Online Privacy

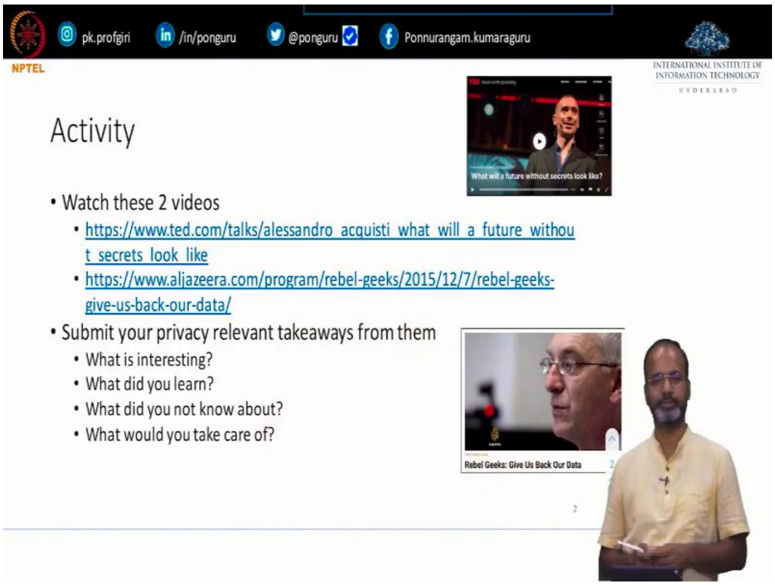
Ponnurangam Kumaraguru(“PK”)
Professor Giri
Department of Computer Science
Indian Institute of Technology, Hyderabad

Week 3 Lecture-03
Privacy-based technologies & decision making

Welcome back, NPTEL students for the week 3, I hope you enjoy the content that we created for week 1 and week 2, I hope you are also getting some insights on the topics outside the topics that we are covering in the class, because this topic is very, very engaging.

And you must be able to see some of these topics outside the class also must be able to relate to some of these topics outside the class also.

(Refer Slide Time 0:42)


pk.profgiri
/in/ponguru
@ponguru
Ponnurangam.kumaraguru
NPTEL
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD
What will a future without secrets look like?
Rebel Geeks: Give Us Back Our Data

Activity

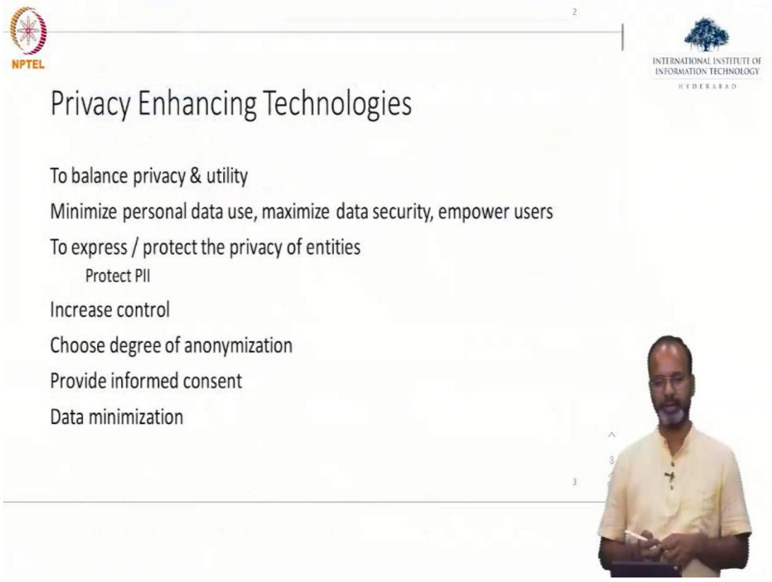
- Watch these 2 videos
  - https://www.ted.com/talks/alessandro_acquisti_what_will_a_future_without_secrets_look_like
  - https://www.aljazeera.com/program/rebel-geeks/2015/12/7/rebel-geeks-give-us-back-our-data/
- Submit your privacy relevant takeaways from them
  - What is interesting?
  - What did you learn?
  - What did you not know about?
  - What would you take care of?

2

So, I asked you to do activity last week, thanks for doing the activity. And thanks for actually sharing some of the comments on the mailing list, I encourage you to continuously do these activities, look at these videos, they are not really very difficult to look at.

And they are not very long also, so and there, many of them are public, open, so you should be able to actually watch it, and then make some comments about it in the mailing list, please consider doing it. And please come up with some interesting thoughts as you see these videos also.

(Refer Slide Time 1:23)



Privacy Enhancing Technologies

To balance privacy & utility

Minimize personal data use, maximize data security, empower users

To express / protect the privacy of entities

- Protect PII

Increase control

Choose degree of anonymization

Provide informed consent

Data minimization

So, what we will cover this week is actually going over some ideas called privacy enhancing technologies, privacy, invasive technologies, and then look at some social media privacy as well.

Privacy enhancing technologies by the name by itself, you can understand that this is technologies that will enable balance between privacy and athletic. So, we have been talking about privacy, until now, what is privacy, all that utility is functions that is available, for example, if you have swiggy the functionality or the utility that it is providing us to go order food. So, that is the utility.

So, how to balance between this act of ordering food and having privacy also is what the privacy enhancing technologies is all about. And keeping the privacy policy discussions earlier on Facebook and Twitter, balancing the act of I want to say what I wanted to connect to people around the world, I want to share information to the world.

But still I want to actually protect my privacy, that balancing act as for privacy enhancing technologies would be so, this is more like also called as pets. Privacy Enhancing Technologies minimized the goal for these technologies are minimized personal data use wherever possible, can the use of personal data be minimized, maximize data security and empower users right at the end of the day, we want to make sure that users have a great experience using the tool and they get what they want.

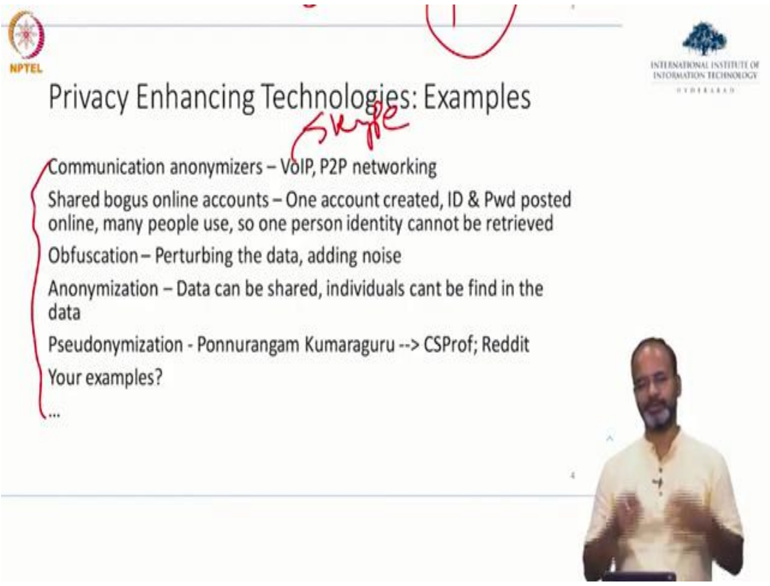
Using the using the functionalities and using the tools that is being built. To express protect the privacy of entities. Particularly I want to refer back to this PII personally identifiable information, which is what you want to protect using these technologies.

Increase control, which is connected to empower users choose degree of anonymization. So you also want to make sure that there are ways by which users actually can anonymize themselves. Meaning go back to the week 1, we talked about Weston’s categorization of users categorization, taxonomy or privacy by Daniel Solloway. All that keep, if you keep that in mind, you want to give you the continuum also, to set their anonymization, right, somebody wants to keep no anonymization to full anonymization.

That was choose degree of anonymization. Now let us look at provide informed consent. We have already seen what consent is for the users to actually sign up, opt in for some information or opt in for some functionality features all that informed consent, User should be aware of all the information for which they are consenting to.

So, they should be able to make a very informed decision on what they want. Data minimization which is already mentioned, relevant to minimize personal data used so that is, that is what privacy enhancing technology is very broad characteristics of what a privacy enhancing technologies are. So, now let us look at some examples of pet.

(Refer Slide Time: 5:06)



Privacy Enhancing Technologies: Examples

- Communication anonymizers – VoIP, P2P networking
- Shared bogus online accounts – One account created, ID & Pwd posted online, many people use, so one person identity cannot be retrieved
- Obfuscation – Perturbing the data, adding noise
- Anonymization – Data can be shared, individuals cant be find in the data
- Pseudonymization - Ponnurangam Kumaraguru --> CSProf; Reddit
- Your examples?
- …

First one, which I think some of these you may have already used, you may be already aware of, but I am just putting it in, in context for this class. specifically saying that these are privacy enhancing technologies as examples.

Communication anonymizers, Voice over IP. So, you must have used something like Skype, which fits this category. Where the people who are speaking, it is actually hard to find out who are actually involved in the in a conversation if we just give you the conversation between two people, peer to peer networking. And so, I am sure you are using a lot of these things for downloading movies, interacting with people, chatting with people, all of that these kinds of networks provide you the facility of being anonymous, as to share bogus online accounts.

Another the list here is just some methods by which you can actually do anonymization, you can actually do provide more privacy to the users. So, here is one method that people also tend to use, which is create one email address, publish the username and password for everybody to use.

