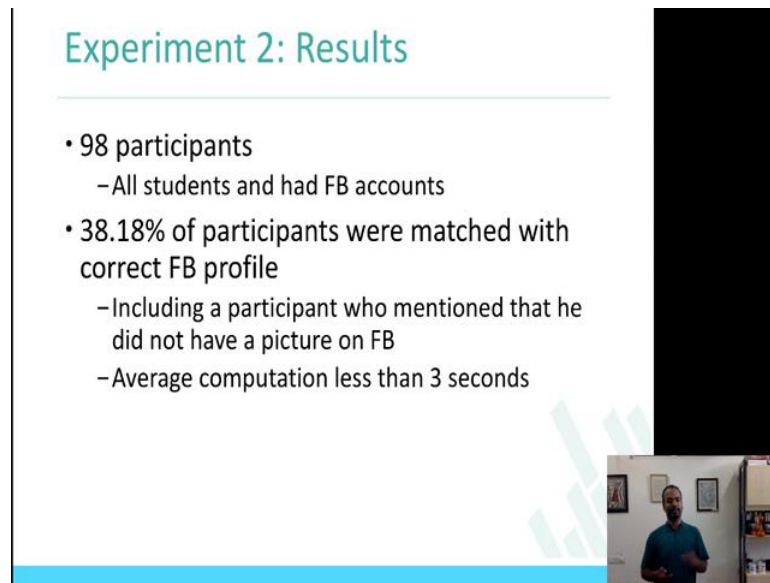
(Refer Slide Time: 27:22)



This is the result what they did from the data collection. The left picture is the picture autonomous to the picture for the purpose of just re-identification of the user itself. The picture on the left is the picture that they took while the user was actually participating in the study. So when the user logged in they took the picture that on the left.

Using that the picture they are able to actually identify the picture on the right which is the picture from Facebook where this user was actually identified. So, that is the output so to say, the input is the picture with the survey and output is the image from Facebook which is re-identified this person in particular pictures. This can be actually pretty revealing the pictures compared on Facebook.

(Refer Slide Time: 28:06)



## Experiment 2: Results

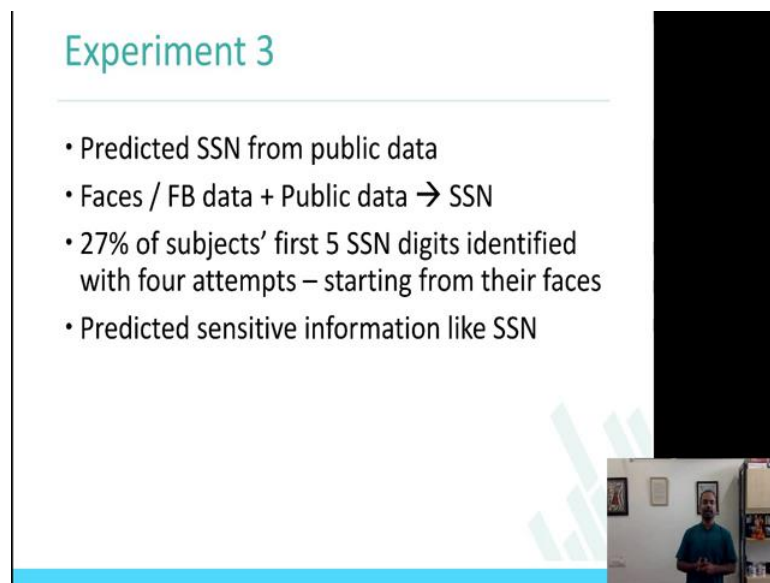
- 98 participants
  - All students and had FB accounts
- 38.18% of participants were matched with correct FB profile
  - Including a participant who mentioned that he did not have a picture on FB
  - Average computation less than 3 seconds

The slide features a light blue header, a white background with a faint bar chart, and a small video inset in the bottom right corner showing a man in a blue shirt speaking.

In about 98 participants all students in the study, there were about 98 participants, all students were the ones who participated they were collecting it from the university **setup** and they all had Facebook accounts also. The results were 38 percent of participants were matched with correct Facebook profiles, which is the pictures that were taken, 38 percent of the people who took the pictures in the study were exactly matched with the Facebook profile and their account, their information is actually brought back to compare to confirm it with the user.

Interestingly there was also a participant who mentioned that he did not have the picture on Facebook, actually information of that particular person, of that particular participants was also brought back. Of course, it was actually taking very less time to do this comparison. I hope the study is making sense which is 38 percent of the times the users that were taken pictures from the university campus were identified from the Facebook profile.

