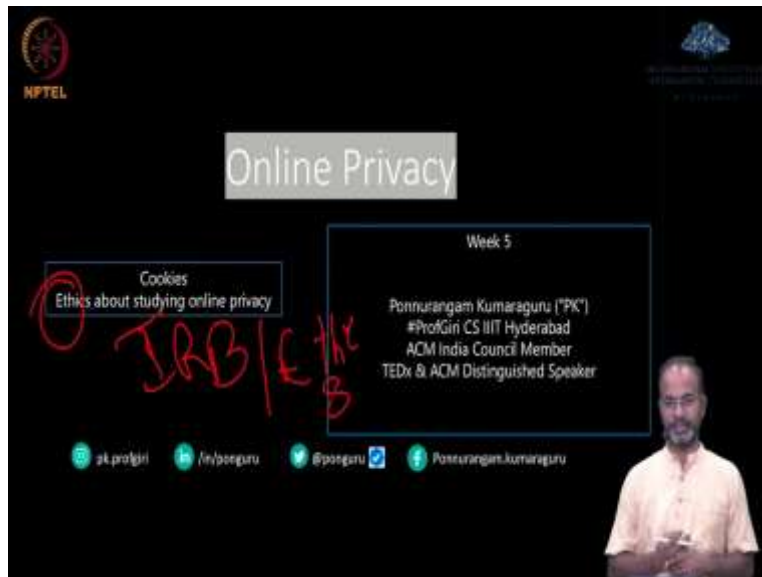


**Online Privacy**  
**Professor Ponnurangam Kumaraguru**  
**Indian Institute of Technology Hyderabad**  
**Week 5**  
**Cookies**

(Refer Slide Time: 00: 11)



Welcome back NPTEL students for week 5, this is course on Online Privacy. I hope you are enjoying the class, I hope you are enjoying the content that we are generating. I hope you are also making connections to the external world, other than just the content that you are seeing as part of the class. And it is good to see some action on the mailing list.

But as I always say, I think it will be nice to see more people join the discussion on mailing list, ask questions, answer questions, ask clarifications, find something somewhere else posted here, let us have a discussion around a topic or a news article or a hack that happened or a data breach that happened all of that, or your experience of going doing something and you saw that privacy is questioned there, all of that would be very, very nice to speak in the mailing list.

What we will cover actually, as part of the week 5 content is the cookies and ethics about studying online privacy. Cookies are an important component of sort of say tracking users, and how companies are getting to know about our behaviour, using that for advertisements, all of that. So, we will look at what is cookies, how to set cookies, how to retrieve information from cookies, where do cookies store in our browser and how to actually delete the cookies.

What are the pieces of information that cookie actually keeps, how probably those can be used for tracking us and all of that. And the second part of week 5 we will do is about this very important and critical, actually, as now, it is about the question of ethics. Ethics about studying online privacy, meaning where do you draw the line, meaning you want to collect as much information as possible or company wants to collect as much information as possible, that is one type.

But if you are doing research, if you are collecting data from users, where do you draw the line? How do you set up the study? What study should you set up? What data you can collect? What is IRB institutional review board or ethics committee? What approvals do you need? And why do you need this approval? What are the problems that has happened in the past which is made this approval necessary all of that we will actually look at as part of week 5. Week 5 seems to be pretty exciting. Let us, see how it goes.

(Refer Slide Time: 02:59)



What we saw in week 4, we saw identity resolution and privacy not just I hope you tried out some experiments with your own data, in terms of your own accounts, I hope you also tried out looked at started looking at the nudges that you are seeing on your online behaviour and connecting it to something that we saw in the class.

(Refer Slide Time: 03:22)



The slide features the NPTEL logo on the top left and the Activi logo (International Institute of Information Technology) on the top right. The main content is a list of instructions for an activity:

- Find instances of regrettable disclosures
- If you were to think about more ways to nudge users about privacy, what / how would it be?
- Submit
  - Instances of regrettable disclosures
  - Nudge ideas

A small video inset on the right shows a man in a light-colored shirt speaking.

I asked you to do an activity as part of week 4. Look at regrettable disclosures information that we have and instances of regrettable disclosures that we have seen or others in the new status come and actually the nudge ideas also, which is what are the better ways to create these nudges. How all would you create if the nudge, if you were the one who is designing these nudges.

(Refer Slide Time: 03:56)



The slide features the NPTEL logo on the top left and the Activi logo on the top right. The main content is a question:

How are online privacy concerns different from offline privacy concerns?