And therefore, in the process, nobody will get to know who is actually using this email address and how it is being used. So, the personal information that is part of this email address will be actually because given that many people are using it, it is not possible to detect who the individual characteristics of the person who was actually using the email address, which is what it says one account created ID and password posted.

ID and password posted online many people use so one-person identity cannot be actually retrieved, obfuscation by the word obfuscation, meaning itself just add some noise by adding some noise in the data that you have.

For example, while you are browsing, can you actually make the browser do some activity by which that service that you are using thinks that there are activities that are not just you who is doing it, somebody else is actually doing that activity, from your own browser itself? In addition to whatever websites are accessing?

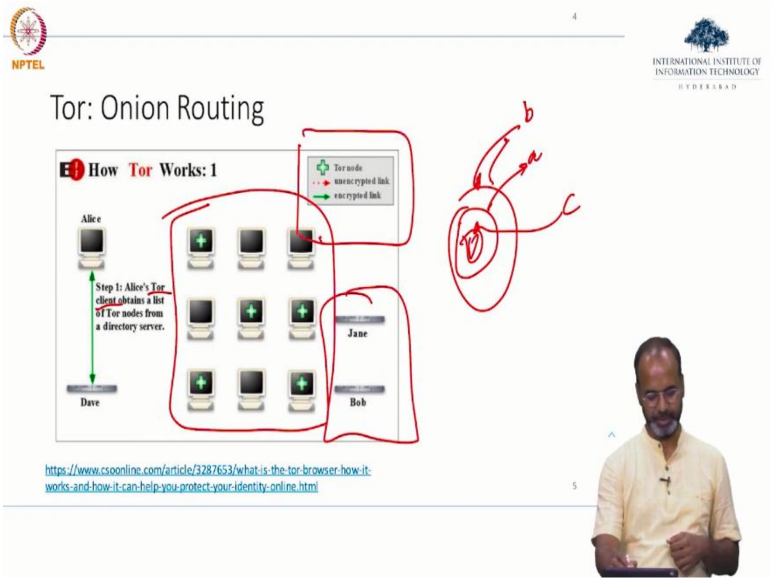
Can you add some noise that these websites also being accessed when you are not really accessing those websites, by which the service provider will think that you are accessing these websites and think create a persona personalization for you according to that, when it is not you who is actually doing it? So, that is like adding noise here.

That is the idea that you are adding noise. Anonymization, we will actually look at anonymization techniques later in the semester, look at different techniques, how anonymization can be done. But for now, data can be so example of healthcare provider hospital sharing the data with a data analytics company where the data analytics company can make some choices, analysis, results and give it back to the hospital is a good example for anonymization, data can be shared individuals can be found, if I am in the data set or not. It is impossible to find that is the idea for actually anonymization.

Pseudonymization. Where I think the idea of a breaded where you can actually use pseudonyms handles, Punnurangam Kumaraguru can become Prof. CS Prof. And then nobody would know that it is actually PK there, which is using the.

So, that is the idea for pseudonyms, I am sure you can come up with many examples. If you think of some examples where privacy enhancing, privacy enhancing tools that you use, is there please post it on mailing list, we can take it up and discuss it also.

(Refer Slide Time 12:07)



Tor: Onion Routing

How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

One very common and very important and influential technology that had come up for privacy enhancing technologies is actually Tor, which is built on this idea called onion routing, onion routing. The idea is, think of it as just onion when you start peeling onions. When you peel the outside layer, only the layer that is inside is visible to you.

You get to see only one layer at a time and that layer is just attached with the one layer that you peel and the one layer that is below that. If I peel this layer. If I peel this layer off, it is attached to this layer and attached to this layer, a layer is big getting peeled, b layer is this and c layer is this.

Just built on this idea that the only two layers are attached to the layer in between to the layer and that you are peeling it layer that you are looking at in any way you can see it. That is the idea for onion routing and Tor built on this onion routing method to provide anonymization and then the primary motivation for these kinds of technologies are like journalists.

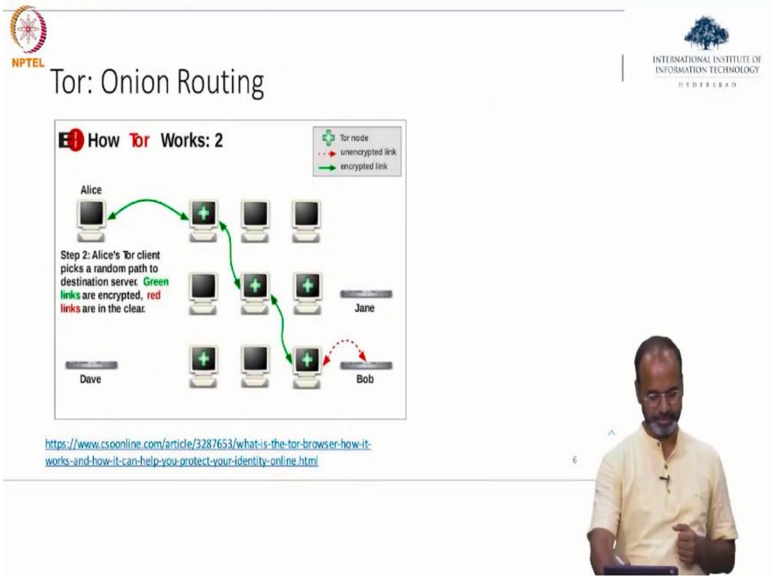
Journalists want to sit in some part of the world and share some information to their headquarters and nobody should know that they are the ones who are sharing it, nobody should know the, from where this information is coming all that.

So, that is the kind of, or the journalist wants to access some websites to write about it, and they do not want the trace of this particular journalist accesses website or the service should be tracked. That is idea for onion Tor. Here is next three slides just shows you how Tor works.

So, the idea is, step one, Alice's Tor client. So, some terms here is a Tor client, which is installed at Alice's place, let us take PK wants to access something obtains a list of Tor nodes from a directory server. So, I want to access some website, in that my client, my Tor client goes get a list of Tor nodes, Tor nodes are these three test let us take different servers that are connected on the Tor network gets the list of the star servers, my client. And then if these are other services that others people that I want to connect with.

And here it says through North Node unencrypted link and encrypted link, you will see all these colours. In the next slide also, here it is the encrypted link between the users that want to interact with I want to access some websites. That is the website that is being talked about here.

(Refer Slide Time 12:30)



Tor: Onion Routing

How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

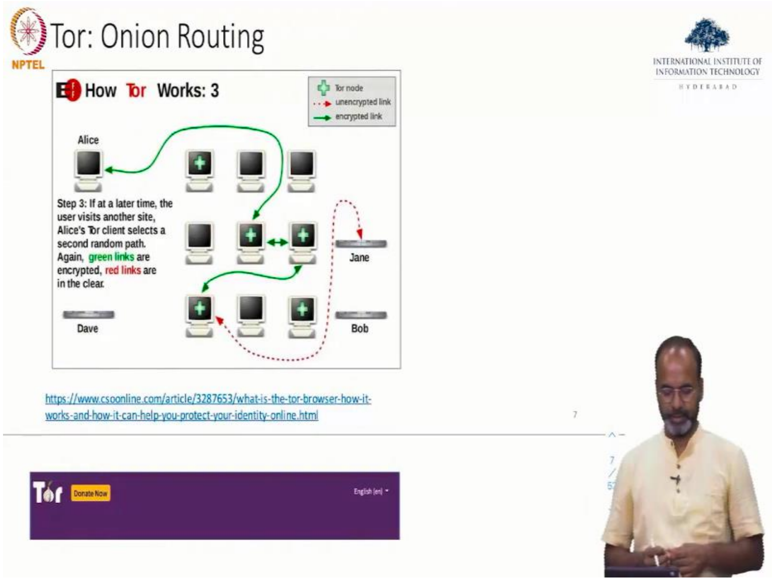
Step 2, Alice's Tor client picks a random path. So that is why is this random, we will come here for now. So, if we look at this, these are the these are the nodes. You want to keep the random because so that the traceability is not there, which is if Alice wants to go to another website later. That is not, you cannot trace back the path that Alice took because she is taking random parts every given time.

And every user in the network will take random paths every given point in time. That is one advantage of the Tor. The Alice's Tor client picks a random path to destination server green links are encrypted. Green links are encrypted and red links are in the clear text the last bit which is jumping from the exit node, it is called, the exit node to the service that I want to access is this one.

And where is the onion routing coming into picture? This sever, this node sort to say knows only the information that look it has to be sent to Bob and it is coming from let us take a server same whereas this node knows only that it is coming from here and it has to go here. So let us take this was B and this was C.

That is the reason why it is based on onion routing. And that is, that is what gives it the power of getting an anonymity while accessing the services.

