**Taking a stand for privacy**

Workshop facilitator’s guide

This facilitator’s guide accompanies the *Taking a stand for privacy* workshop slides. Also included in the *Taking a stand for privacy* workshop materials is a badge design (in PNG image format). The badge was designed to be used on 32mm diameter round pin badges distributed to workshop participants.

The workshop materials were created as part of a project funded by the [Carnegie UK Trust](https://www.carnegieuktrust.org.uk/). This project has also resulted in the publication of *Leading the way : a guide to privacy for public library staff*, available from the Trust’s website.

These workshop materials were created by Aude Charillon at Newcastle Libraries for the Carnegie UK Trust in March and April 2018 and used to deliver workshops from March to May 2018. The materials therefore reflect Aude’s opinions and style of presentation; it is likely they will need to be adapted for use by a different workshop facilitator.

Just like for the slides and badge design, copyright in this facilitator’s guide has been waived and content placed in the public domain (under [CC0](https://creativecommons.org/publicdomain/zero/1.0/)). Please copy, adapt, re-use and share.



Who is this facilitator guide for?

This guide is for anyone looking to run a digital privacy session for library staff. It takes you through the steps needed to deliver your own *Taking a stand for privacy* workshop. Delivering the workshop does require some prior knowledge of digital security and online privacy issues and tools.

Who is the workshop for?

1. library assistants;
2. librarians;
3. library managers.

What will staff gain by attending?

By the end of the session, participants will:

* have an understanding of how and why the issue of online privacy affects libraries and citizens using them;
* know what personal information is shared when accessing a website or using a mobile app;
* be able to use and recommend basic digital privacy tools and practices;
* know what steps to take to better protect the online privacy of citizens using library services.

What do we hope to achieve by delivering the workshop?

After attending the workshop, participants will:

* be informed citizens when it comes to how the Internet works, how it impacts their online privacy and how to protect it;
* take a stand for citizens' privacy in libraries by:

1. supporting and advising citizens when they use computers in libraries;
2. developing services or activities to support citizens in protecting their privacy online;
3. reviewing library policies to better protect the privacy of citizens using library services;

* share what they have learnt with colleagues.

Outline

This workshop lasts about 3 hours and includes a 15min break.

Welcome and introductions (15min)

Why privacy and libraries (15min)

How your privacy is affected online (30min)

What we can do about it

Assessing risk (15min)

Basic tips and tools (30min)

Break (15min)

Basic tips and tools (10min)

What we can do for citizens in libraries (35min)

What next (15min)

Preparation

An experienced facilitator would be able to manage a group of up to 15-20 people (for big groups, add an extra 30min to the workshop length). A beginner facilitator may prefer a smaller group. It is not recommended to have a group bigger than 20, as it would make the discussions parts of the workshop more difficult.

Attendees should preferably bring a laptop if they have one; smartphone or tablet also useful.

Requirements:

* a meeting room equipped with a big screen that can be connected to the facilitator’s computer;
* a computer on which the facilitator has installed the software to be demonstrated;
* Wi-Fi for all participants;
* a flipchart and pens;
* a book to demonstrate generating random passwords.

On the facilitator's computer, install:

* Mozilla Firefox, with add-ons:
  + [Lightbeam](https://addons.mozilla.org/en-US/firefox/addon/lightbeam/);
  + [Privacy Badger](https://www.eff.org/privacybadger);
  + [HTTPS Everywhere](https://www.eff.org/https-everywhere);
* Google Chrome;
* [Tor Browser](https://www.torproject.org/projects/torbrowser.html) (stable version).

Before the session starts:

* open the websites you are going to use (Mentimeter, Cookies video on YouTube…);
* clear the data on Lightbeam and your Mentimeter presentations if you have used them before;
* disable Privacy Badger and HTTPS Everywhere.

You may also like to check that Tor Browser is not blocked by your Internet Service Provider.

To print before the session (one per participant):

* threat modelling exercise sheets;
* information and resources handout.

Both documents can be found at the end of this guide.

[Mentimeter](https://www.mentimeter.com/) is used for some of the interactive parts. To respond to the online polls participants need to access the website; that’s one of the reasons why they are asked to bring a laptop, tablet or smartphone and that Wi-Fi is needed.