The word "Physical" is written in red cursive handwriting on the left side of the slide. A small video inset on the right shows the same man from the previous slide speaking.




Now, let us take a look at cookies. Let us, get into the topic of cookies. How are online privacy different from offline privacy concerns? If you just think about it, the question of offline privacy

is mostly about physical your physical being your surrounding information there are people around you looking at you the dress that you wear, all that is probably the offline world and the discussions that we have talked about also the conversation the train that you are having somebody is actually asking you about your salary.

Somebody is hearing the conversation that you are having in your neighbours in the train. Person sitting next to you is actually hearing the conversation that is going on all of that is probably the physical concerns. The online concerns are the online behaviour, social media, websites, all of that. What are the differences if you think about it? The one of the critical difference is that information, the behaviour that you have in the online world can be kept stored, looked at again, and decision could be made.


Offline world, you had the conversation with somebody on the train. Meaning I think the chances of that information being get recorded and somebody going and looking at it later. It is all very minimal. So, that is the most important critical difference between the online privacy and the offline privacy, which is the information that is information data about us that is getting collected is stored, analysed, processed, inferences are drawn from that, and that is actually used for making decisions. Keep that in mind that is one of the thing that we will keep looking at in week 4 and future also.

(Refer Slide Time: 05:58)



## Cookies

- What are cookies?
- What are people concerned about cookies?
- What useful purposes do cookies serve?



What are cookies? Cookies are definitely not the ones that you eat. These cookies are about the online cookies. What are people concerned about cookies? So, what I would like to see as your responses, pause the video now, send the mailing, send a response in the mailing list, which is what are cookies? What are people? Why what are you concerned about cookies? What is the concern about cookies? What purpose does cookies really have?

Why did they come up with this idea called cookies? And why cookies have become so prevalent? If you think about the websites that you are accessing, now, even the last week or so the online websites that you would have accessed, it will actually asked you for settings, saying allow cookies, reset cookies, change the settings for the cookies, all of that.

Because these are all because of many new regulations and requirements on these companies. Everybody is making sure that the user's consent is taken in terms of cookies, I am sure if you looking at any of the European websites, because of GDPR, this is become a mandatory while they actually get access to your they get concerned from you about the cookies that they are setting on your machine.

Similarly, in the US also. So, pause, send a response on the mailing list. Let us, see what you have. I am asking you to do all this, I hope you are actually doing it as I ask because the answers are in the next slide. If you just go forward in the video and then answer it, look at it and then send it is of no meaning. I think the idea is to make you think, and the idea is to make you think before I give you the answers.

(Refer Slide Time: 07:54)

The slide features the NPTEL logo on the left and the IIT Bombay logo on the right. A small image of a cookie is positioned above the text. The text is organized into bullet points. A red circle is drawn around the section 'Cookies can do unexpected things'.

- Cookies can be useful
  - Used like a staple to attach multiple parts of a form together (User preferences)
  - Used to identify you when you return to a web site so you don't have to remember a password (Authentication)
  - Used to help web sites understand how people use them (User tracking / Personalization)
- Cookies can do unexpected things
  - Used to profile users and track their activities, especially across web sites
- Cookies are only data
- Cookies have expiration date

Cookie can be actually extremely useful in many different ways. So, I think I said, I have cookies, I mean, I will show you some of the cookies that I have it is in my machine that I can actually show you later. How these cookies are extremely useful in terms of our own user behaviour.

Cookies, meaning generally the idea is like a staple that you attached, meaning you take multiple forms, that you are filling, multiple documents that you printed out, put them all together, staple it, that is very real world in the offline definition of what a cookie could be, and why that is interesting, or why that is that is because of user preferences.

A user preferences are like that, all the that pages that you have gone, if I just have to staple it together and say that, this is PK PK is online behaviour, that is cookie. That is capturing my user behaviour, used to identify you, when you return to a website. This is also very, very important purpose of a cookie, which is that I go to a website multiple times, let us take Amazon dot com I do not want to be actually giving my username, password giving my preference all of that again, and again.

The searches that I have done it just helps my user behaviour that is all. So, user behaviour is one and the other one is also authentication I mean, I think if it keeps my I am sure many of you have

set your Google login, the browser saves your username and password, and it is actually giving you quick access to your emails.