(Refer Slide Time 14:16)



Tor: Onion Routing

How Tor Works: 3

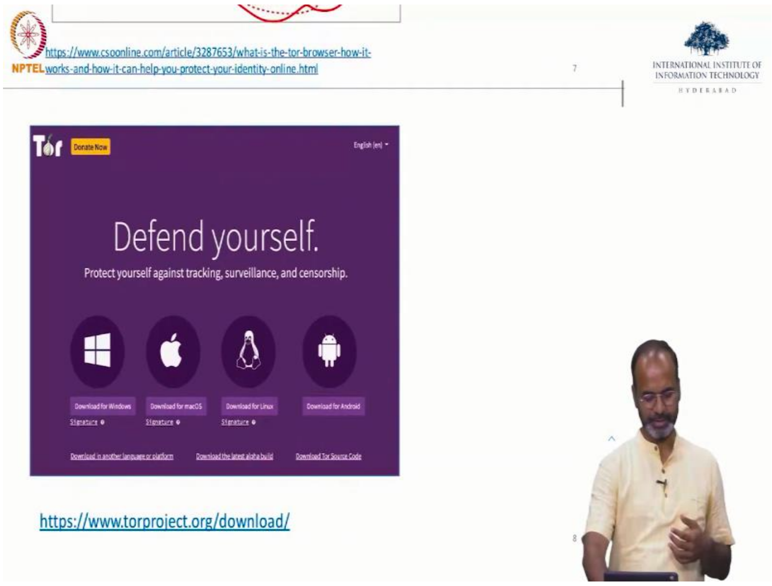
Step 3: If at a later time, the user visits another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

Step 3, if at a later time the user visits another website, Alice's Tor client selects second random path again green links are encrypted and red links are in the clear. It wants to go to another site which is this again here he takes, it takes a different path. So, it is taking a different path which was not the path that was taken first time and therefore the anonymity is provided.

And again, Onion Routing method still follows in this in this image also hope that helps you to get a sense of what a Tor is.

(Refer Slide Time 15:05)



https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

Defend yourself.

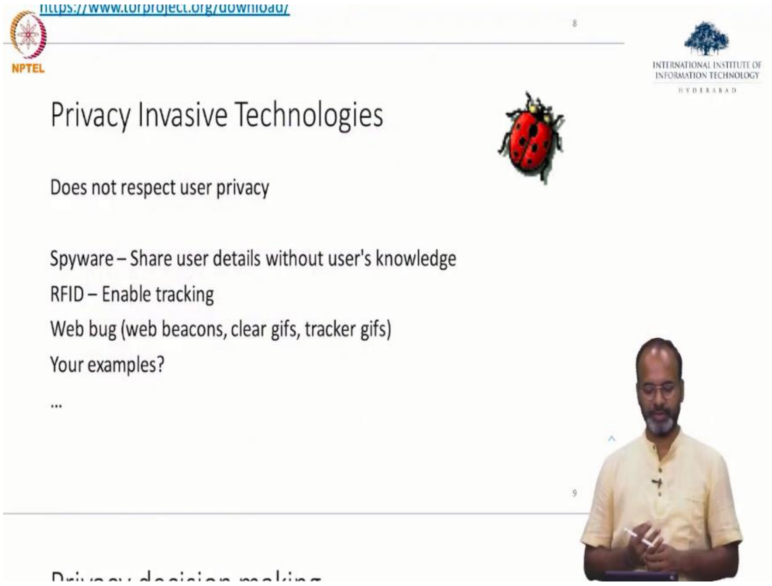
Protect yourself against tracking, surveillance, and censorship.

https://www.torproject.org/download/

This is come up with actually Tor is Tor has a browser also now you can actually go download the Tor browser and use it again, the way Tor browser works is the way I explained before. And you get anonymity to the services that you go access, you do not get, nobody gets to know you access these services.

I am sure you would understand now tar. Again, the there are many, many, there are many attempts to also show how Tor can be broken. There is a very active research area, which is to look at methods by which you can provide more and more these kind of anonymity, and how these anonymity can be broken. That is a very fertile research area, if you were to think about it.

(Refer Slide Time 15:55)



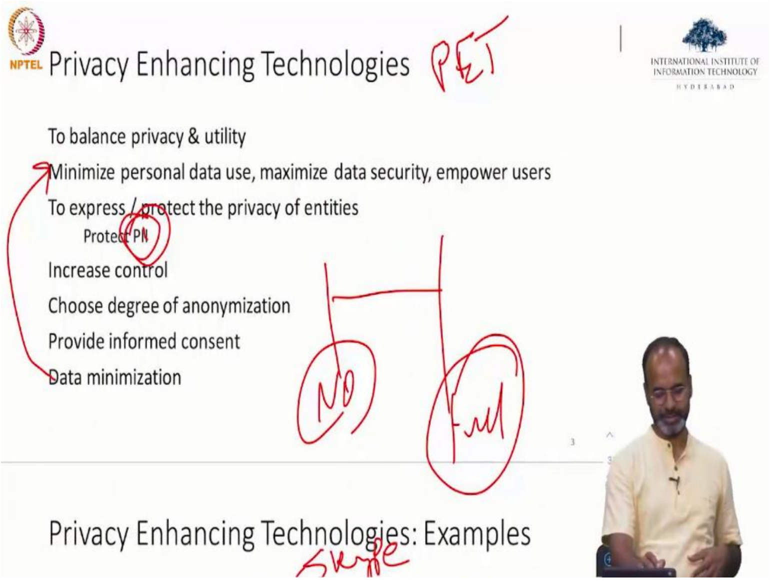
https://www.torproject.org/download/

Privacy Invasive Technologies

Does not respect user privacy

Spyware – Share user details without user's knowledge
RFID – Enable tracking
Web bug (web beacons, clear gifs, tracker gifs)
Your examples?
...

Privacy decision making



Privacy Enhancing Technologies

To balance privacy & utility
Minimize personal data use, maximize data security, empower users
To express / protect the privacy of entities
Protect PII
Increase control
Choose degree of anonymization
Provide informed consent
Data minimization

Privacy Enhancing Technologies: Examples

Next is privacy invasive technology even that we spoke what privacy enhancing technologies, I think itis very apt to discuss privacy, invasive technology, I am sure this list you can come up with a bigger list than what have written it here.

And then the basic idea is that it does not respect users privacy, if you were to think about if you were to go to this slide of where I defined what privacy enhancing technology is. And if you were not to do all of this, but become privacy invasive technologies.

Spyware is one example share user details without user’s knowledge, spyware sitting on your machine sending out information about your username, password, or your web history, those information is shared to a third party, which is what a spyware does. And that is actually breaking. That is, that is part of the privacy invasive technology.

RFID, RFID tag has a lot of positive usage in terms of understanding my production line, in terms of knowing where the product does all that, but it also has this negative effect of using the RFID tag, which is actually somebody can track the product, I buy the shirt, and then I have RFID attached to it, my some receiver can know if the RFID tags still on the shirt that I am wearing.

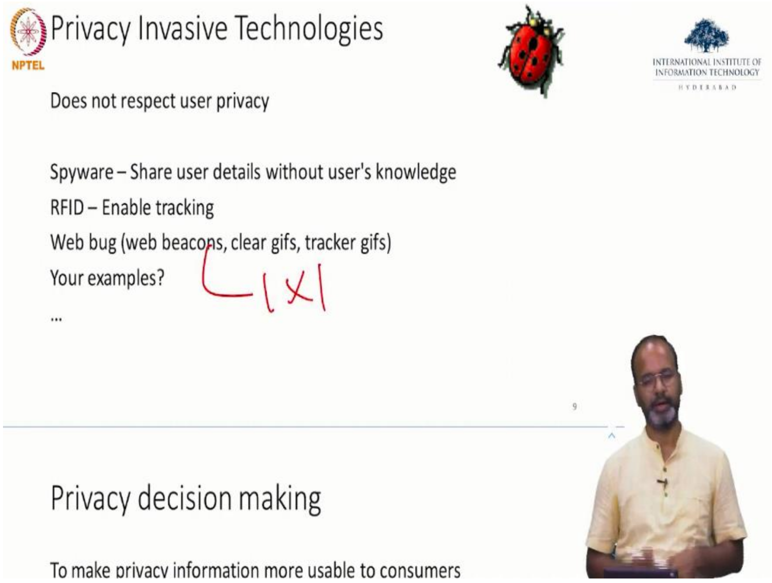
Again, there are the pros and cons, I think if you were to look at RFID by itself, you will understand more and more meaning that the receivers are not all around the world, the receivers are only at some point, at some places and also my RFID tag is not live always, for example, when you buy, I am sure you have seen many of the shops, where when you buy something they remove a plastic piece from the cloth, which is some kind of a tagging, you can think of it as a some chip that is there which is actually allowing and you will also see two devise at the entrance or exit of these shops, which can also understand or pick up signals that whether any of the products that is being taken out has this tags in it.

Similarly, you can think that this tags can be kept these receivers, so to say it can be kept anywhere and then kept, they can track us. If the RFID tag was not properly taken away when I bought the shirt.

And the advantages of these technologies are very helpful, for example, cattle management, You want to know, if I have like 1000 cows that I have to manage, I think it is going to be extremely hard to keep a count on which all has come in black to the back. And then it is going to be very hard to keep track of these calls.

So, therefore they put the RFID tag and then the receivers can keep track of who is and which call is inside. And they get a sense of okay, the 6 missing now we should go look for those 6.

(Refer Slide Time 19:30)



Privacy Invasive Technologies

Does not respect user privacy

Spyware – Share user details without user's knowledge
RFID – Enable tracking
Web bug (web beacons, clear gifs, tracker gifs)
Your examples?
...

Privacy decision making

To make privacy information more usable to consumers

A Web bug, another example this is a very simple idea. This is more like one by one pixel image that can be put on any website. Let us take you put on your own website, this one by one transparent image. And then anybody who comes to the website will your web page this web page will make a request for this image and therefore you know that somebody is accessing this website.