You can set up a free Mentimeter account and create two presentations of two questions each: one presentation for the “Why privacy and libraries” part and one for the “What next?” part as follows.

|  |  |
| --- | --- |
| **Why privacy and libraries** | |
| Question 1 (type: word cloud) | Question 2 (type: scales)  Your heading: How does it fit with the role of library staff?  Statements  1. “Privacy? It’s none of our business”  2. We collect citizens' personal information all the time  3. We do things around digital skills  4. We have a role in protecting freedom of information & freedom of expression  5. It's a requirement (laws, library national strategies...) that we look into it |
| **What next?** | |
| Question 1 (type: open ended)  Your question: What is the first thing you will do / would like to implement when you get back to your library to better protect the privacy of citizens? | Question 2 (type: open ended)  Your question: Is there anything I mentioned in the workshop that you think would be difficult to change / implement / install in your library? What is it and why?  Longer description: Here I'm trying to gauge what barriers and challenges you may face, to then try to understand what could possibly be done to help. |

Workshop step by step

| On the big screen | Facilitator | Time |
| --- | --- | --- |
| Slide 1. | **Welcome and waiting time**  Wait for all participants to arrive.  Start the session by:   * welcoming participants; * doing the housekeeping; * mentioning planned break; * explaining how to get on the Wi-Fi. | 5min |
| Slide 1. | **Introductions**  If the participants do not know each other: introduce yourself and ask participants to briefly do the same.  Explain the aims of the session, what will happen, what the rules are, e.g.:  “*I want you as citizens to have an understanding of what happens to your personal information online, and to know what steps you can take – should you wish to – to protect your privacy. Obviously, I also want you to have this knowledge so that you can apply it to your job: to how you do things in your library service and so you may pass some of this knowledge on to the citizens you serve.*  *As an introduction we will look into why we’re here to talk about privacy. The first part of the workshop will be focusing on you as an individual and how your privacy is impacted online. In the second part we will discuss how to draw on what you’ve just learnt and apply it in your library.*  *I don’t believe there is such a thing as “stupid” questions; there are just questions, so feel free to interrupt me and ask some. We are here, a small group in a safe space; it’s ok to share examples of our personal and professional lives. If used again outside these sessions, those examples will not be attributed. Finally, I will say things that you might disagree with; it’s normal. I could even say: it’s on purpose! We will all have different perceptions, be sensitive to different things and therefore have different opinions; do voice yours.”* | 10min |
| **Why privacy and libraries** | | 15min |
| Slide 2. | **What is privacy?**  Switch from this slide to the first question on the *Why privacy and libraries* Mentimeter presentation. |  |
| Mentimeter | To take part in the poll participants will need to go to the website www.menti.com and type in the number that is displayed at the top of the facilitator’s screen. The word cloud will take shape as soon as participants start to submit their answers.  Briefly comment the Mentimeter word cloud. |  |
| Slide 3. | **Privacy definition**  Read out the dictionary definition. Briefly compare with the word cloud and/or ask participants if the dictionary definition fits with theirs. |  |
| Slide 4. | **How does it fit with the role of library staff?**  Switch from this slide to the second question on the *Why privacy and libraries* Mentimeter presentation. |  |
| Mentimeter | Read each statement. Explain the ratings: 1 if you strongly disagree, 2 if you slightly disagree, 3 if neither agree nor disagree, 4 if you agree, 5 if you strongly agree.  Once participants have submitted the answers, comment on the results and explain the statements.   * + - 1. “Privacy? It’s none of our business”   This attempt at a witty statement is also there to provide a contrary view. [I used the quotation marks because the credit for it goes to a friend of mine! Aude]   * + - 1. We collect citizens' personal information all the time   We collect citizens’ details when they join the library or register for an event, we collect other personal information when they use computers or the Wi-Fi, we record what they borrow, we take pictures of them at events, etc.   * + - 1. We do things around digital skills   Library staff run digital skills sessions for citizens or offer the use of library space for digital skills courses.   * + - 1. We have a role in protecting freedom of information & freedom of expression   The [IFLA Statement on privacy in the library environment](https://www.ifla.org/publications/node/10056) endorsed August 2015 states: “Freedom of access to information and freedom of expression, as expressed in Article 19 of the Universal Declaration of Human Rights, are essential concepts for the library and information profession. Privacy is integral to ensuring these rights.”  ([Universal Declaration of Human Rights](https://www.un.org/en/universal-declaration-human-rights/index.html) Article 19: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” The IFLA statement also quotes article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”)   * + - 1. It's a requirement (laws, library national strategies...) that we look into it   We have to comply with data protection laws such as GDPR and the Data Protection Act. Example of privacy mentioned in national library strategy on the next slide. |  |