So, that is authentication, used to help websites understand how people use them, which is the Amazon search result that I set, recommendations set it is provided, all of that information can be actually captured in a cookie. And that information can be used to help provide recommendation for us, which is more like user tracking or personalization.

So, therefore, the usefulness of cookies are user preferences, authentication, and personalization and of course, in terms tracking. Cookies can do unexpected things, which is that they can be used to track which is an advantage here listed here, it can actually become a disadvantage also. So, that they know which books have you searched on Amazon, they can use it and then they can probably give that information to a third party or two, three different services such recommendations are put together and a third party company can actually profile you and present a promoted ad, which is very relevant to the book that you search recently.

So, that is the sort of negative aspect of cooking. Cookies are only data, which is set it to only stores the search terms that you are used, the recommendations that were provided to you all of these that are provided that your user behaviour is getting tracked into the stored in a cookie. All cookies have an expiration date. So, I will actually show you later what the expiration date is, how to set it all that. I hope that helps you to get a sense of what a cookie is.

(Refer Slide Time: 11:45)

The slide features the NPTEL logo on the left and the IIT Bombay logo on the right. The title "Setting & Retrieving Cookies" is centered. Below the title, there are two bullet points: "Client Side (JavaScript)" and "Server side (PHP)". Under "Client Side (JavaScript)", the text "document.cookie" is circled in red. Under "Server side (PHP)", there are two lines of text: "Set cookie by server to the browser for new sites" and "\$\_COOKIE by server to the browser for coming-back sites". Both lines are circled in red. A small video inset of a man in a light-colored shirt is visible in the bottom right corner of the slide area.

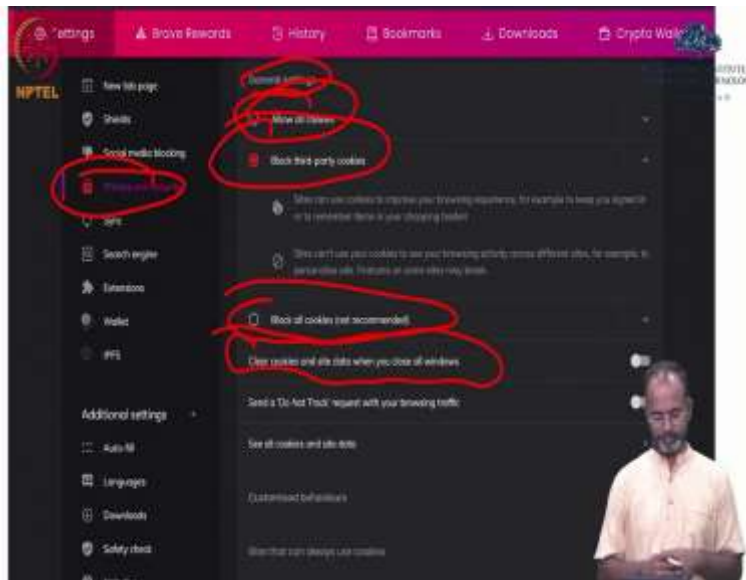
So, here is how you set the cookie. So, which is so and again, cookie setting and all of this can be done in many different ways. I am showing you JavaScript, I am assuming that some of you know already Java scope, if not the thing that you need to know about cookie is very limited. So, I will show you only that. You can also do this in PHP and other programming languages also.

Setting the cookies, which is document dot cookie in JavaScript, set cookie would be by the server to a browser on new websites, if the website is already, for example, I go to Amazon dot com and I access Amazon dot com tomorrow, the cookie will not be set cookie, it will be actually dollar cookie.

Which is to say that look, I already this, this browser is already seen Amazon dot com and therefore I do not have to set the cookie, I am just going to only use the cookie that is already there, which is dollar cookie. So, that is the new website that is coming back sites.



(Refer Slide Time: 13:01)



So, let me show you some examples of how cookie settings are in our browser. So, this is from my Brave settings. I will show you also Chrome I am assuming most of you are using Chrome but if you are using Brave this is how it will look. So, this is a Brave preferences a Brave settings and privacy and security.

So, it talks about allow, so what are the settings that we have? What are the things that we can actually control in terms of cookies? You can do allow all cookies. You can do block third party cookies, which is what I have set up, which states that site can use cookies to improve your browsing experiences.

For example, to keep you signed in or to remember in terms of your shopping basket, which is what I actually showed you in the slide, sites cannot use your cookies to use your browsing activity across different sites for example, to personalise ad's features and some sites may break. So, that helps to that is the blocking third party cookies which is the cookies that are set by third parties for tracking across the domains is what is actually blocked.

