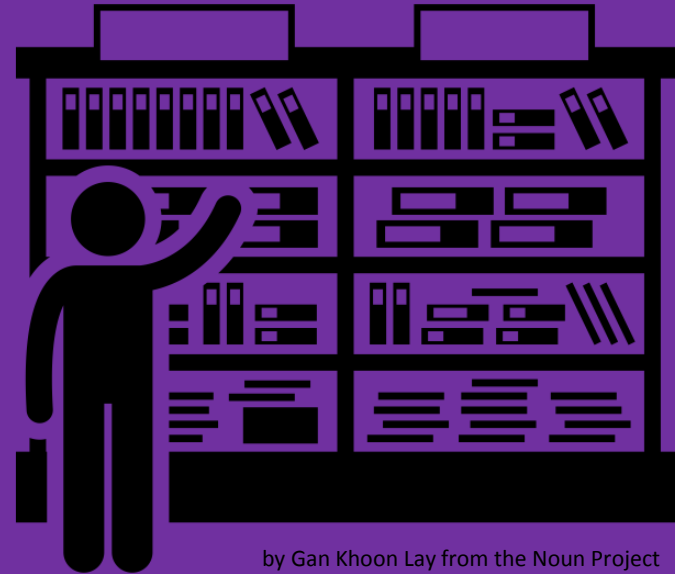


Taking a stand for privacy

#libstaff4privacy

by Gregor Cresnar from the Noun Project



by Gan Khoon Lay from the Noun Project



Created by Aude Charillon at Newcastle Libraries for the Carnegie UK Trust in April 2018.
Copyright in this presentation has been waived and content placed in the public domain (under [CC0](#)).
Content not under CC0 is credited on the slide it appears on.

For you, what is privacy?

privacy [noun]

1 A state in which one is not observed or disturbed by other people

1.1 The state of being free from public attention

How does it fit with
the role of library staff?

“Librarians have the understanding and expertise to
champion and promote openness and the public’s right to information;
oppose censorship and efforts to inhibit access to information;
select and make available information;
guide and support the public to seek, obtain and navigate
available information;
support the public to utilise and share this information;
facilitate intellectual and cultural creativity;
and safeguard the privacy of the public through ensuring data collation
and surveillance are necessary, proportionate and lawful.”