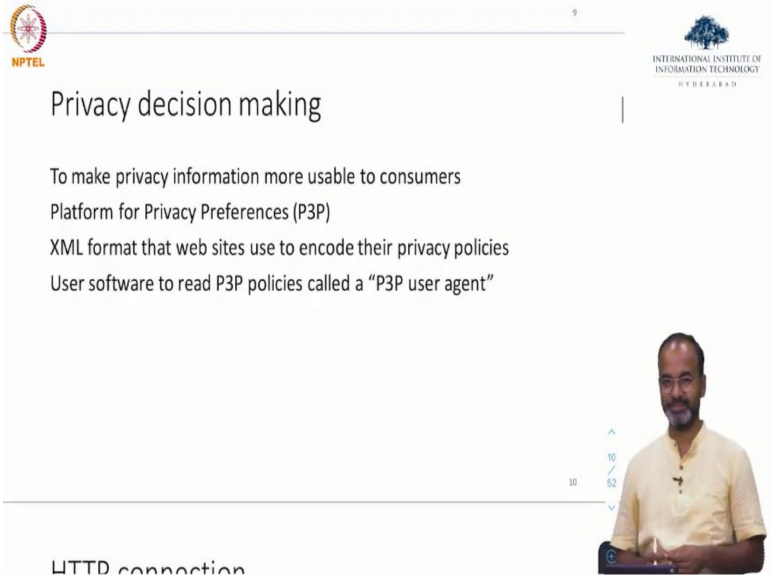
This image can be put on any web pages and therefore tracking can be done using this one by one transparent image. So that is what it is called Web bug. And it is also called as web beacons, clear gifs, tracker gifs, all of that. All of them mean the same thing. But the idea is this that it is put on a website. And then this image, so what, how the tracking happens because this image is being requested.

To serve this image on the page that the user is seeing, this image has to be served from a server. And that request is being made. That server can keep track of this image being this web page being visited, by knowing that, oh, this image from this website was actually requested. And you can also think about this image being served by a common third party now.

Multiple web pages can have one of this image is from a company A, and this company A can track all the websites that users are actually going to, and company A can produce analytics to the companies and to the services to the websites that people are accessing. And that can be very, very useful in terms of personalization advertisements.

So, that would give those are the list of privacy invasive technologies. And I am sure again, as I said before, you can have some examples in this list. And feel free to share the list that you have. So that was privacy invasive technologies.

(Refer Slide Time 21:40)



Privacy decision making

To make privacy information more usable to consumers
Platform for Privacy Preferences (P3P)
XML format that web sites use to encode their privacy policies
User software to read P3P policies called a "P3P user agent"

HTTP connection

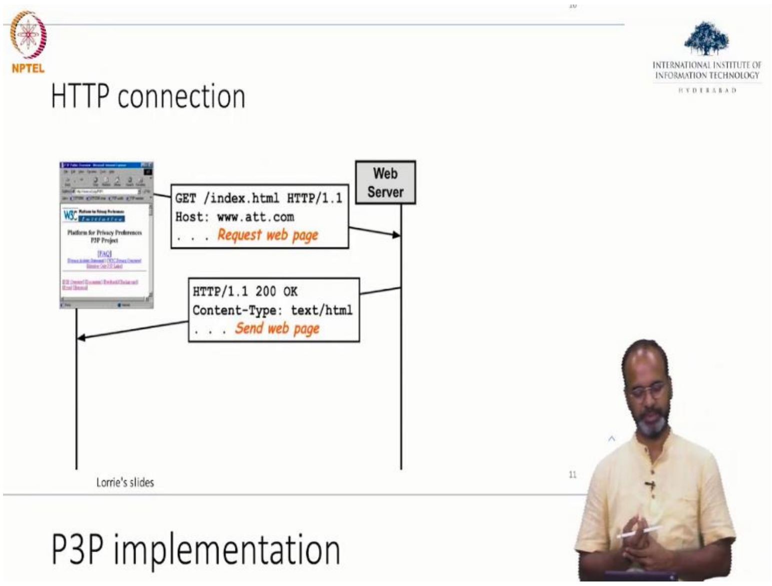
Now, let us look at some techniques by which these privacy enhancing can be done. And tools that have been developed in the past, which can provide more privacy to the users. Again, this is only a small sample. This is not comprehensive. We can go on, on this list if needed. But I am giving you some sense of what are the tools that can that are available, which can be used.

So, to make privacy information more usable to consumers, the decision making privacy decision makings. Is it a part of the privacy enhancing technologies itself, to help users make choices, of what all options that are available? A platform for privacy preferences is one technique, one solution that has been developed, where users can actually represent their privacy preferences. Companies can represent their privacy preferences, and some matching can be done in these preferences and decision can be made.

I am going to walk you through what it is. But in short, that is what it does. User privacy expressed in this P3P format, company's privacy expressed in this P3P format, a machine can understand both of this now, because it is expressed in a machine readable format. And this decision can be made whether this website does something I need to go or not go, should I be allowed or not allowed.

XML format, and when you think about it, this comparison can be done in many different ways. Some different methods could be built. One of the techniques that has been built is called privacy bird. But I am sure you can think of many other interesting way to set this comparison, set this user and company privacy policy comparison to be done.

(Refer Slide Time: 23:38)



HTTP connection

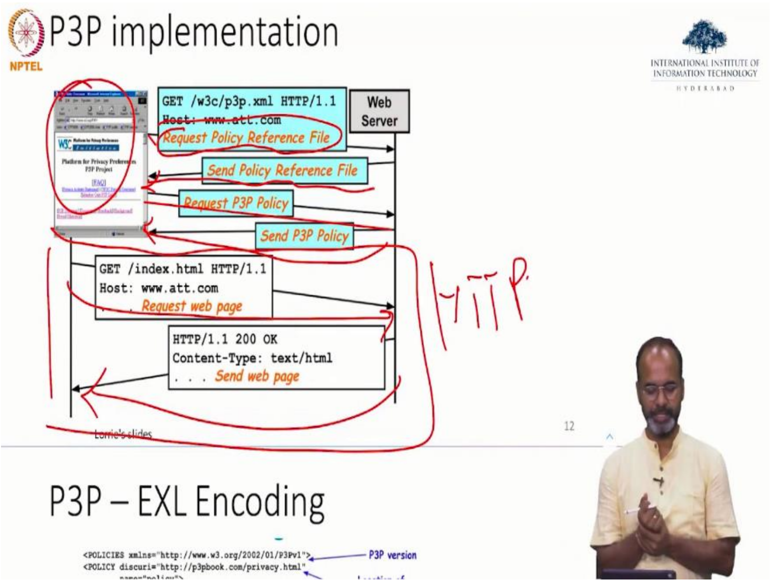
```
GET /index.html HTTP/1.1
Host: www.att.com
. . . Request web page
```

```
HTTP/1.1 200 OK
Content-Type: text/html
. . . Send web page
```

P3P implementation

How does a general HTTP connection work? It works in a way that, so, first a website is making a request this is W3C website a request is being made. Web server says, web servers looks at the request from PKS machine and it actually serves the web page as P3P, W3C website, it could be IIIT Hyderabad website also.

(Refer Slide Time: 24:11)



P3P implementation

```
GET /w3c/p3p.xml HTTP/1.1
Host: www.att.com
Request Policy Reference File
```

Send Policy Reference File

Request P3P Policy

Send P3P Policy

```
GET /index.html HTTP/1.1
Host: www.att.com
. . . Request web page
```

```
HTTP/1.1 200 OK
Content-Type: text/html
. . . Send web page
```