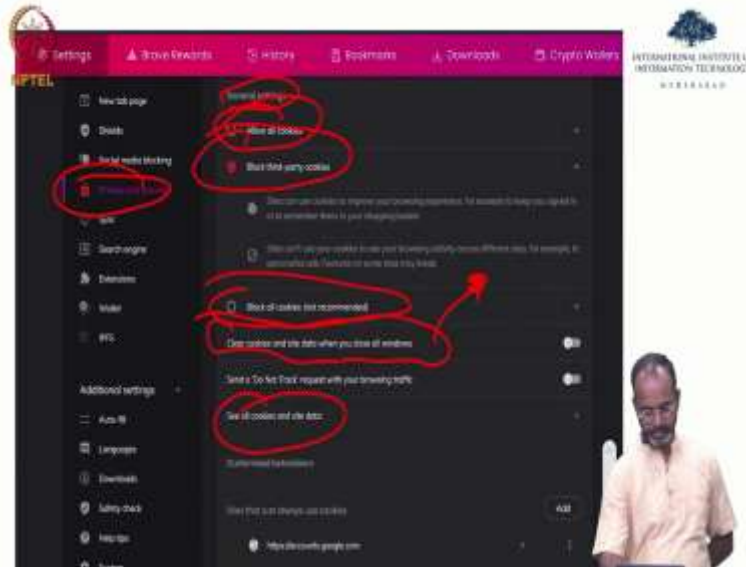
So, the other option that we have is block all cookies, which is just I do not need cookies at all every time I will do actually all the username, password myself recommendations everything I will search every time that I need. Clear cookies and site data when you close all windows, which is this is also another one another interesting feature that you can use is every time you

close the window the cookies for that particular domain, that particular sessions are actually deleted sender do not track request with your browsing traffic. So, this is also an information which you can actually set up where every request that your making this a do not track request that goes up and that actually is used to make some choices. So, I will actually show you this option more detail see all cookies and site data in a second.

Customise so you can actually see. So, you can control what cookies are doing. You can control you can control the cookies that are coming in, you can control actually what meaning to allow third party cookie or not, you can allow you can control whether they are third party cookies are tracking and then those things you can actually control. I hope that helps. I am assuming that you can parallelly you can go look at your own browser now and see how the settings in your browser are.

(Refer Slide Time: 16:15)





So, this is about clear browsing data, which is if so, again, the settings are so this is same, this would be the same. So, from the cookies, you can actually delete right clear. So, this option if you click you will reach here. I wanted to show how what are the options in terms of getting rid of all these cookies.

So, basic advanced on exit are the three options that are available, again, you talks about browsing history, you have an option cookies and other sites and cached images and files. So, this you can actually get rid of which is saying that look, the data that in the last so if you click on this drop down, also you will get last hour I think last 24 hours last week or three four options are there which you can actually delete the data for.

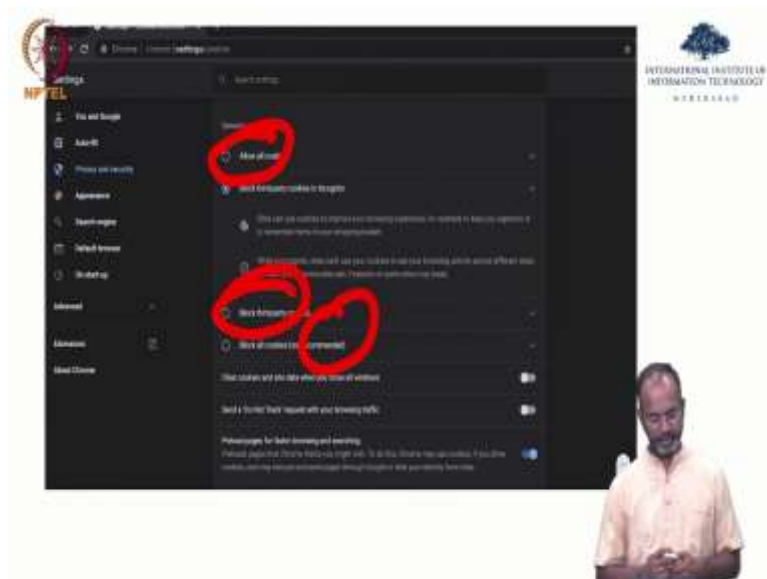
Advanced if you do the same, the same, so from the system basic one that shown if you do advance, you will come to this screen, which again shows you more detail meaning this advanced is nothing but just having the same information. But it is actually more giving you a detail saying, there are 22 sites that you are actually deleting cached images, same as 48 MB that it is showing here and other details also show. You can actually check, uncheck some of these, and then do the clear here.

