u3a Computing Group

Alan Hopwood, 4 May 2023

Presentation
Cookies

Worst Nightmare
or
Supportive Tech

Presentation Agenda

Cookies

- What are Cookies?
- Why are the various types of Cookies for?
- How do Cookies work?
- How are 3rd Party or Tracking Cookies used?
- How do various Browsers handle Cookies
- How you can block 3rd Party Cookies

What are Cookies?

http Cookies

(also called web cookies, Internet cookies, browser cookies, or simply cookies)

- Cookies were invented to support the interaction between web browsers and Websites. They allow the website to remember you, your website logins, shopping carts, personalisation choices.
- Cookies are small packets of information sent between an internet server and your web browser
  - Internet Servers - e.g. amazon.co.uk, lloydsbank.com, dorchesteru3a.org.uk
  - Web browsers: Google Chrome, Internet Explorer, Edge, Safari, Firefox…
- There are 3 main flavours of Cookie: 1st party (Session & Persistent), and 3rd party.

What are Cookies for?

http Cookies

<u>Session</u> Cookies support Session Management:

- “Tag” the user’s online activities
- Set up a unique session identifier so that the website can for e.g. keep track of shopping items viewed, selected for buying - can go to check-out at any point.
- The session identifier is sent from browser to server with every request made.
- Expire as soon as the user closes out of webpage
- Without the session cookies, each new webpage wouldn’t take any account of what the user had already done.

What are Cookies for?

http Cookies

<u>Persistent</u> 1st party Cookies support Personalisation:

- Track online preferences
- Can store login information, language selections, menu preferences, internal bookmarks, names, addresses, and payment card numbers. etc. so that these are retained for the next time the user logs in to the website.
- Information is retained on user's computer until the cookie expiration date - typically for up to a year.
- A 1st party cookie is only accessible from the domain that created it.

What are Cookies for?

http Cookies

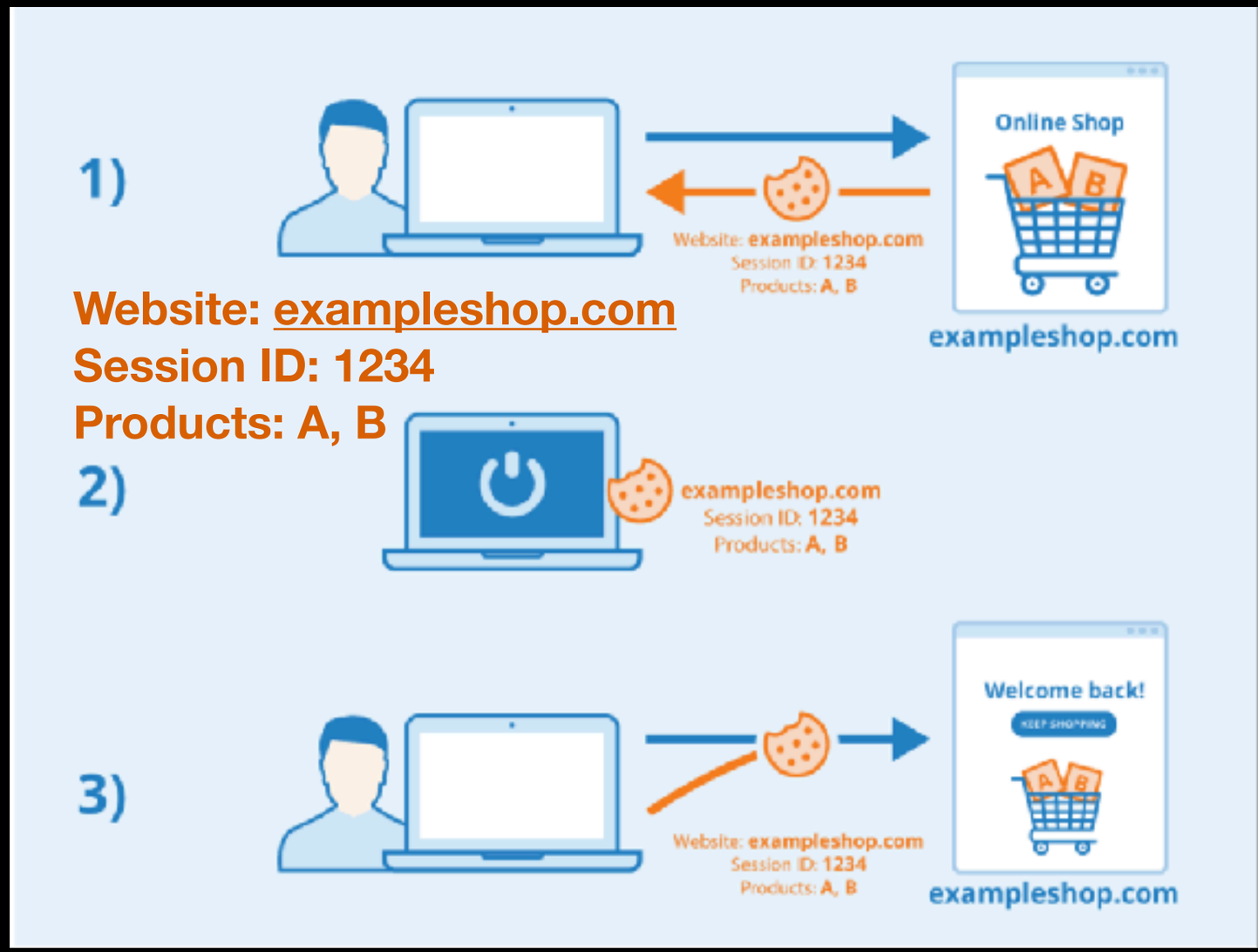
Third-Party or Tracking Cookies keep track of users across websites:

- Collect data based on a user's online behaviour
- When user visits a website, third-party cookies collect various types of data that are then passed on or sold to advertisers by the website
- They track interests, location, age, and search trends, can provide custom advertisements when user goes on to a different website

How to Cookies Work?

http Cookies

- http defines the message structure used on the internet
- Cookies are sent in the http header
- Each Cookie is sent in “value pairs” e.g. id=xyz99
- Actually:
  - Header
  - Value pair
  - Attributes
- The browser stores Cookies on user’s computer



How do Cookies Work?

http Cookies

Messages Structure

Headers:

- Set-Cookie: from Server to User Agent
- Cookie: from User to Server

Valued Pair:

- Can be anything - only needs to be meaningful to the server/website. All the browser does is send the pair back as defined by attributes

Attributes: (standard meaning so that browsers can respond appropriately)

- Expires: date and time that cookie expires
- Max-Age: lifetime of cookie in seconds
- Domain: hosts to which user will send the cookie e.g. example.com
- Path: scope of cookie limited to path within host
- Secure: limits sending of cookie to “secure” channel

Browsers should accommodate:

- At least 4096 bytes per cookie
- At least 50 cookies per domain.
- At least 3000 cookies total.

To summarise

http Cookies

- Websites are allowed to leave a “message” on your browser.
- Your browser sends that message back only to that website (or really to that internet domain) with every request.
- The Cookie does nothing on your browser or computer. It is just stored.

So how do those adds follow you around different websites?

And why are we continually asked to accept cookies?