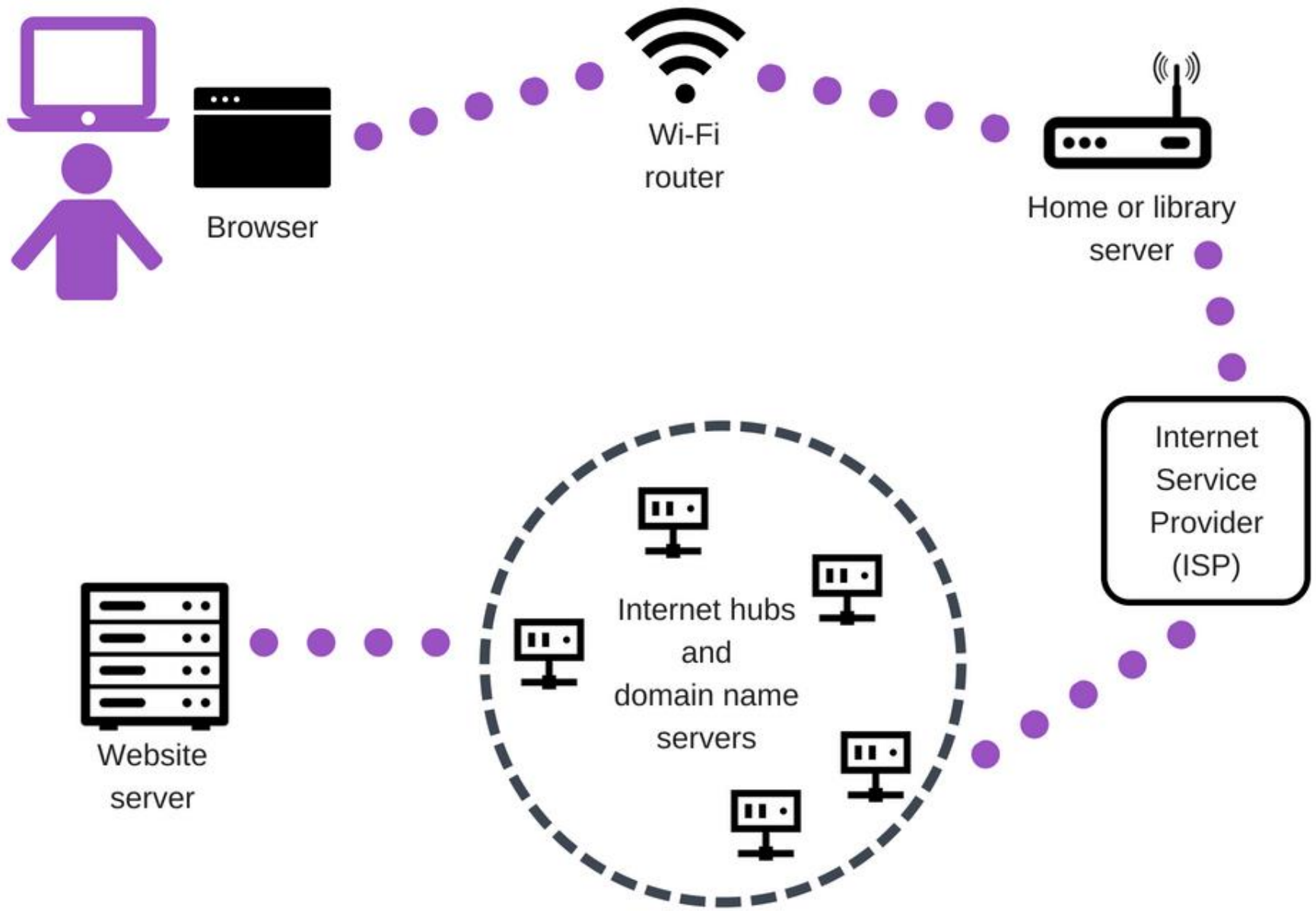
*Ambition & opportunity: a strategy for public libraries in
Scotland 2015-2020.*

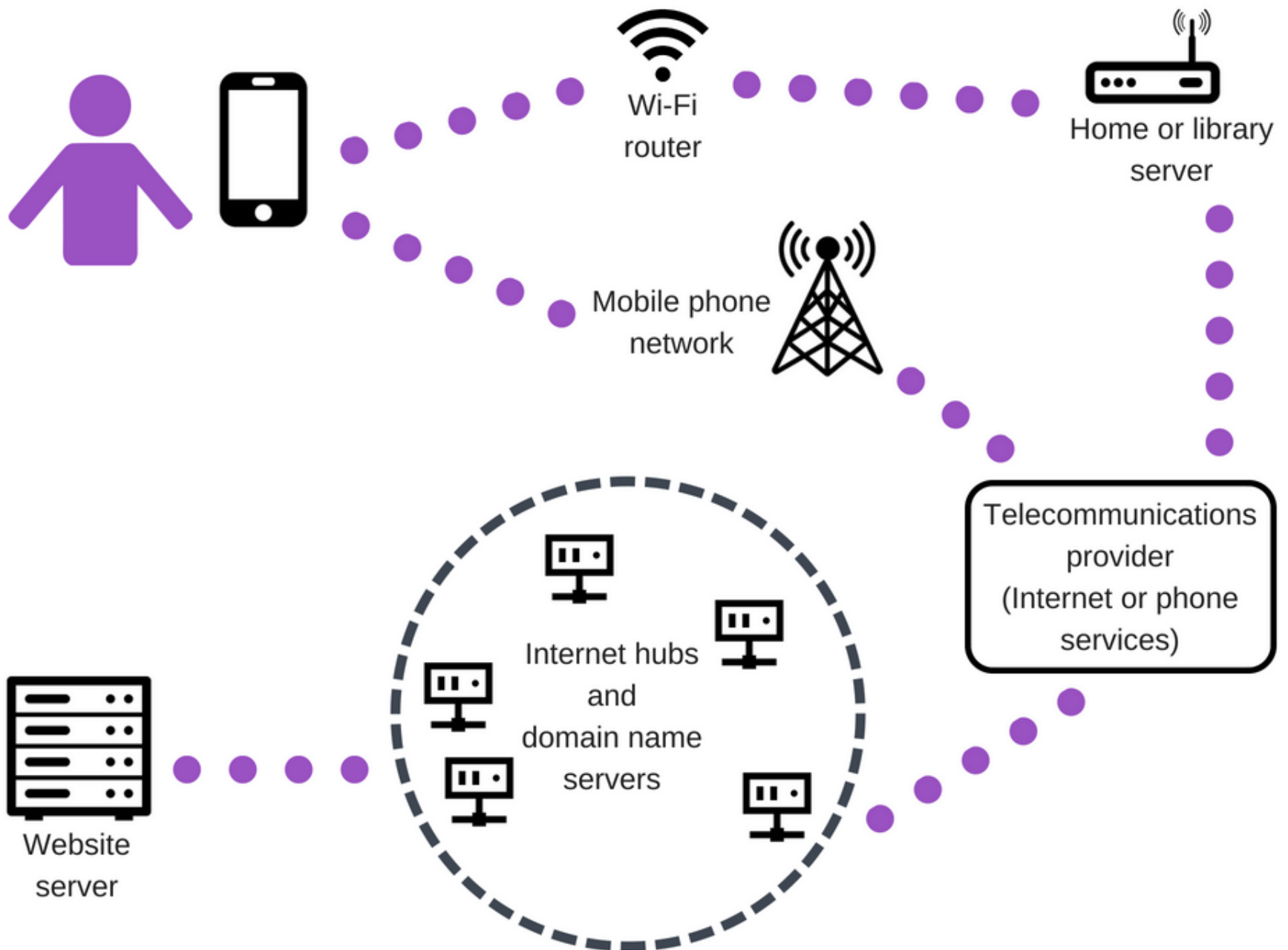
Strategic aim 5: Libraries promoting culture and creativity