| Slide 5. | **Scottish public libraries strategy**  In Scotland there is a national strategy for public libraries. In the “Strategic aim 5: Libraries promoting culture and creativity”, it says that “Librarians [which I read to mean “library staff”] have the understanding and expertise to […] safeguard the privacy of the public through ensuring data collation and surveillance are necessary, proportionate and lawful.” |  |
| Slide 6. | **Ethics**  *“This is one of the times in this workshop when you might disagree with me!*  *Some of us may be members of CILIP, the library and information association. As members we have signed up to the CILIP ethical framework. The current [in May 2018]* [*CILIP ethical principles*](https://www.cilip.org.uk/page/Ethicalframework) *approved in 2004 state: “The conduct of members should be characterised by the following general principles and values […] no.8. Respect for confidentiality and privacy in dealing with information users”.*  *I would argue that we need to go further than respecting citizens privacy; we need to take active steps to protect it. We offer access to information and are trusted to do this in a way that is safe and impartial. But we cannot be neutral: if we do nothing to support citizens we are implicitly supporting commercial interests or others to invade citizens’ privacy in our libraries. That’s why I believe we have to take a stand to protect citizens’ privacy.”*  If needed: mention the definitions of [neutral](https://premium.oxforddictionaries.com/definition/english/neutral) and [impartial](https://premium.oxforddictionaries.com/definition/english/impartial) to highlight the difference. |  |
| **How your privacy is affected online** | | 30min |
| Slide 7. | **How is your privacy affected online?**  *“Today we’ll be mainly talking about what’s happening online. In this first part we’re looking at the issue from our point of view as individuals: how is our personal privacy affected online anyway? At what point is our personal information collected, what is being collected, and by whom?”* |  |
| Slide 8. | **How the Internet works**  *“To understand what happens with our personal information online we need to look at how the Internet works. This is what this diagram shows, very roughly!*  *Let’s imagine I want to look something up on my library’s online catalogue. This is me in front of my computer. I access the library website by using an Internet browser. Once I’ve typed in my keywords and clicked “search” my browser sends my request on. If I’m on the Wi-Fi my request goes via the Wi-Fi router, then to the Internet server (either my home’s or the library’s, depending on where I am), the Internet Service Provider… My request is on its way to the server that hosts my library’s online catalogue webpages. To get there it will travel via several other servers known as Internet hubs and domain name servers. Finally it reaches my library website’s server, which deals with the request and sends the response back via the same way, all the way back to my browser.”* |  |
| Slide 8. | **List of personal information**  *“We’ve seen the journey of the Internet request. What information relating to you do you think is circulated on that journey or can be collected when you use the Internet? Let’s a make a list. I’ve used the example of searching the library’s catalogue so the first thing relating to me that is circulated around the Internet is my search query, the keywords I’ve typed. What else?”*  Use the flipchart and pens to make a list from participants’ suggestions. If they stall, ask them what information can be collected about them in different situations, such as: when they are accessing information websites, doing some online shopping, using email; or ask more direct questions, e.g., have you ever been on a website of, say, a hotel in a foreign country, and it was showing you the English version even though the country uses another language?  You should end up with a list that looks like this:   * Search query * Login/username * Password * Content posted * Website (destination) * IP address * Location (e.g. country through ISP) * Wi-Fi network used * Browser * Plug-ins used * Other sites visited (pages within sites, videos watched if on YouTube…) * Operating system * Size of screen * Language (of operating system or browser) * Time zone * Links to other accounts (e.g. Google, Facebook)   If you can’t get all the answers out of participants, add the missing elements to the list yourself and give examples of when this information would be collected. |  |
| Slide 9. | **On your mobile phone**  Go through the diagram of how the Internet works, this time when accessed from a mobile phone.  Go back to the list of information relating to the individual using the Internet. Ask participants: *“What else can be shared when you use apps on your mobile phone? Have you ever checked to see what apps have access to?”*  Using participants’ suggestions, your list should expand with the following:   * Photos on phone * Contact lists * Content downloaded (apps, docs, images) * Calendar * Messages * Location from phone provider or GPS |  |
| Slide 10. | **Tracking**  *“We now have a list of information that may be collected about us when we use the Internet. Often we do not notice this collection happening as they are done by third-party elements being embedded in websites. Those elements can collect even more information about us when they are present on several websites and therefore can get a better insight into our online behaviour. This is known as tracking.”* |  |