(Refer Slide Time: 17:57)



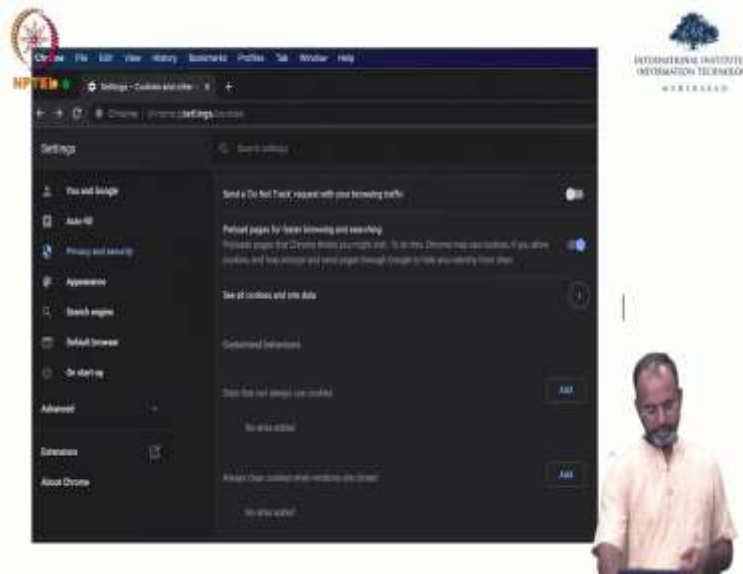
On exit again so this is the this is something that I have not set up. So, I am sure if you are more sort to say privacy aware and want to be more critical about the information that you are sharing with these companies. I am sure you can do this on exit thing. Same options, on exit meaning getting out of the tab, getting out of the browser, all of your cookies are gone. So, that is how you can actually clear the browsing data, which is basic advanced and on exit. So, this is on Brave.

(Refer Slide Time: 18:39)



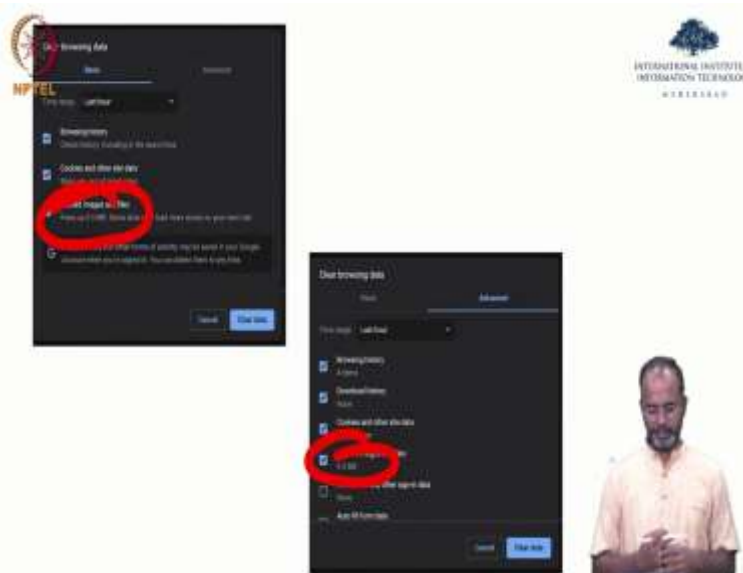
If you just do the same thing on Chrome, I mean even I was looking at it, it almost looks the same. So, same options allow cookies, blocked allow cookies, blocked third parties and allow cookies, blocked third parties block all cookies. So, the settings look very, very similar, both on Chrome and in Brave.