In order for libraries to be
safe and impartial spaces...

...we library staff have to
take a stand to protect
citizens' privacy.

How is your privacy
affected online?







What are cookies?

You've heard a website uses cookies. But what does that mean?

► Watch video



What can you do
about it?

Threat modelling

- What information / data do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

Threat modelling

in the library

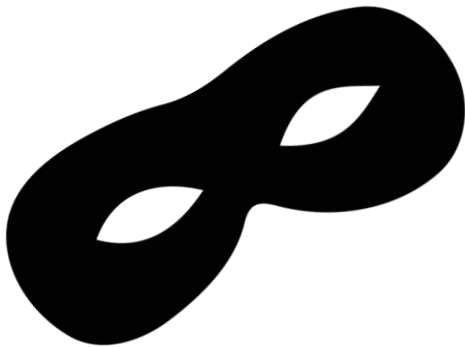
- What information / data do you want to protect?
Members' personal info in the LMS and the OPAC
- Who do you want to protect it from?
Malicious individuals; commercial interests
- How likely is it that you will need to protect it?
Quite likely
- How bad are the consequences if you fail?
Breach of legal duties = big fine, reputational damage
- How much trouble are you willing to go through in order to try to prevent those?
Quite a bit, actually



Passphrases rather than passwords

- The longer the passphrase the more difficult for a computer to crack it.
- Words are easier for us humans to remember.
- Make it random.

Big Browser is watching you!



mask by Sergey Patutin
from the Noun Project

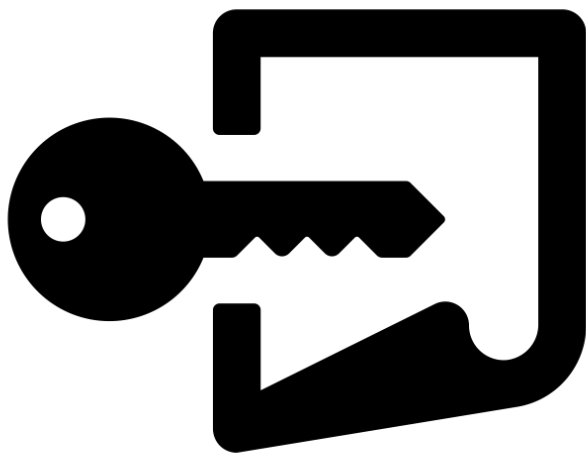
- Browser history
- Private modes
- Browser add-ons
- Search engines