| Browser: Firefox | **Lightbeam demonstration**  *“To get a better idea about who collects data about us, I’m going to use Lightbeam. Lightbeam is an add-on for Firefox that shows you which third parties are present when you visit a website and which may be tracking you.”*  Show and explain what Lightbeam looks like before you start. You should only have a couple of nodes: mainly Mentimeter and YouTube. Each of these websites have third-party elements on them, shown as triangles linking to the website node. None of these elements should connect with others on another website yet as you haven’t started browsing.  Open a new browser tab alongside Lightbeam and start browsing in this new tab. Use Google to access a local news website. Make sure you scroll down the page, give it time to fully load all elements. Click on an article, navigate from this article to another. Repeat the process with a few more websites; for example a national TV channel website, a travel website, look for items to buy on Google and click through to some of the results, watch a YouTube video…  Tip: the more loaded with adverts the websites you visit are, the more impressive the result on Lightbeam is likely to be!  Go back to Lightbeam; it should now look like a teeming spider web. Hover over the elements that are interconnected with more than one node – this interconnection means the third-party knows you’ve been on both websites and can use this information to track your behaviour. Read aloud and comment what they are.  Read aloud the statistics on Lightbeam’s top bar: “You have visited […] sites” and “You have connected with […] third party sites”. |  |
| Slide 11. | **Cookies**  *“Third-party elements can take the form of cookies placed in your browsers. There is more to cookies than meets the eye, though.”*  Switch from this slide to the *Cookies explained quickly* video at <https://youtu.be/yoE9-tNvhRs> |  |
| Cookies video | **Cookies explained quickly**  Make sure the sound is loud enough for everyone to hear.  After watching the video check with participants that it made sense for them. |  |
| **What we can do about it** | |  |
| Slide 12. | **What can you do about it?**  *“Now you are better informed about what happens to your information on the Internet, how do you feel about it? Are there some types of information that really matter to you that you would want to protect? If you are concerned about the use of your personal information by others, here are some steps you can take.”* |  |
| Slide 13. | **Threat modelling**  (If not familiar with threat modelling, read the [EFF guide](https://ssd.eff.org/en/module/assessing-your-risks) before the session.)  *“When it comes to your digital privacy and security, what are you most concerned about? Threat modelling is a quick exercise that helps you conduct a risk assessment of your personal data.”*  Distribute the threat modelling exercise sheets (print the one from the end of this guide). Read aloud the 5 questions. The last question can also be phrased as: “What are you ready to change, how far are you ready to go to protect this data?” If participants need an example show them slide 14, which is an example of threat modelling for library staff.  Ask participants to go through the threat model questions as applied to them as individuals (in their personal rather than their professional lives). They can do it on their own or in pairs. They can use the list of personal data collected when using the Internet (from slides 8-9) and pick ideas from it. Give participants 5-10min to do this.  Use the flipchart. Ask participants for two examples of information they want to protect and have used in their threat modelling. Take the group through all the questions for both examples. For the last question, make sure you give different examples of how far someone might go to protect this information, from easy steps to a big change. | 15min |
| Slide 15. | **Basic tips and tools**  *“Now we’ve identified what we care about, let’s see how we can protect it… I’m going to explain and show you some basic tips and tools linked to passwords, using a browser and secure communications.”*  Explain that protecting personal information online is linked to keeping information secure. |  |
| Slide 16. | **Passwords and passphrases**  (If you need a refresher on the topic, read the [EFF guide](https://ssd.eff.org/en/module/creating-strong-passwords) before the session.)  Ask participants: *“How much do you re-use passwords? Raise your hand* [do it too] *if you use the same password for more than one thing. Keep your hand raised if you use the same password for more than 3, 5, 10…”*  Explain that re-using passwords is not a secure practice (even if we all do it!). Use examples from high profiles data breaches (Yahoo, LinkedIn…)  *“How easy would it be for somebody looking you up online to guess your password? How often do you change your passwords?”*  Mention password managers and other ways to securely keep track of all the different passwords you might have. Discuss how these would fit in your threat model (what if somebody cracks your master password?)  Move on to password strength. Explain the difference between passwords and passphrases, and why passphrases are now considered the better option (use the brilliantly simple [xkcd comic on password strength](https://www.xkcd.com/936/) if it helps).  Give an example of generating random passphrases simply by using a book. Explain diceware.  Explain to participants they should also beware of security questions, as someone more or less close to them might be able to guess their answers. The security best practice is to lie to security questions… | 7min |