(Refer Slide Time: 29:14)



**Experiment 3**

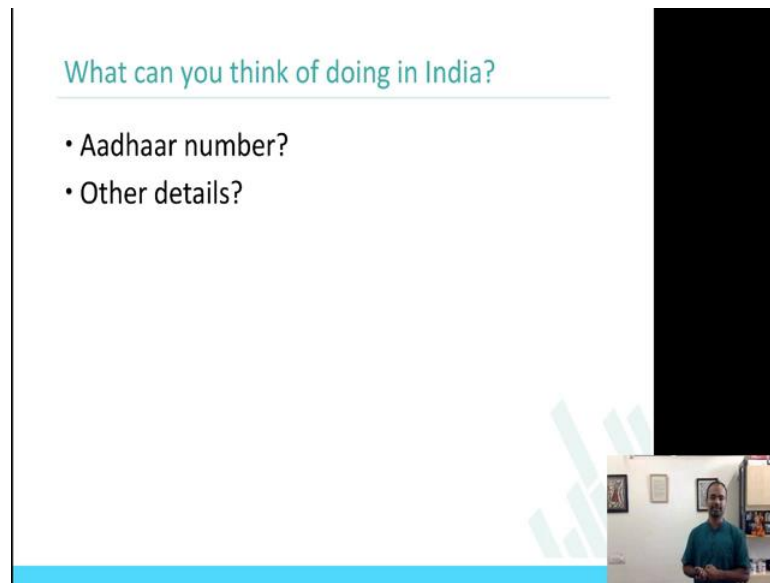
- Predicted SSN from public data
- Faces / FB data + Public data → SSN
- 27% of subjects' first 5 SSN digits identified with four attempts – starting from their faces
- Predicted sensitive information like SSN

The slide features a light blue header with the title 'Experiment 3'. Below the title is a horizontal line. The main content is a bulleted list. To the right of the text is a vertical black bar. At the bottom right, there is a small video inset showing a man in a blue shirt speaking. A faint bar chart graphic is visible in the background of the slide.

Experiment 3 is interesting because they actually tried using the experiment understandings from experiment 1 and 2 to take this personally identifiable with information likes Social Security Number. In this experiment 3 they wanted to predict Social Security Number from public data. So, they used the faces and the Facebook data that were collected from the experiment 1 and 2 with the public data to predict the Social Security Number. 27 percent of subjects' first 5 Social Security Number digits were identified with four attempts.

So essentially what is this means, this means that every time I took up a face from the database, I was able to identify the first 5 digits of the Social Security Number, 27 percent of the times. That revealing, that is not a very good sign, were 27 percent of the subjects were able to find out five SSN digits of them. So that is the third experiment. And I am keeping the third experiment little light because this is in total the interesting things were pictures, un-identified data sets, identified data set and at the end they were able actually do connected to social security member also.

(Refer Slide Time: 30:37)



What can you think of doing in India?

- Aadhaar number?
- Other details?

Interestingly I am **sure** you could also think about how these kinds of techniques can be applied in terms of identifying **Adhaar** number in India also and other personal details. The study was done in the US and therefore if you were to repeat this study and find out **Adhaar** number or others details of Indian Citizens it will be actually interesting to look at that. If there is any ideas, if **there** is any questions that you have in terms of how study could be performed in India, it will be interesting to talk about **it in the** forum.

(Refer Slide Time: 31:09)



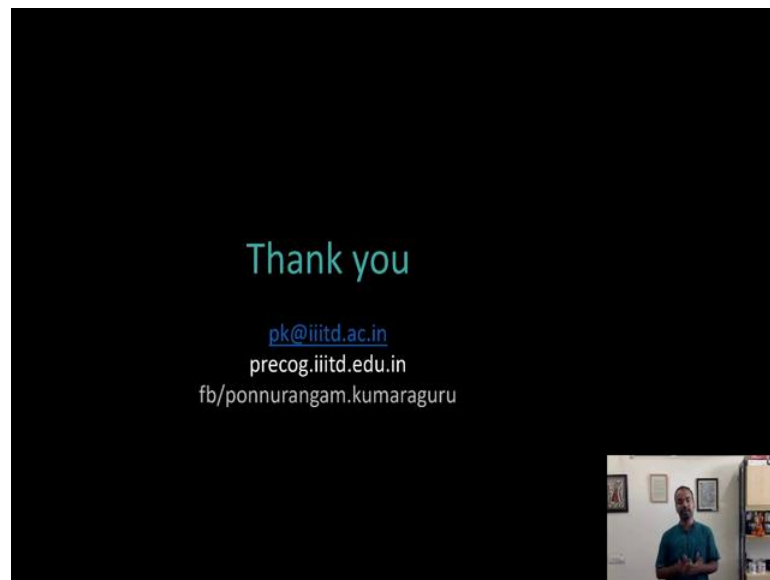
References

- <https://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf>
- <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>

Here are the pointers to study that I just now discussed about.



(Refer Slide Time: 31:17)



And with this I will actually wrap-up the 4.1 week. I hope you understood **what** we were talking about, we just talking about the Privacy Issues in Online Social Networks particularly focused on collecting images and identifying users using the face, pictures, using the images that are uploaded on social networks.