Install and try one of these tools:
compare it with what you normally use



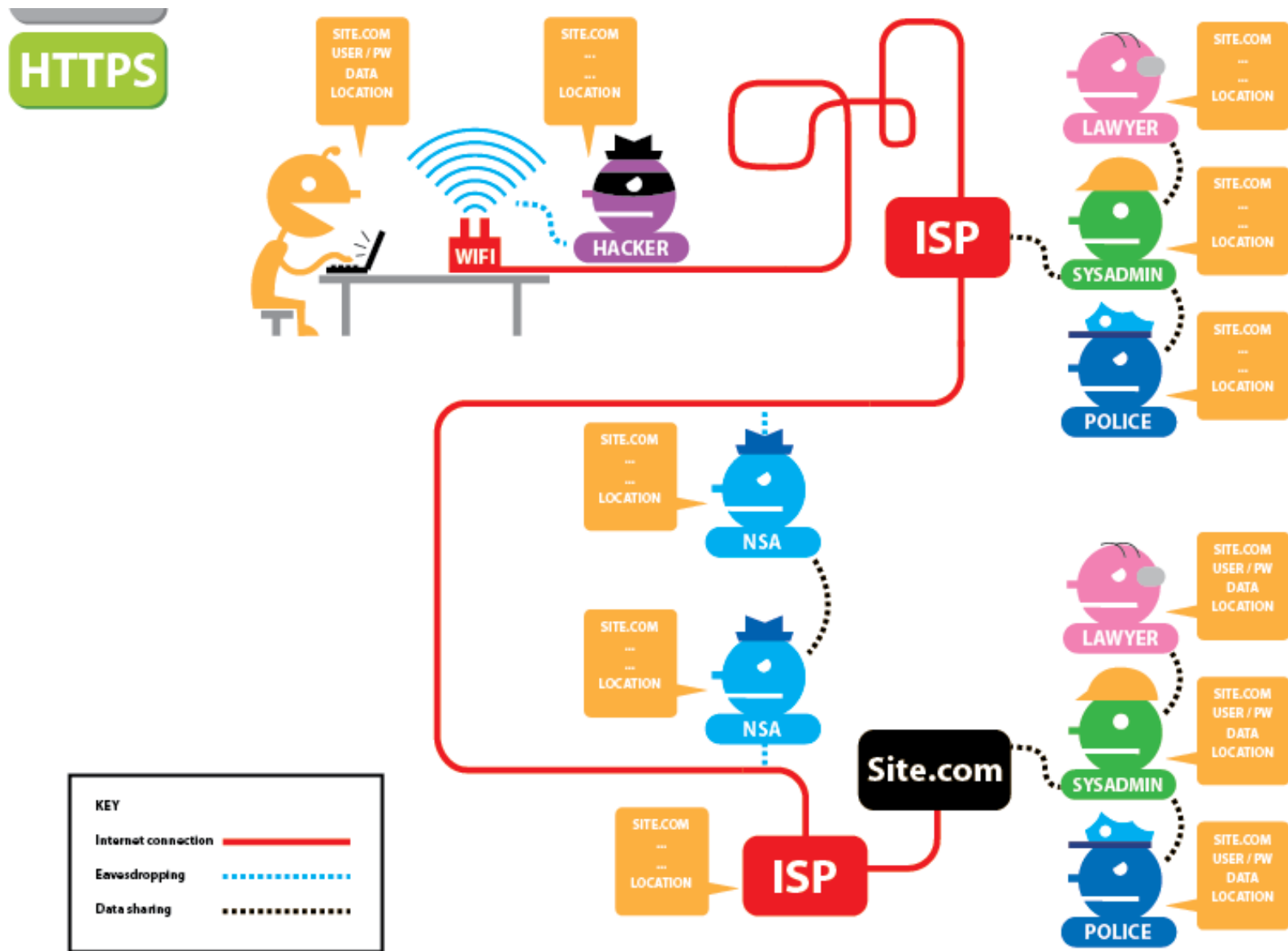
Or clear your browser history and cookies;
try a private browser.

