UNIVERSITY OF
Southampton

UNIVERSITY OF
Southampton

Cookies

COMP3200 Web Infrastructure

Dr Nicholas Gibbins – nmg@ecs.soton.ac.uk

The infamous cookie

Intended as a way for web servers to persist state across HTTP requests

- (but isn't HTTP supposed to be stateless?)

Invented in 1994 by Lou Montulli of Netscape

- (also the inventor of the <blink> tag)

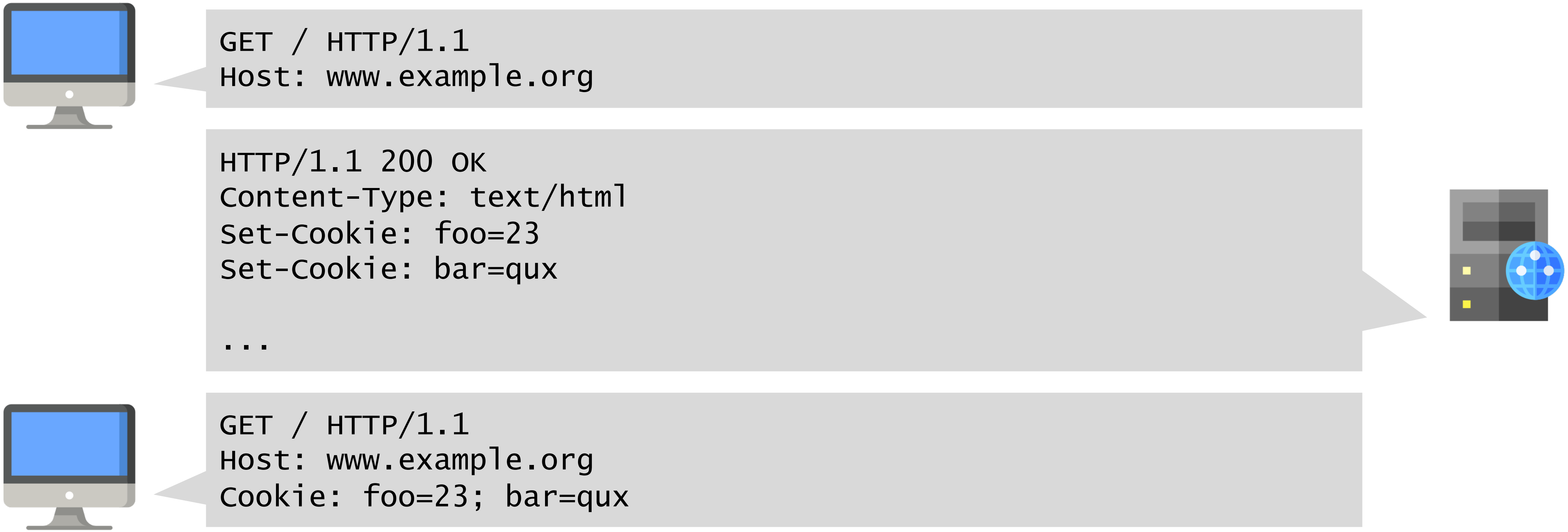
Patented in 1995

- (Netscape Communications Corp. vs ValueClick Inc.)

Ostensibly deprecated in favour of HTML5 local storage ... and yet it still lives!

Barth, A. (2011) *HTTP State Management Mechanism*. RFC6265. Available online at: https://tools.ietf.org/html/rfc6265

Cookies



```
GET / HTTP/1.1
Host: www.example.org
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Set-Cookie: foo=23
Set-Cookie: bar=qux

...
```

```
GET / HTTP/1.1
Host: www.example.org
Cookie: foo=23; bar=qux
```

Lifetime

Cookies can either be session cookies or permanent cookies

- Session cookies expire "when the current session ends" (when the browser is closed?)
- Permanent cookies have a specified expiry time

```
Set-Cookie: foo=23; Expires=Fri, 23 Oct 2020 10:05:34 GMT
```

- Indicates that the cookie should expire after the given date

```
Set-Cookie: foo=23; Max-Age=21600
```

- Indicates that the cookie should expire after `Max-Age` seconds

Access restriction

`Set-Cookie: foo=23; Secure`

- Indicates that the cookie should only ever be sent over HTTPS

`Set-Cookie: foo=23; HttpOnly`

- Indicates that the cookie should not be visible from within the `Document.cookie` interface

Scope

`Set-Cookie: foo=23; Domain=example.org`

- Cookie should only be sent to example.org or its subdomains (i.e. foo.example.org)
- Defaults to the origin server that set the cookie (excluding subdomains)