P3P – EXL Encoding

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"
```

How does a P3P work on top of this? P3P works like same website is being requested iiit.ac.in instead of actually the website being served my web server first IIIT’s web server first only looks at it is the request is sent as request.

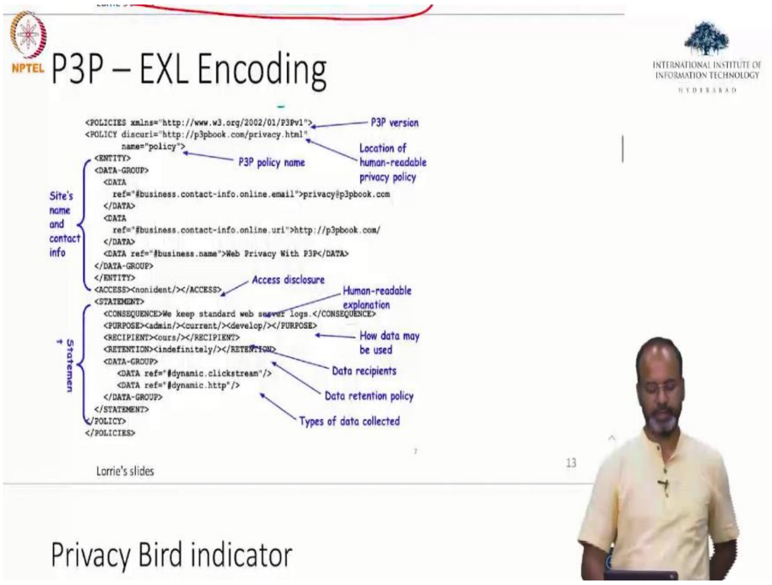
Policy reference file first it is not asking for the website. It is saying that look, somebody wants to access to iiit.ac.in and it gets the IIIT’s website.

And then it says can you tell me where your privacy policy reference file is and web server says OK, here is the location of my reference file. And then the browser is making the request for that particular P3P file, reference file, and the reference file is served. And now depending on the output that you can do, the web browser knows the P3P policy.

Now then the HTTP request is made on the web pages so, this part we already saw, this part is what the HTTP request is. So, that is how P3P works again, quickly, let me go through it again, instead of just the web page being requested and web page being served, first the reference file is requested, what is the reference file, reference file is the place where the HTML is kept P3P XML format file is kept.

And when I know that location, then the browser makes a request for that particular P3P file, P3P file is served. And then now that P3P file has the preferences of the company, which you can think of it as all the privacy policy that we have seen until now, that format is converted into a P3P file, that P3P file is what is served back to the webpage. And then the webpage makes a request to the for the iiit.ac.in. So, that is what how a P3P works.

(Refer Slide Time: 26:25)



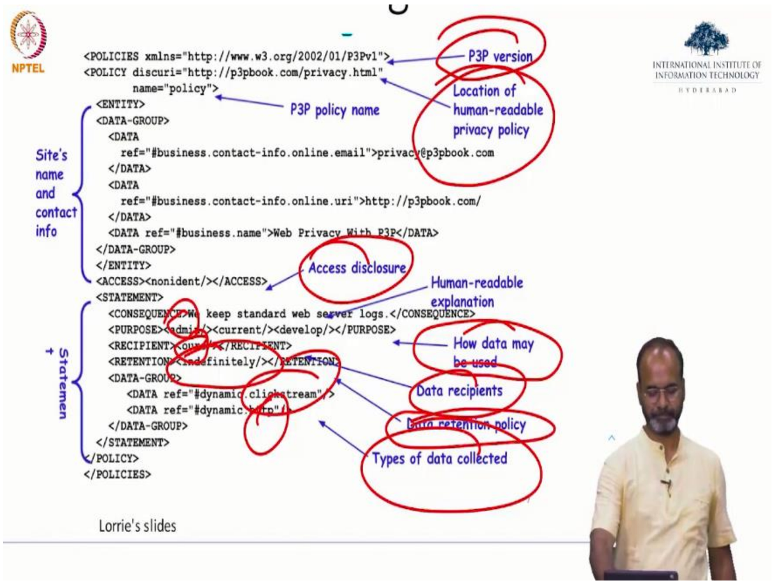
P3P – EXL Encoding

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"
        name="policy">
  <ENTITY>
  <DATA-GROUP>
    <DATA
      ref="#business.contact-info.online.email">privacy@p3pbook.com
    </DATA>
    <DATA
      ref="#business.contact-info.online.uri">http://p3pbook.com/
    </DATA>
    <DATA ref="#business.name">Web Privacy With P3P</DATA>
  </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <STATEMENT>
    <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
    <PURPOSE><admin/><current/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA ref="#dynamic.clickstream"/>
      <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```

Lorrie's slides

13

Privacy Bird indicator



```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"
        name="policy">
  <ENTITY>
  <DATA-GROUP>
    <DATA
      ref="#business.contact-info.online.email">privacy@p3pbook.com
    </DATA>
    <DATA
      ref="#business.contact-info.online.uri">http://p3pbook.com/
    </DATA>
    <DATA ref="#business.name">Web Privacy With P3P</DATA>
  </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <STATEMENT>
    <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
    <PURPOSE><admin/><current/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
       <DATA ref="#dynamic.clickstream"/>
       <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```

P3P version

Location of human-readable privacy policy

P3P policy name

Site's name and contact info

Access disclosure

Human-readable explanation

How data may be used

Data recipients

Data retention policy

Types of data collected

Statemen t

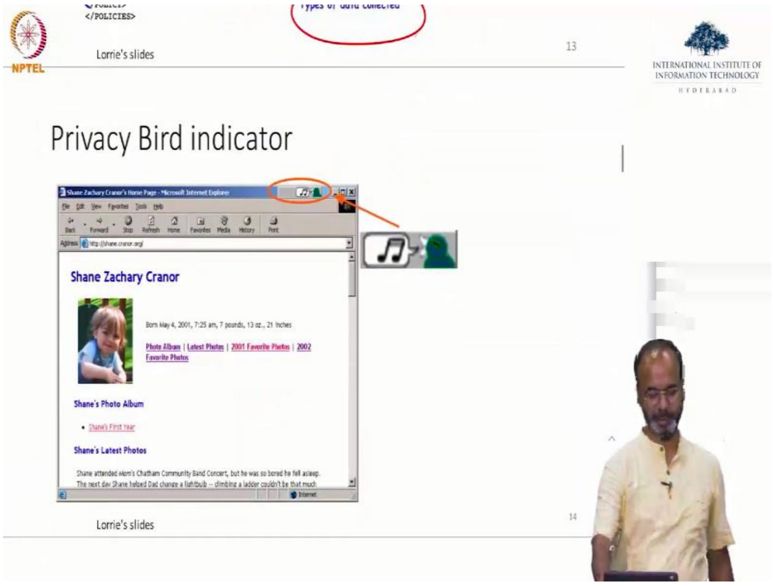
Lorrie's slides

So, as I said P3P is an XML. So, here is an example of what the P3P XML file could look like. And what all should it cover, it should cover the same things that we said. Which is a everything in the privacy policy, the concern, data protection, security that it is provided all the Swiggy's and Amazon's policies that we saw, can be expressed in this XML.

So, this shows policy, what version of the P3P policy is, location of the human readable policy. So, you should know that iiit.ac.in slash privacy is where the privacy policy is. This is the access disclosure, human readable explanation, how data may be used, data recipients, which is who gets access to the data.

So, this is our, this is our admin who is getting access to the data. And then retention, data retention policy, how long the policy can be kept, data can be kept with off the users in definite needs is here. Types of data collected, which is clickstream HTTP, all that. It is talking about data being collected, who has access to the data, how long they can keep the data with them. Think of it as a privacy policy of any of the organizations that we have seen until now. That is P3P.

(Refer Slide Time: 28:09)



</POLICIES>

Types of data collected

Lorrie's slides 13

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Privacy Bird indicator

Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

Address http://shane.cranor.org/

Shane Zachary Cranor

Born May 4, 2001, 7:25 am, 7 pounds, 13 oz., 21 inches

Photo Album | Latest Photos | 2001 Favorite Photos | 2002 Favorite Photos

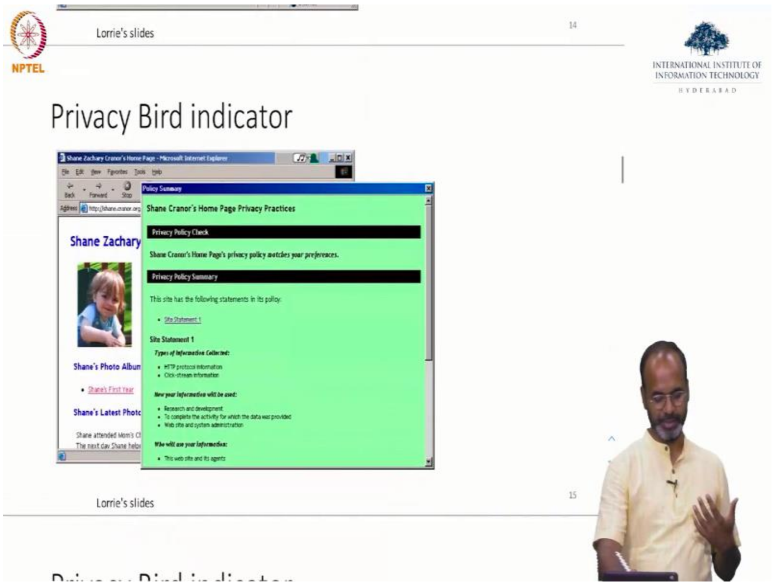
Shane's Photo Album

- Shane's First Year

Shane's Latest Photos

Shane attended Mom's Chatham Community Band Concert, but he was so bored he fell asleep. The next day Shane helped Dad change a lightbulb -- climbing a ladder couldn't be that much

Lorrie's slides 14



Lorrie's slides 14

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Privacy Bird indicator

Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

Policy Summary

Shane Cranor's Home Page Privacy Practices

Privacy Policy Check

Shane Cranor's Home Page's privacy policy *matches your preferences.*

Privacy Policy Summary

This site has the following statements in its policy:

- Site Statement 1

Site Statement 1

Types of Information Collected:

- HTTP protocol information
- Click-stream information

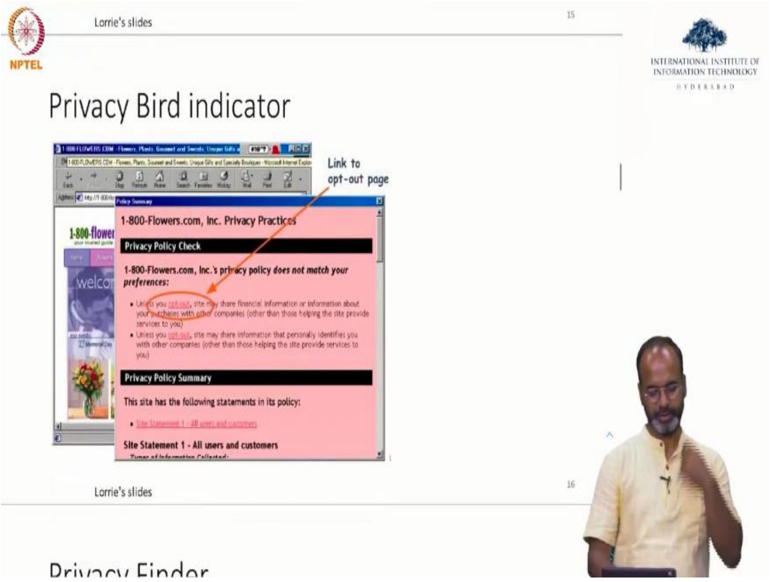
How your information will be used:

- Research and development
- To complete the activity for which the data was provided
- Web site and system administration