Secure communications thanks to **encryption**



Created by Gregor Cresnar
from Noun Project

- HTTPS
- Email encryption
- Messaging services



From Electronic Frontier Foundation
<https://www.eff.org/pages/tor-and-https> (cropped)

Used under a [Creative Commons Attribution licence](https://creativecommons.org/licenses/by/4.0/)

What can we do for
citizens in libraries?

A horizontal tear in a grey surface reveals a white background. The word "Transparency" is written in a purple, sans-serif font across the white area. The tear is irregular and jagged, with a small piece of the grey surface hanging down on the left side.

Transparency



RFID is in use on these premises

**This may, in certain circumstances, constitute a risk
to your privacy. We take this risk very seriously.**

Screenshot from: BIC RFID privacy poster template - July 2017
<http://www.bic.org.uk/161/RFID-Privacy-in-Libraries>



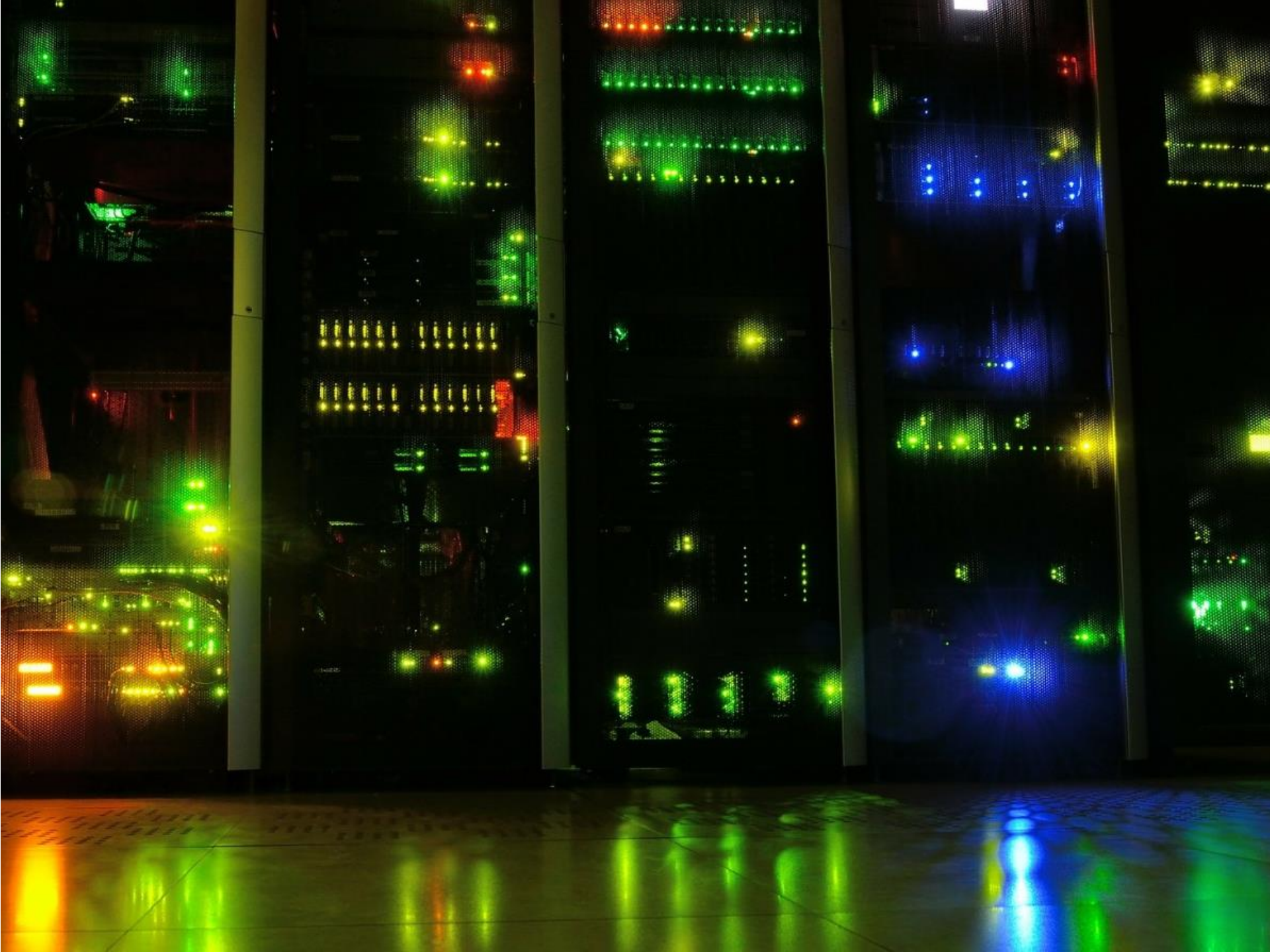
Data retention policies

- computer usage logs
- Internet browsing history on public computers;
- files and other traces left by citizens on public computers;
- Wi-Fi usage logs;
- library members' borrowing history;
- library members' reservation history;
- library members' payments history;
- former library members' details;
- online catalogue / online library account usage logs;
- website analytics;
- events attendees list and personal registration details;
- CCTV logs;
- back-up databases and server logs.

Threat modelling

in the library

- What information / data do you want to protect?
Members' personal info in the LMS and the OPAC