(Refer Slide Time: 19:10)



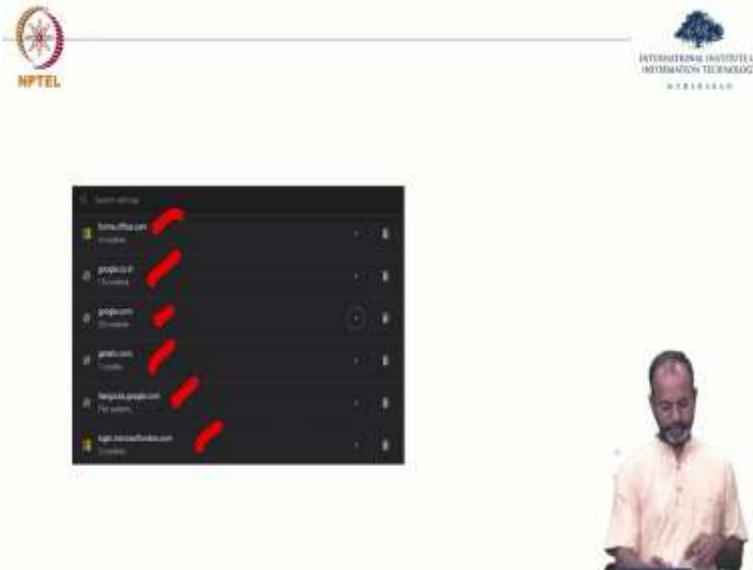
So this is again, Chrome.

(Refer Slide Time: 19:16)



Very much very similar, so you can see my particularly my behaviour of CC, I am not a very Chrome user. So, it says 9.3 percent Brave it was I think about 40 MB. So, same options, browsing history, download history, all of that. So very, very similar I am sure if you do it for Firefox, Safari, all of the browsers must be very similar.

(Refer Slide Time: 19:42)



Please do it on the browser that you use and if there is anything that you want clarification on if anything that is looking different from what I have shown you here please bring it out we can actually talk about it. So, next one I wanted to show you is a cookie itself. So, we are talking about cookies.

So, now we know what is cookies and why it is necessary and what it can do.. Now, let us look at your own browser, you can go look at all the cookies that are in the browser, I am going to show you what cookies are in my machine. So, I did this just a few minutes before when I was preparing for this lecture. So, if you look at the cookies set on my machine, some of them there are many of them in my browser. But this one is about office, Google, Google, I think this is also Google, Hangouts and Microsoft. Alright, so these are the cookies, some cookies.

(Refer Slide Time: 20:47)

The image displays two sequential screenshots from a presentation. The top screenshot shows a mobile browser's cookie list with 'google.com' circled in red. The bottom screenshot shows a detailed view of a 'google.com' cookie, also circled in red, with a red arrow pointing to it from above. The background of the slides includes the NPTEL logo and the text 'INTERNATIONAL INSTITUTE FOR INFORMATION TECHNOLOGY'.

I am just going to go into one of the I am going to go into just this Google cookie, it is a Google dot com cookie. So, I am going to show you cookies. So, what the idea is, what I am trying to do is here, which is 20. So, if you look at it, the 20 what is listed here. All the 20 cookies are listed here.

(Refer Slide Time: 21:15)



We will get into one of them SID, please go do this yourself. So, for you to get a sense of what cookies are again, by doing this, you will learn how it is in your own machine at the end of day. So, here it is actually showing you some details about the cookie, IJ, IP underscore J or name. So, it this is basically an advertisement cookie that is set by Google.

So, that is the ads path, you will also see this path later in the code that we will write to actually to set the cookie in few seconds. So, and then it has this created date and expiry date, which is also you remember, I said one of the things that happens in the cookies is, all cookies have some expiration date.

The cookies get created now and the cookie the server, which is setting the cookies can decide when it has to expire. Otherwise, you can actually do it, the set through the settings that I said on exit or deleted physical yourself. So, even though there is a user interface that I am showing all of this could be done in a programme, I am going to show you how you can do all of this in JavaScript right now.



(Refer Slide Time: 22:30)

**Cookies in JavaScript: setting**

`Document.cookie = cookiestring;`

Cookie string has 3 semicolon separated parts

- 1 name / value pair: `"lastBookSeen=Permanent Record"`
- 2 expiration date: `"expires = Fri, 22 Oct, 2021 12:00:00 UTC"`

Not static, creates a Session Cookie, which will expire when user closes the browser or clears cookies

- 3 path where cookie belongs: `"path=/"` default current webpage

Cookie name: `"lastBookSeen"` already exist, will be overwritten

<https://courses.cs.washington.edu/courses/cs154/18sp/data/lectures/lec26-cookie/>

So, that is the how to set a cookie using JavaScript. You remember I already said you document dot cookie, which is cookie string. So, essentially, the three parts of this first this is setting the cookie itself, which is to have set the cookie. Earlier I showed you set cookie document dot cookie, all of that. Cookie string has three semicolon. So, essentially you will have 1, 2, 3 parts. Next slide I will show you an example with just the code.