Who will use your information:

- This web site and its agents

Lorrie's slides 15



Lorrie's slides 15

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Privacy Bird indicator

1-800-FLOWERS.COM - Flowers, Plants, Gourmet and Sweets, Unique Gifts and Specialty Boutiques - Microsoft Internet Explorer

Link to opt-out page

Policy Summary

1-800-Flowers.com, Inc. Privacy Practices

Privacy Policy Check

1-800-Flowers.com, Inc.'s privacy policy *does not match your preferences:*

- Unless you opt-out, site may share financial information or information about your purchases with other companies (other than those helping the site provide services to you)
- Unless you opt-out, site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

Privacy Policy Summary

This site has the following statements in its policy:

- Site Statement 1 - All users and customers

Site Statement 1 - All users and customers

Types of Information Collected:

Lorrie's slides 16

Privacy Finder

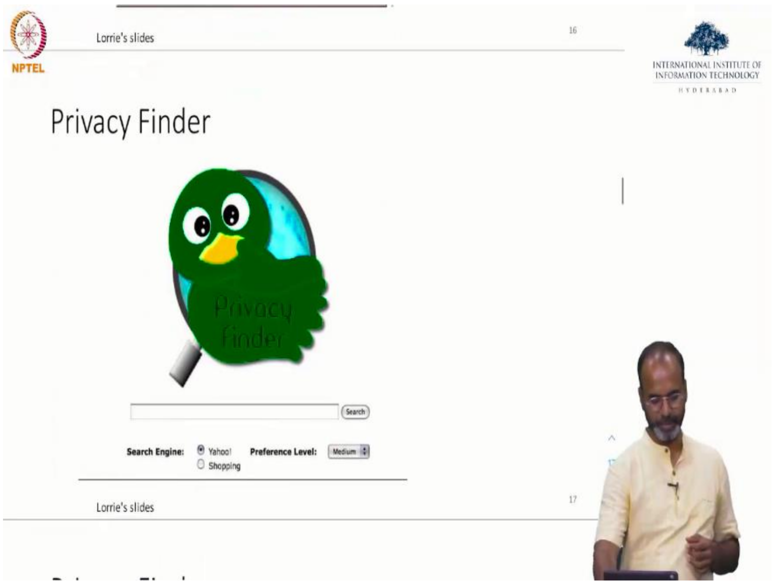
And, and now that the P3P policy is coming to a web browser, the browser can make a lot of decisions. As I said before, P3P is a way by which you can express the privacy policies in an XML format. Now that I have an XML format of IIIT's, IIIT Hyderabad's P3P policy. I can say whether PK is allowed to see that website on or is it aligned with PK's privacy preferences or not, which is what this privacy bird does.

Privacy bird looks at the privacy policy of iiit.ac.in it looks at my preferences, it makes it makes a sound which is if it is aligned, it makes a sound that it is okay in green. And if it does not, it makes it in red. Privacy bird and when it is, you can go look at why it is green and why it is red also, which is matching, if that matching is you say that look, my preference is that I want to go to websites only, which does not allow my information to a third party or which has retention policy as anything lesser than indefinitely which is 90 days only they should keep the information or which has an opt in option.

Any these kinds of preferences you can set easily. Again, you can set the preferences also using some tools. So, this is providing you what the policy matching is and here it is actually red colour. It is showing what where the matching is not there, where it is actually different.

So, if you read this line, it says, unless you opt-out, site may share financial information or information about you, which is the setting that I did not keep as I said, I had said that it should be where opt out option should be by default, the user should have opt-out option. Whereas here, opt-in option whereas here it says, unless you opt-out site maybe there, site may be using that information or sharing that information, think of opt-in or opt out again.

(Refer Slide Time: 30:42)

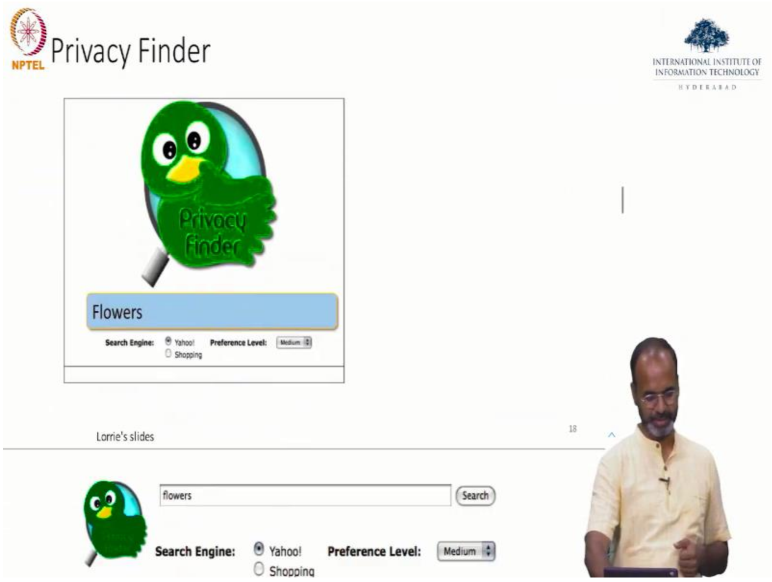


Lorrie's slides 16

Privacy Finder

Search Engine: ◉ Yahoo! ○ Shopping Preference Level: Medium

Lorrie's slides 17



Privacy Finder

Flowers

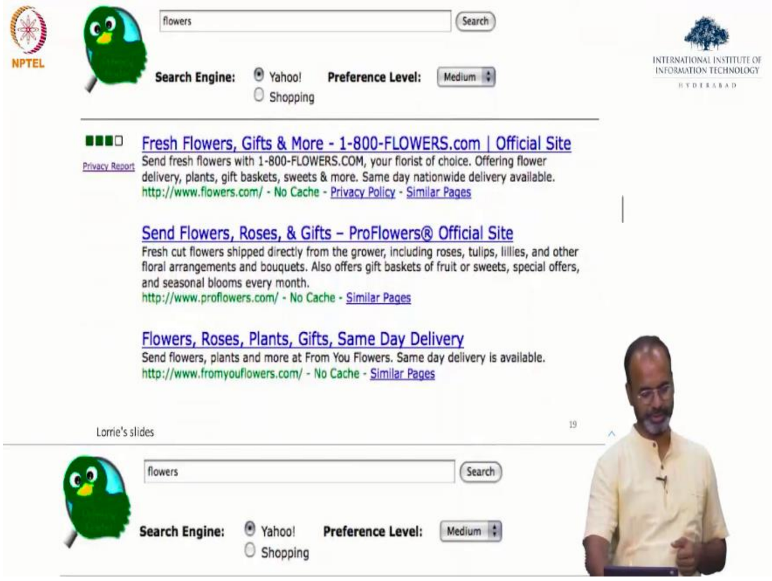
Search Engine: ● Yahoo! ○ Shopping Preference Level: Medium

Lorrie's slides

18

flowers Search

Search Engine: ● Yahoo! ○ Shopping Preference Level: Medium



flowers Search

Search Engine: ● Yahoo! ○ Shopping Preference Level: Medium

■■■□ Privacy Report

Fresh Flowers, Gifts & More - 1-800-FLOWERS.com | Official Site
Send fresh flowers with 1-800-FLOWERS.COM, your florist of choice. Offering flower delivery, plants, gift baskets, sweets & more. Same day nationwide delivery available.
http://www.flowers.com/ - No Cache - Privacy Policy - Similar Pages

Send Flowers, Roses, & Gifts – ProFlowers® Official Site
Fresh cut flowers shipped directly from the grower, including roses, tulips, lillies, and other floral arrangements and bouquets. Also offers gift baskets of fruit or sweets, special offers, and seasonal blooms every month.
http://www.proflowers.com/ - No Cache - Similar Pages

Flowers, Roses, Plants, Gifts, Same Day Delivery
Send flowers, plants and more at From You Flowers. Same day delivery is available.
http://www.fromyouflowers.com/ - No Cache - Similar Pages

Lorrie's slides

19

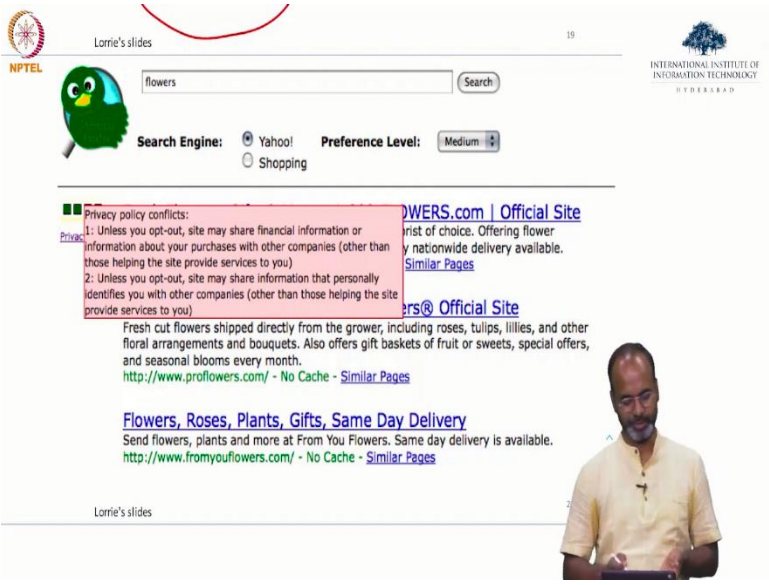
flowers Search

Search Engine: ● Yahoo! ○ Shopping Preference Level: Medium

So, that was one method. So, here is another technique that was built called privacy finder, which is based on search engine, where the weather input is search terms that people want is to search. And the output is same as a Google search or a Yahoo search or search output that you can see being search.