Third Party Cookies

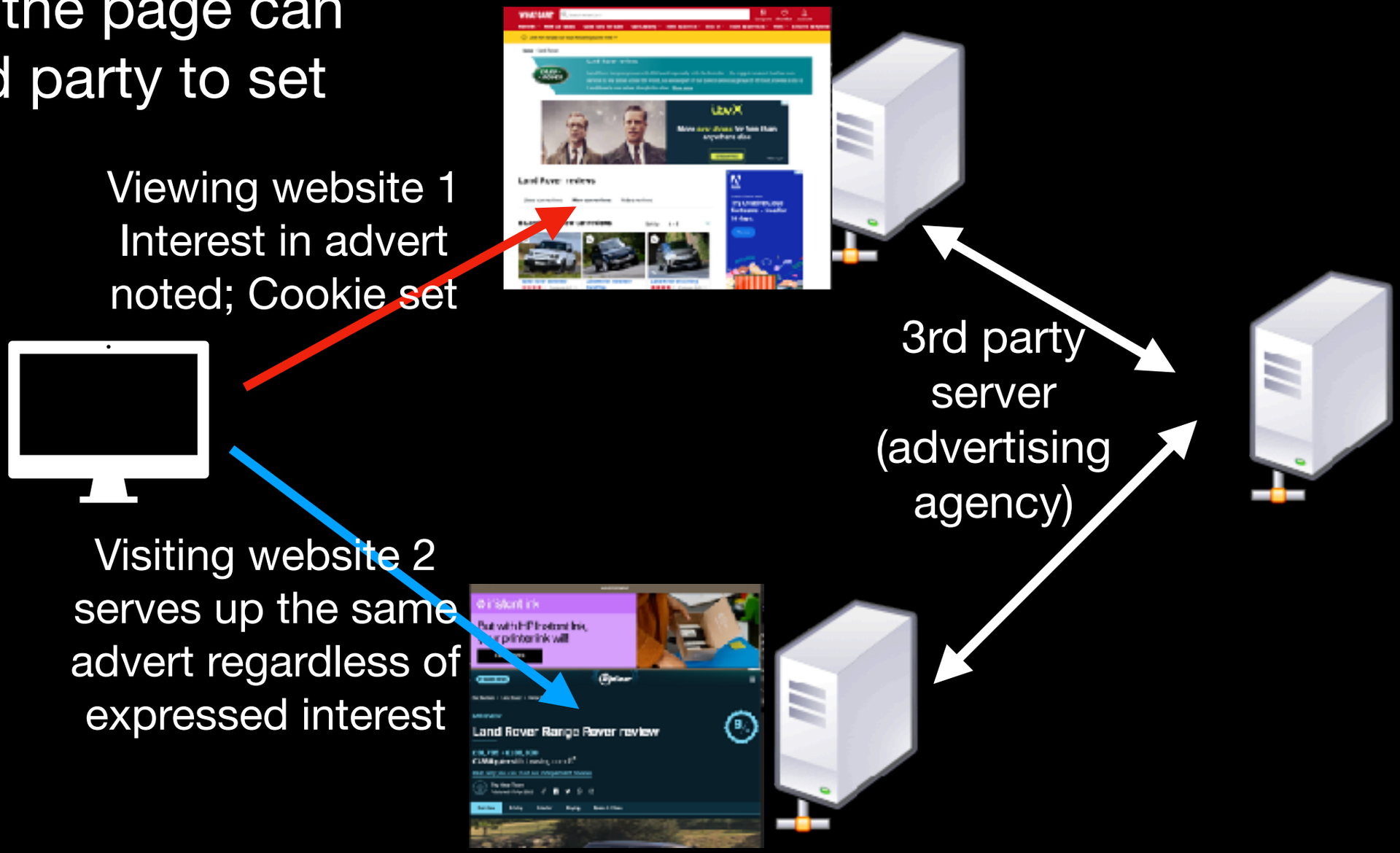
http Cookies

- Third Party Cookies are used for cross-site tracking.
- They are generated and placed on the user's device by a different (3rd party) website to the one the user is visiting. The visited website includes ads or images from the 3rd party sites.
  - e.g. if you play an YouTube video embedded in a website, YouTube will set cookies on your browser.
- They can be used to carry out advertising processes like behavioural profiling and retargeting.

Third Party Cookies

http Cookies

- Webpages display material provided by a 3rd party - for example advertising, YouTube or social media.
- Just visiting the page can allow the 3rd party to set a Cookie on your pc.



Status of 3rd party Cookies

Cookie wars

- Privacy Groups have campaigned against the use of 3rd party cookies.
- Laws like the EU's General Data Protection Regulation (GDPR) and ePrivacy set restrictions on how cookies can be used.
  - An identifying cookie is considered personal data
  - To be compliant, a business must have a lawful basis to process the data.
  - Consent is only acceptable when there are other viable options.

- The consequences are that you should always be asked to accept or reject cookies. And rejecting should not prevent you from using the website.

Cookie treatment by Browsers

Cookie wars

- **Google Chrome**, the most popular web browser (63%)
  - Chrome does not block 1st or 3rd party cookies by default
  - Cookies can be deleted - which removes all cookies
  - 3rd party cookies can be blocked by changing settings
  - Google’s announced plans to allow users to block and delete third-party cookies, while keeping first-party cookies intact have been delayed until at least 2024.
  - A large majority of Google’s revenue (about 86%) is derived from advertising..
- **Microsoft Edge Chromium, Chrome, Opera** and dozens of other browsers are based on the open-source Chromium project and have similar appearance and functionality.

info from https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

Cookie treatment by Browsers

Cookie wars

Some Browser suppliers are making privacy a selling point:

- **Apple Safari** provides intelligent tracking prevention as a default - which stops 3rd party cookies and the use of 1st park cookies in a 3rd party context.
  - Analytics cookies that would previously last for two years (if not purged) are now deleted by Safari after seven days under ITP.
- **Firefox and Mozilla** offer a Safari-like “intelligent” functionality blocking unwanted third-party tracking cookies.
- Most browsers offer some kind of cookie blocking method – but not all of them are based on blacklists or algorithms.

info from https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

How to block third party cookies

http Cookies

Third-party cookies are blocked when a user does one or more of the following:

- Browses the web in private or incognito mode.
- Uses Safari as their web browser on Apple mobile devices, as it blocks third-party cookies by default.
- Changes the cookie and tracking settings in their browsers (detailed below).
- Uses Tor.
- Installs ad blockers or similar add-ons (Ghostery, Pivacy Badger etc).

Most browsers allow users to disable third-party cookies from the settings menu. Doing so will make the ads much less personalised, but shouldn't otherwise compromise the browsing experience.

From: https://securiti.ai/blog/third-party-cookies/

Microsoft Edge

Click the ellipsis (three dots) symbol in the top-right corner and select Settings. Click View Advanced Settings and select Block Third-Party Cookies from the drop-down menu under Cookies.

Internet Explorer

In Internet Explorer, you have to click the gear icon in the top-right corner and select Internet Options. Then go to Privacy tab and click Advanced. Check the Override Automatic Cookie-Handling box, and set Third-Party Cookies to "Block."

Google Chrome

Click the three-lined icon in the top-right corner and select Settings. Then, click Show Advanced Settings at the bottom. Click on Content Settings in the Privacy section. Under Cookies, check the Block Third-Party Cookies and Site Data option and click Done.

Firefox

Click the three-lined icon in the top-right corner and select Options (PC) or Preferences (Mac). Go to the Privacy tab and under History, set Firefox Will to Use Custom Settings for History. Then set Accept Third-Party Cookies to "Never."

Safari

Third-party cookies are turned off by default, but it never hurts to double check. Pull down the Safari menu and select the Privacy tab. Choose the option to block cookies from third parties and advertisers.

Thank You