What are the things that you can set? The first you are saying is that what is the name of the cookie. So, I have set it up here as the name of the cookie to be lastBookSeen, lastBookSeen is the cookie that I am the server is going to actually put it in your machine. And what is the expiration date expiration date, I have set it up as Friday 22nd October 2021 and 12 UTC. UTC is just the time zone you can set, commonly use time zone as UTC.

So, I have just put UTC there. There not static cookies so not static, you can of course change these expiration dates, creates a session cookie, which will expire when users closes the browser or clears cookies again. Session cookie is created, what is the session? Session is basically an interaction between the server and the client.

And that session cookie, which is for the cookies that are set a session is created and the session cookie expires in the time that is set in the cookie, which is the expiration date. Path where cookie belongs. So, this is the path if you look at so all the cookies that I went and showed you

from Chrome, those are the cookies from my browser. Those are the cookies that are set in the browser itself.

So, if you are a Mac user, you should be able to go to application support, Chrome or Brave and then cookies you should be able to see all of that. So, that is why I picked up all of all of these cookies. Cookie name lastBookSeen already exists will be overwritten. So, if all of this lastBookSeen cookies already there, it will actually be overwritten.

So, that is how you set a cookie using JavaScript. So, essentially, you have to name the cookie, you have to set the cookie and you have to put with the name, give the expiration date and where the cookie has to be stored. If you do that a cookie would be set, cookie is generally set by a server on your client on the browser.

(Refer Slide Time: 25:34)

The slide displays the following JavaScript code for setting a cookie:

```
document.cookie = "lastBookSeen=Permanent Record; " +  
"expires= Fri, 22 Oct, 2021 12:00:00 UTC; " +  
"path=/";
```

The slide includes the NPTEL logo on the left and the International Institute of Information Technology logo on the right. A presenter is visible in the bottom right corner of the slide.

Here is a example of a cookie lastBookSeen permanent record that is the book that I am reading right now. So, expires February 22 October sorry Friday October 22 2021 on 12 UTC and path where it should be set. So, that is how it is done in JavaScript.

(Refer Slide Time: 25:57)

The slide is titled "Retrieving Cookies" and features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. The main content includes the following text and code:

```
let cookies = document.cookie;
```

Will return all name value pairs as in previous slide

Parse it and get information that is needed

```
document.cookie = "lastBookSeen=Permanent Record; "+  
"expires= Fri, 22 Oct, 2021 12:00:00 UTC; "+  
"path=/";
```

Handwritten annotations in red ink include:

- A red circle around the code `let cookies = document.cookie;` with an arrow pointing to the text "Will return all name value pairs as in previous slide".
- A red circle around the code `document.cookie = "lastBookSeen=Permanent Record; "+ "expires= Fri, 22 Oct, 2021 12:00:00 UTC; "+ "path=/";`.
- Two diagrams below the code:   
1. "Amazon" with a circled "1" below it, an arrow pointing to a box labeled "PK".   
2. "PK" with a circled "2" below it, an arrow pointing to "Amazon".

A presenter is visible in the bottom right corner of the slide.

So, what do you do when you want to retrieve a cookie? For example, I am, using my Brave browser. Amazon has already set a cookie on my machine, I am going to Amazon dot com again, Amazon needs to look at the cookie that I already have in my browser. Because that is what will help them to know who I am, what I have searched in the past and can they actually use that to make any choices after that.

So, `let cookies` is equal to `document.cookie` that is how retrieving can be done, so this particular command will retrieve will return all name value pairs in the previous slide. Essentially, if you do `let cookies` is equal to `document.cookie` (26:42), `document.cookie`. So, it will pick up all the three things that we set in the last slide, which is the cookie name, last book seen, permanent record expiration date and the path.

And so once you have this that is what you will get when you when so Amazon so this is PK that is Amazon Amazon send request, Amazon has already put the cookie in the first session. Let us, take this session number 1 session number 2, PK Amazon PK sending the cookie details to Amazon Amazon is looking at it, he is already the last book that is seen as permanent record. Now, let us actually present to him 1984 book as a recommendation.

These are all privacy related books, I am show you you may be interested in some of these books also. So, that is what cookie helps for. So, now that I can parse this cookie and make a choice

quickly about what books to recommend to PK and all. So, that is about cookies, which is to what it be see in cookies, we saw, what is a cookie? Goods and bad's of cookies, how to set a cookie, how to retrieve a cookie and what what processing can be done and what choices can be made because of cookies there.