But in addition to the search results, it is annotated with the information of saying that, look, the privacy policies, comparison that we did, this is the output for that, same as input, flowers searching. In addition to the search output, it has this report of the privacy policy saying that look, there is three matching happening on the four, for the policy for this particular website, for this particular website.

(Refer Slide Time: 31:46)



Lorrie's slides

19

flowers

Search

Search Engine: ● Yahoo! ○ Shopping

Preference Level: Medium

Privacy policy conflicts:
1: Unless you opt-out, site may share financial information or information about your purchases with other companies (other than those helping the site provide services to you)
2: Unless you opt-out, site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

WERS.com | Official Site
rist of choice. Offering flower
y nationwide delivery available.
Similar Pages

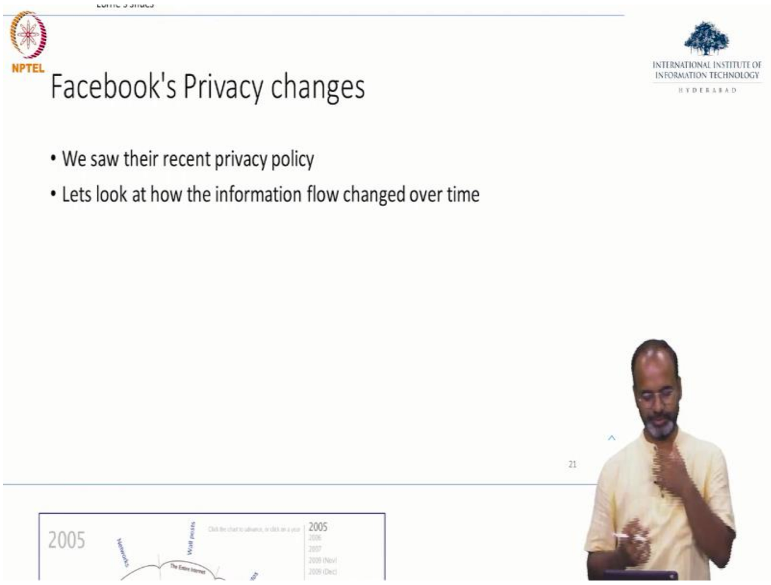
rs® Official Site
Fresh cut flowers shipped directly from the grower, including roses, tulips, lillies, and other floral arrangements and bouquets. Also offers gift baskets of fruit or sweets, special offers, and seasonal blooms every month.
http://www.proflowers.com/ - No Cache - Similar Pages

Flowers, Roses, Plants, Gifts, Same Day Delivery
Send flowers, plants and more at From You Flowers. Same day delivery is available.
http://www.fromyouflowers.com/ - No Cache - Similar Pages

Lorrie's slides

And, why it is 3, again, if you click on the report, it shows it is the same policy, so it is actually showing you the opt-out again, so that is about some funk technologies that are available to actually make privacy decisions better to provide enhancing experience for the user with respect to privacy.

(Refer Slide Time: 32:25)



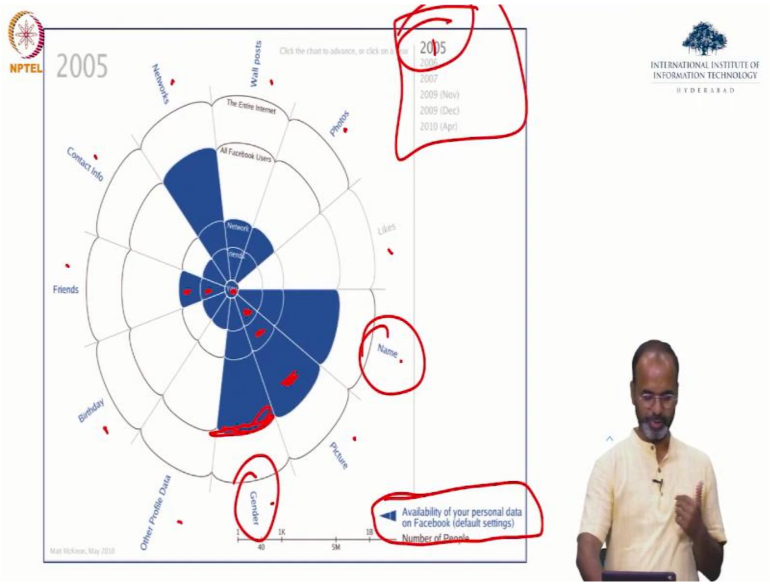
Facebook's Privacy changes

- We saw their recent privacy policy
- Lets look at how the information flow changed over time

21

Let us continue. Let us continue looking at social media go back to social media. But again, all of this is very connected. So, let us look at, we saw the recent privacy policy, we saw Facebook’s recent privacy policy in week 2, we went through in details about what the policies are all that. Now let us look at how information flow in Facebook has changed over a period of time. Over a period of time, unfortunately, this data is only till 2009 or 2010. But I am sure one can actually draw these kind of figures beyond that, also, to know what is going on.

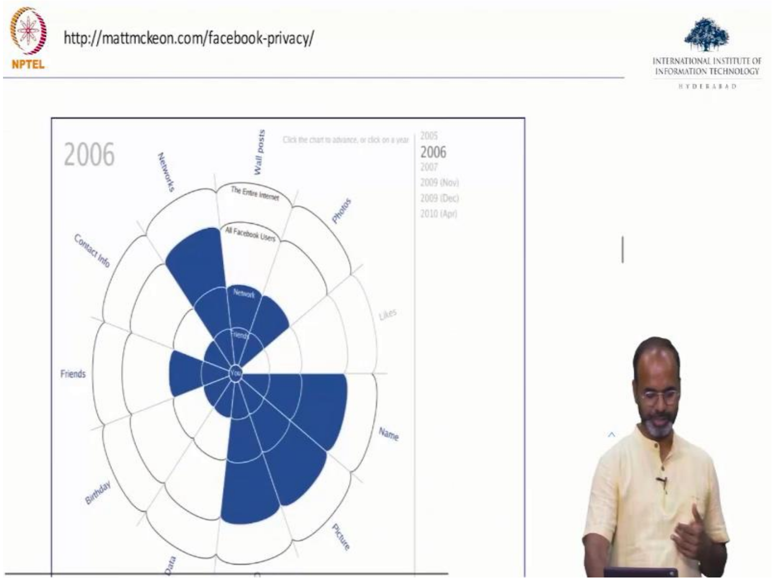
(Refer Slide Time: 33:07)



Lots of information is provided in this one graph, let me help you understand what is there. In 2005, so, this graph is for 2005, the way to read it is there is a set of time here. And there is there are different fields across here, which is name likes, photos, wall pose, networks, contact information, friends, birthday, other profile data gender and picture, picture is a profile picture. What does this mean, this is availability of personal data on Facebook, which is default settings how to read this, this means that my profile picture that is there in 2005 was available to me, was available to my friends was available to my network, all Facebook users.

That is how we should read it. Friends was available to me, was available to friends, and it was also available to the network. So, that gives you a sense of meaning you can go through each one of the information that is mentioned here, gender was available to everybody until here, it is available to all Facebook users, they could come to my profile and they could know my gender in 2005. Hopefully that is helping take a pause, stop the video, look at the graph if you want more closely.

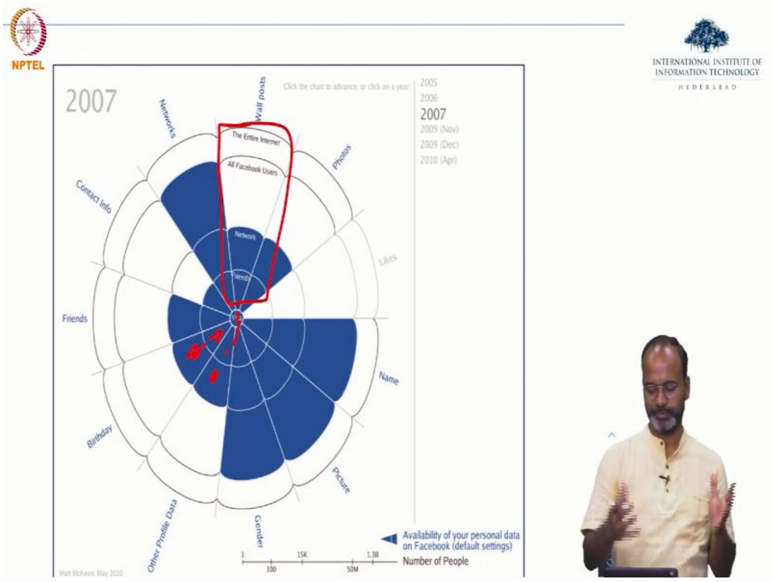
(Refer Slide Time: 34:54)



http://mattmckeon.com/facebook-privacy/

Now, if you go to the next year 2006. Slight changes happen if you look at changes, if you look at some of these changes that are happening in 2006 a little bit of changes are happening in terms of in terms of friends, in terms of photos, not much change all of them name picture and gender is available to everybody. And friends very similar, let us jump to 2007.