`Set-Cookie: foo=23; Path=/bar`

- Cookie should only be sent if value of `Path` is in the requested URI

`Set-Cookie: foo=23; SameSite=Strict`

- `Strict`: only send cookie to the same site that originated it
- `Lax`: cookie is withheld for cross-site subrequests (i.e. images) but sent when user follows a link (typical browser default setting)
- `None`: no restrictions on cross-site requests

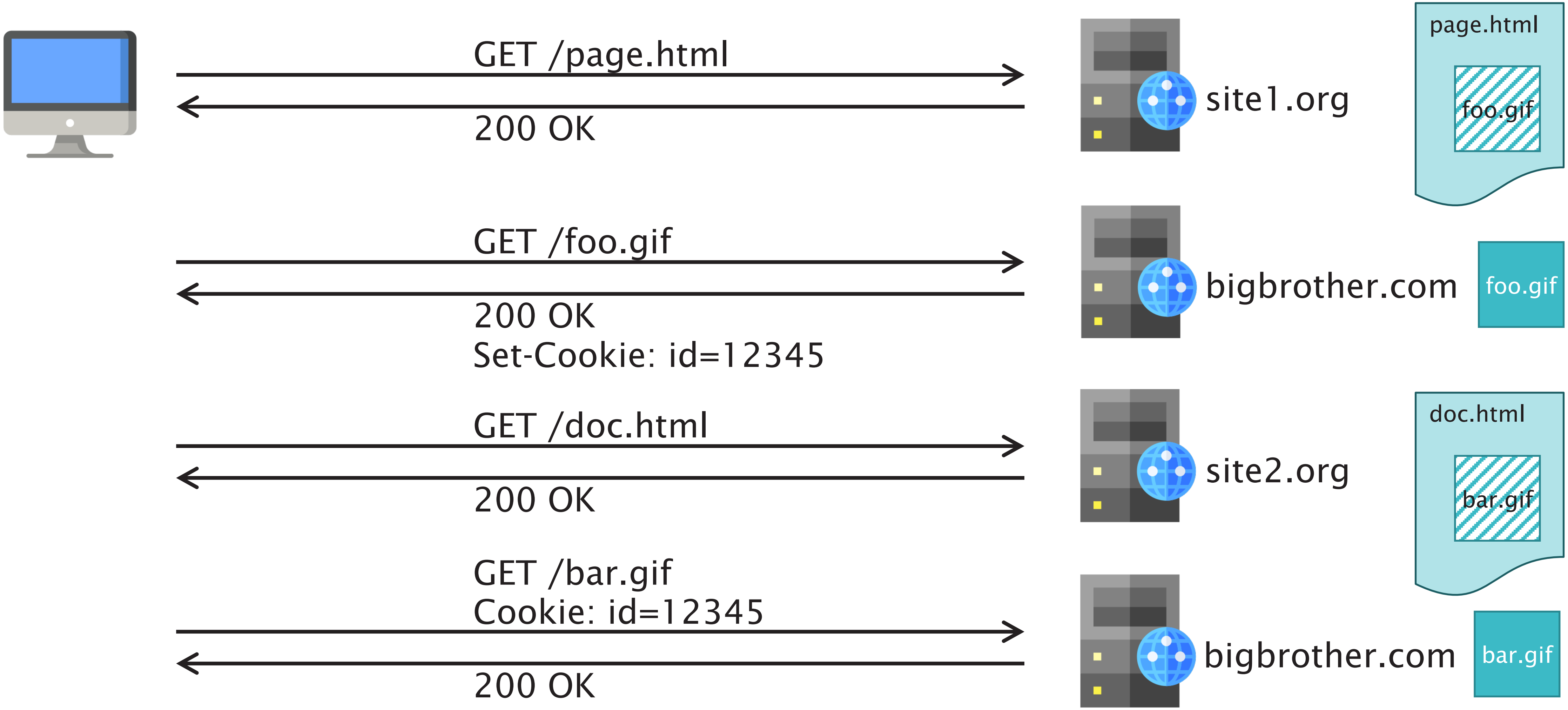
Privacy considerations

Cookies can be used to track users across websites

Relies on websites embedding resources (typically images) from third parties

- When a user fetches the third party resource, it sets a cookie
- Cookie may be read when the user fetches a resource from the third party in future