(Refer Slide Time: 28:22)

**Web bugs**

- Invisible "images" (1-by-1 pixel, transparent) embedded in web pages and cause referer info and cookies to be transferred
- Also called web beacons, clear gifs, tracker gifs, etc.
- Work just like banner ads from ad networks, but you can't see them unless you look at the code behind a web page
- Also embedded in HTML formatted email messages, MS Word documents, etc.
- For software to detect web bugs see: <http://www.bugnois.org>

*iit.ac.in*

Again, please feel free to look at cookies more look at these slides. And if you have any questions, feel free to ask in the mailing list, I will be happy to take it. And as I promised earlier all these slides, I am also making the annotation slides I am also making it on the website. So, feel free to take it from there also.

So, here is another one, this is also an interesting one, this website was not working. But I put it I still put it here just for you to show that how these things work. So, this is another way that tracking can be done, cookies is (( ))(28:59), cookies is a server putting some information and then server is actually looking at it, what information is there.

But web bugs has been an interesting way to actually also track users. It is a simple one by one pixel transparent image, which is when we go to a website that website can actually have this for example if you go to triple IT dot ac dot in. Let us, take that homepage has those one by one pixel that one by one pixel what is it happening for the web page to be served on my browser that one by one pixel has to be actually (( ))(29:41).

So, in that request, iit dot ac dot in is tracking that look that image was requested by PK and therefore PK is actually looking at this website. What is interesting is that now a third party can actually put that. So, if you assume that iit dot ac dot in is put that image on my browser, that is okay because iit otherwise also serving me the webpage.

But if I let us take if iit works with a third party and who can actually give sense of others who are actually accessing iit dot ac dot in. People who are from other domains or in other places people are actually looking at iit dot ac dot in not just the domain information about iit. Wherever it is presented with this one by one pixel is press put in the webpage.

The third party can actually look at PK looking at iit dot ac dot in is there, PK also looked at let us take a website education review dot com on something in that there is a iit review and that page also had the same one by one pixel of iit. Now, it is clear that PK is the one who is requesting these two pixels from the same browsers from the same IP.

So, you can actually say that PK is the one who saw this review and PK is one who is also looking at iit dot ac dot in. So, that is what bug does. Just to again, to summarize it is helping you helping a third body, helping an organization to track users, very similar to cookies, but it just, this is just one by one pixel, also called as web beacons, clear chips work just like banner ads from ad networks, ad networks are placed it here is because of the third-party example that I gave you.

And the bugnosis dot org is used to be a website, which helps you to see if your website the website that you are accessing actually has bug in it. Whenever you do website or input, the website that you wanted to see whether there is a bug, it will actually show you this bug on all the places that they have placed the one by one pixel. Just to help you to see which websites have this box.

(Refer Slide Time: 32:26)

The slide features the NPTEL logo on the left and the IIT Bombay logo on the right. The word "Activity" is centered at the top. Below it, a list of tasks is presented with red handwritten annotations: "Find cookies in your machine / laptop" has a red bracket above it; "Go through all the cookies, details" has a red bracket above it; "Share it on the mailing list" has a red checkmark to its right; "Total # of cookies on your machine / laptop?" has a red checkmark to its right; and "Any interesting cookies / name + value pair that you found?" has a red checkmark to its right. A presenter is visible in the bottom right corner of the slide.

Simple technique, but very, very efficient way of actually tracking users across. One pixel, third-party pixel kept and that pixel is placed in different websites web pages and whenever somebody is making a request for that let us take a unique pixel that is kept for iit dot ac dot in you can actually track all these users profile, all these users.

So, what I want to do now, what I want you to do now is to actually do look at your cookies in your machine I showed you how to go look at in your browser. Take a look at the cookies. Go through all the cookies details say for example the like the one that I showed you Google 20 cookies, expiration date, when it was created all of that. What I would like you to share in the mailing list is total number of cookies on your laptop or a machine, total number of cookies.

So, if you just saw a few of mine probably there like 27, 28, I would like to know how many cookies are there in browser. And any interesting cookie names value pair that you find, value pair again so you looking at the name of the cookie, the expiration date and the path, that is kept, look at the name value pair and see whether there is like the lastBookSeen are you finding anything, interesting. I will wait for seeing your response on the mailing list.