- Who do you want to protect it from?
Malicious individuals; commercial interests
- How likely is it that you will need to protect it?
Quite likely
- How bad are the consequences if you fail?
Breach of legal duties = big fine, reputational damage
- How much trouble are you willing to go through in order to try to prevent those?
Quite a bit, actually



- “1. **Data breach policy**: is there a formal process in place to report data breaches if / when they occur?
2. **Data encryption**: if patron data is stored by the vendor, is it encrypted?
3. **Data retention**: does the vendor purge patron search history records on a regular basis?
4. **TOS “ease of use”**: can the average patron read and fully understand the vendor’s terms of use policy?
5. **Patron privacy**: does the vendor use Google Analytics or other tracking software to monitor users?
6. **Secure connections**: does the vendor’s website enforce secure connections only? (HTTPS or better?)
7. **Advertising networks**: does the vendor’s website participate in ad networks?”



City Library (5 January 2017) – level 4 [cropped] by Newcastle Libraries (Source: [Flickr](#))
Used under Creative Commons Attribution licence ([CC BY 2.0](#))

CRYPTOPARTY

Come and learn how to protect your privacy online

What next?



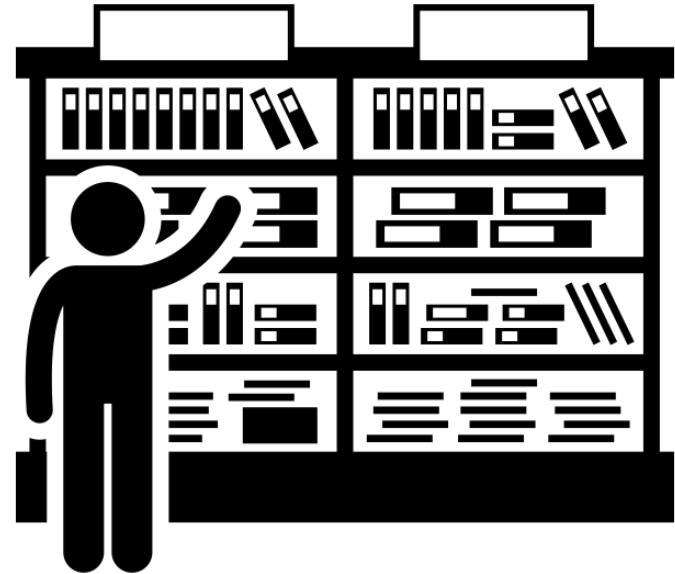
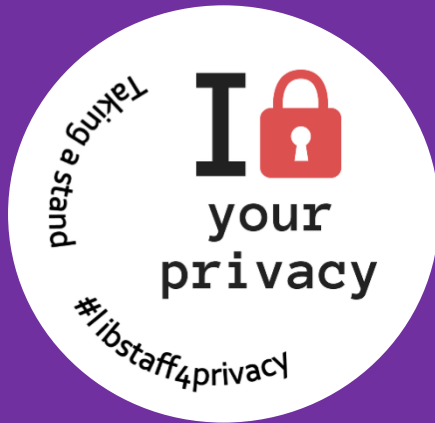


Image left: by Gregor Cresnar; image right: by Gan Khoon Lay. Both from the Noun Project

Taking a stand for privacy



Please get in touch!

aude.charillon@newcastle.gov.uk
@Audesome

#libstaff4privacy