Relies on default browser cookie scope of `SameSite=None`



GET /page.html

200 OK

site1.org

page.html

foo.gif

GET /foo.gif

200 OK
Set-Cookie: id=12345

bigbrother.com

foo.gif

GET /doc.html

200 OK

site2.org

doc.html

bar.gif

GET /bar.gif
Cookie: id=12345

200 OK

bigbrother.com

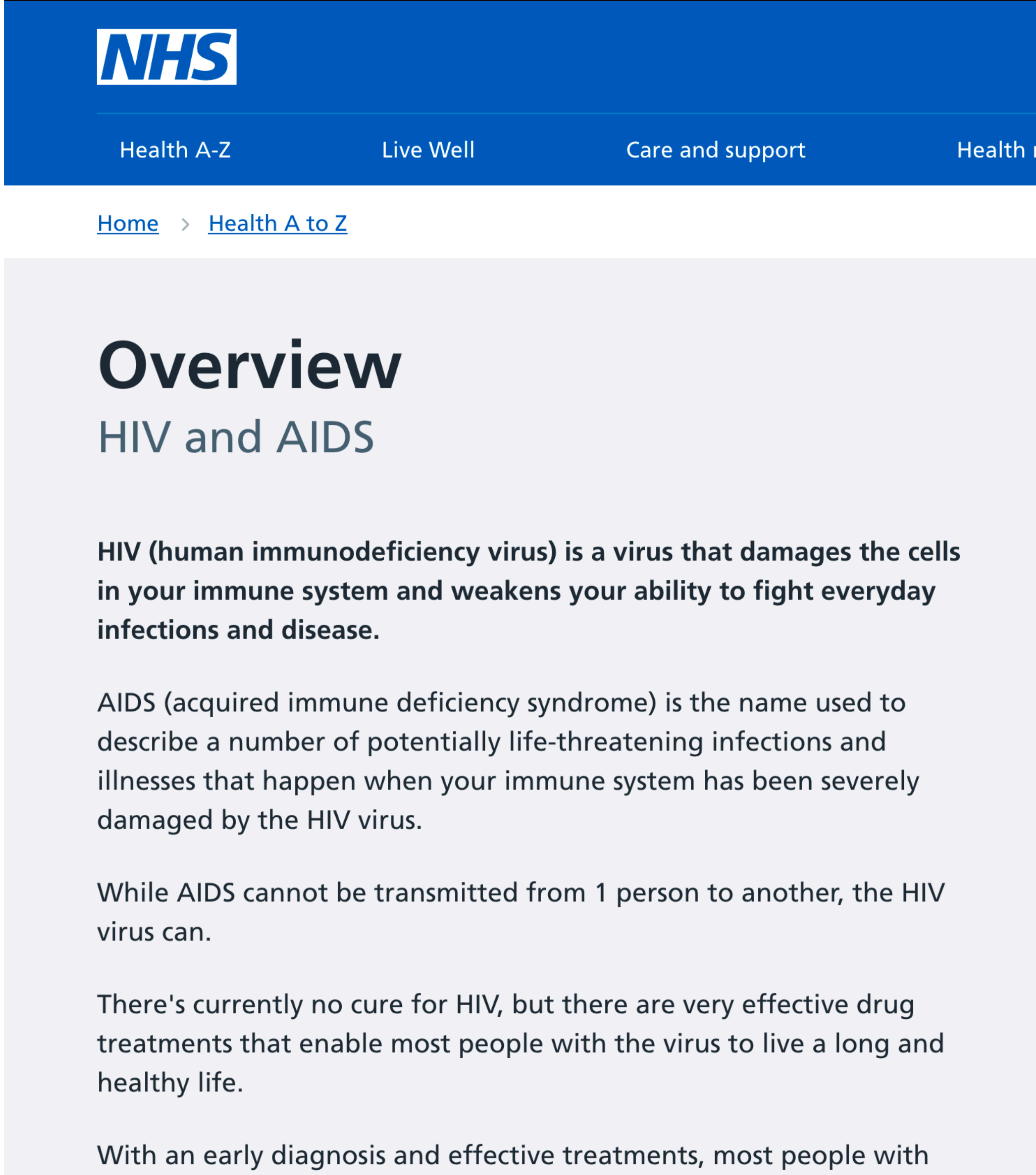
bar.gif

Privacy considerations

High profile UK case in 2010
(discovered by a Southampton graduate!)

- NHS put Facebook "like" buttons on their webpages (loaded from Facebook's CDN)
- When a user visited an NHS webpage, Facebook set a cookie
- If the user visited a different page with a like button, Facebook could read the cookie and correlate those visits
- If they were logged into Facebook, Facebook now knew what their users are searching the NHS for

https://mmt.me.uk/blog/2010/11/21/nhs-and-tracking/



Overview

HIV and AIDS

HIV (human immunodeficiency virus) is a virus that damages the cells in your immune system and weakens your ability to fight everyday infections and disease.

AIDS (acquired immune deficiency syndrome) is the name used to describe a number of potentially life-threatening infections and illnesses that happen when your immune system has been severely damaged by the HIV virus.

While AIDS cannot be transmitted from 1 person to another, the HIV virus can.

There's currently no cure for HIV, but there are very effective drug treatments that enable most people with the virus to live a long and healthy life.

With an early diagnosis and effective treatments, most people with

Next Lecture: HTML