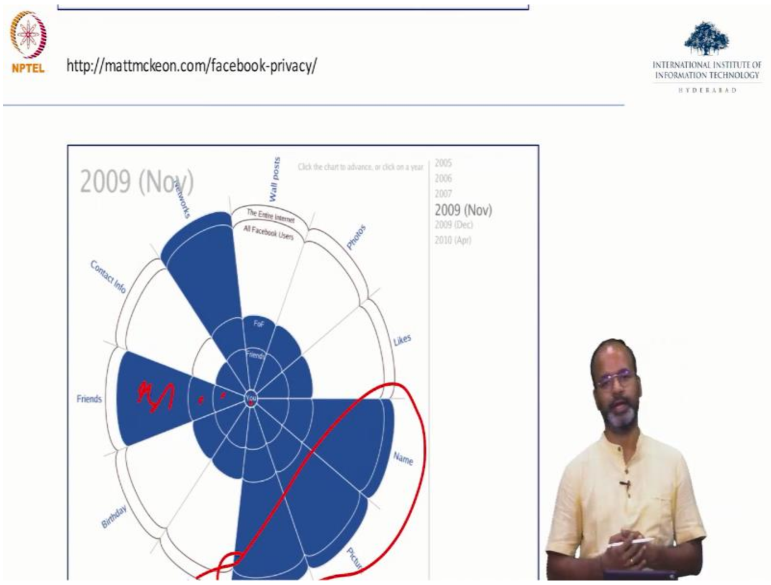
(Refer Slide Time: 35:25)



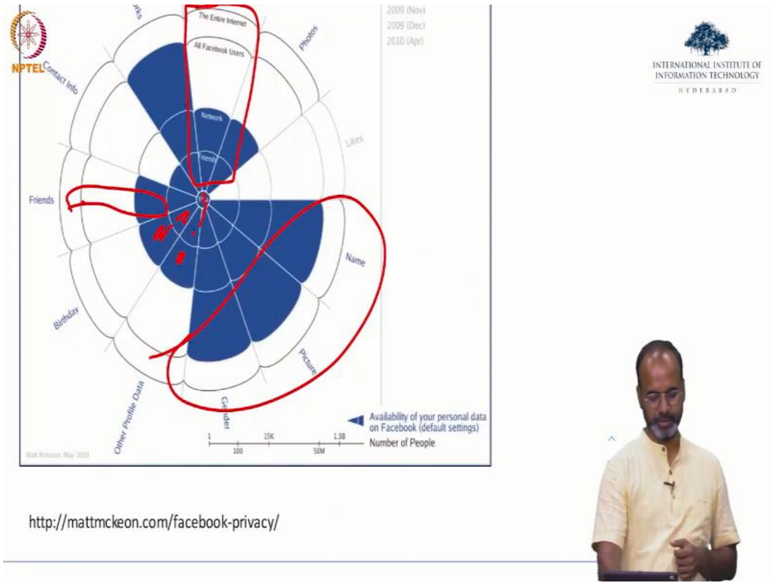
Just look at it in 2007, how things are changing. If just keep a watch on the spot. So, what does this mean? This means that birth date which was available only to me, birth date is here, which is available to me and my friends. Now birth date is available to me, my friends and all Facebook users also, same things other profile data also if you look at it other profile data here it was available to me and my friends only but it increases me, my friends and to all Facebook users to the network, sorry to the network.

Let us keep the discussion also focused on these things the categories of friends, you, friends, network, which is friends of friends, and all Facebook users. So, that would give you a sense of in 2005 the information started flowing more.

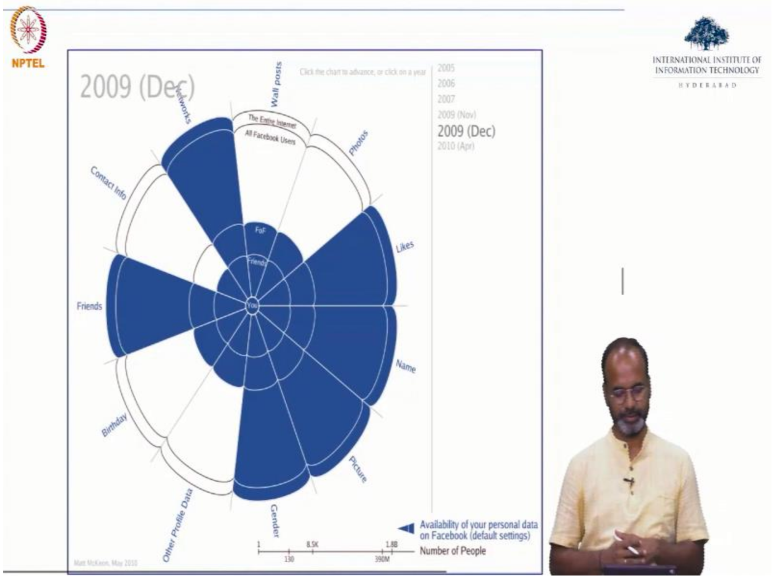
(Refer Slide Time: 36:39)



http://mattmckeon.com/facebook-privacy/



http://mattmckeon.com/facebook-privacy/

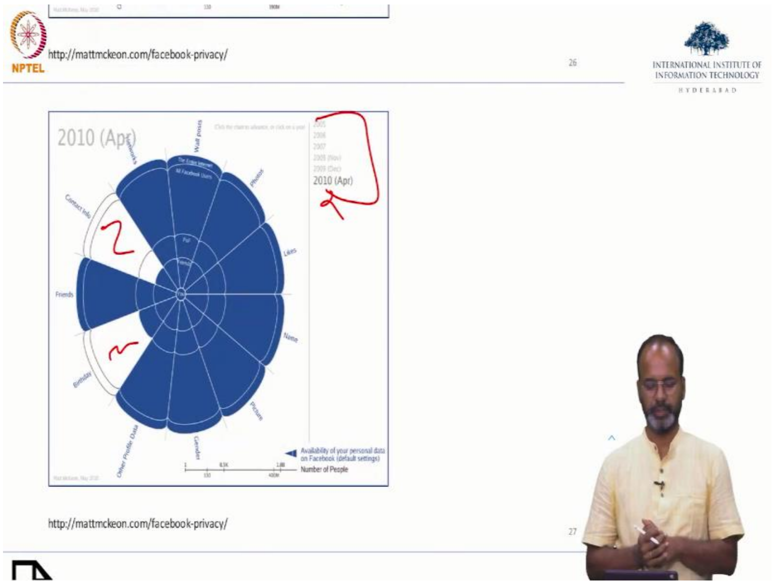


And now in 2009, the information is flowing much more if you just look at the profile picture just see this part, so this part is changed, which is your gender, picture and name from all Facebook users, it went to the entire internet, which is anybody on the internet can actually look for your gender when they come to your Facebook profile.

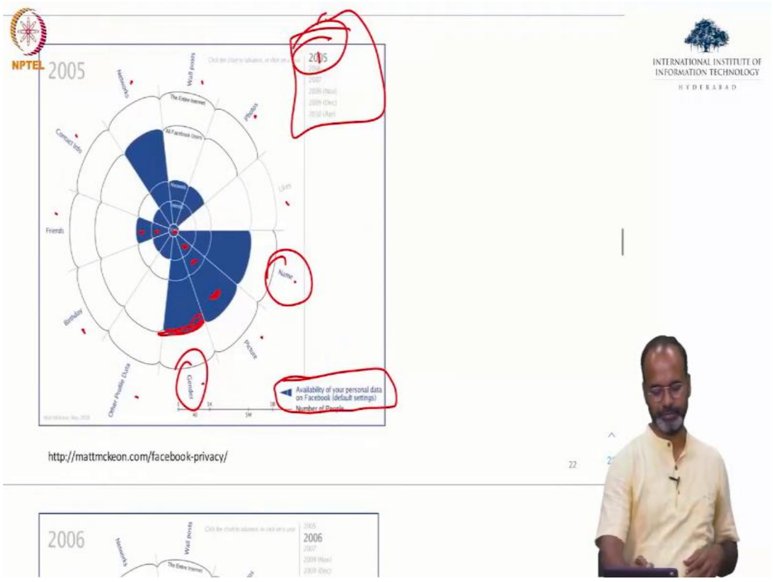
Similarly, if you see friends, this part also moved from you, friends, friends of friends to all Facebook users, any Facebook user could show up on your profile and see all your friends, as 2009. I let you to go through these even more carefully if you want pause and watch the pictures more closely to see any other differences.

But these are the differences that are very evident. 2009 December, the earlier one was 2009 November things are changing, things are becoming more and more. So, the basic idea.

(Refer Slide Time: 38:10)


http://mattmckeon.com/facebook-privacy/ 26

http://mattmckeon.com/facebook-privacy/ 27



http://mattmckeon.com/facebook-privacy/

Let see jump to even 2010. So, the idea here with this graph, I put the URL from where I took this images also here. If you look at the theme, what is the idea that is happening between 2000, from 2005 till 2010? Information is just flowing to larger set of people. Just look at it here only some set of, is white.

That is 2010 Compared to 2005. Lot more things are whiter here. So, given that information flow, and I think you I am sure you will also agree that 2010 is fine, but now I am pretty sure the graph if you draw it for 2020 it may be very different. I will let you think about it. Think about how to, how will the graph look. If you draw it for 2021 right now for these privacy preferences of Facebook default settings, just check your own Facebook and think of some ways you think you can draw this graph and send it. It will be an interesting exercise.

And keep in mind all the changes that has happened between 2010 and 2020, where the privacy discussion itself has influenced, must have influenced Facebook privacy settings also. So, that was knowing about Facebook privacy changes, how information has been flowing for many years between 2005 and 2010.