| Slide 17. | **Browsers**  *“As we’ve seen earlier, there are so many things relating to individual information that happen within your browser… but there are also many small steps you can take to better protect your data. I am going to show you a few tools you can use and then we’ll have a play with them. I’m going to briefly cover browser history, private modes, two browser extensions and search engines.”* | 15min to slide 18 |
| Facilitator computer screen | **Browser history**  *“Your browser remembers where you’ve been. Some of the websites you have visited have placed cookies in your browser. For this reason it is good practice to clear your browser history on a regular basis.”*  Show where to find the cookies and history settings in Firefox and Chrome. Demonstrate clearing all browser data on Chrome. |  |
| Browser: Chrome | **Private browsing**  Show Chrome Incognito mode. Explain what it does compared to the “normal” mode.  Mention private browsing in Firefox, Safari and Microsoft Edge. |  |
| Browser: Firefox | **Browser add-ons**  Explain how Privacy Badger protects privacy and how it works.  Enable it on Firefox. Demonstrate what it does (e.g. go back to a website full of adverts you visited during the Lightbeam demonstration). Show where you can see how many trackers it has detected and how to manually adjust the settings. |  |
| Firefox or Chrome | **Search engines**  Explain how [DuckDuckGo](https://duckduckgo.com/) is different from Google. Demonstrate it – include telling it to show you results for the UK.  Briefly show [Qwant](https://www.qwant.com/) and its junior version. |  |
| Slide 18. | **Have a go yourself**  Ask participants to try at least one thing for themselves: review their browser settings, install or try one of the tools mentioned previously, compare the search or browsing experience when using one of those tools.  Participants with a laptop can:   * review their browser settings for cookies and browsing history; * clear their browser history; * set DuckDuckGo as their default search engine and have a play; * try their browser’s private mode; * install and test Privacy Badger.   Participants with a smartphone can:   * review their browser settings; * clear their browser history; * set DuckDuckGo as their default search engine and have a play; * install and try the DuckDuckGo app; * install and try the Firefox Focus app. | max. 10min |
| **Break** | | 15min |
| Tor Browser | **Tor Browser**  *“Depending on your threat model, you might prefer to use one browser over another. For example, I prefer using Mozilla Firefox over Google Chrome because Firefox is open source so everyone can scrutinise how it works and it is not made by a company whose business model is based on selling people’s data.*  *You can also choose to compartmentalise your browsing and use different browsers for different things. For example, to only use Chrome to logon to Google services, use Firefox to logon to your other accounts and use Tor Browser to search for and view information.*  *Despite what you may have heard reported, Tor Browser is just a normal browser!”*  (You may like to use the parallel from the Nos oignons [*Tor is for everyone*](https://nos-oignons.net/Actualit%C3%A9s/20180716_tor_est_pour_tout_le_monde/index.en.html) article.)  Show Tor Browser on laptop and explain what privacy-enhancing features are built within it. Navigate to a website and show how the Tor relays hide your IP address. | 3min |
| Slide 19. | **Secure communications**  *“A method to keep communications secure and private is to encrypt them: this way, even if they are intercepted they cannot be read without the encryption key to decipher them.”* | 7min to slide 21 |
| Browser: Firefox | **HTTPS**  Explain what HTTPS is.  You can use slide 20 (from EFF’s [*How HTTPS and Tor work together to protect your anonymity and privacy*](https://www.eff.org/pages/tor-and-https)) to go over how the Internet works again but this time with HTTPS − or switch directly to the Firefox browser.  Explain how to check a website uses HTTPS.  Show what a security certificate looks like on a website e.g. [www.librarieswest.org.uk](http://www.librarieswest.org.uk) Show an unsecure site e.g. the Northumberland & Durham Family History Society’s <http://www.ndfhs.org.uk> (navigate to Members login).  Explain what the EFF HTTPS Everywhere browser add-on does. Activate the add-on and demonstrate it if you know a website that has an HTTPS version but uses an HTTP by default! |  |
| Slide 19. | **Secure messaging**  Email encryption: mention PGP and email providers like Protonmail.  End-to-end encryption in messaging services: Signal, WhatsApp, secure messages in Facebook Messenger… |  |
| **What we can do for citizens in libraries** | |  |
| Slide 21. | **What can we do for citizens in libraries?**  Ask participants to use what they’ve learnt in the previous part and what they knew already to propose ideas of what we library staff can do to protect the privacy of citizens using libraries. Write their answers on the flipchart (try and group them in a similar way to what will be covered in this section of the workshop). | 5min |
| Slide 22. | **Transparency**  *“Transparency is about telling citizens how we handle their personal information when they use library services. It is one part of compliance with the General Data Protection Regulation (GDPR).”*  Explain what GDPR is and the principles it sets out for data protection. Explain what is required of libraries, including:   * information audits; * review what is collected and why; * legal basis for processing information; * how consent is obtained where necessary; * document findings of audits and reviews; * publicise (privacy notices).   *“All library services and their parent organisations will have undertaken work to comply with GDPR. However, library staff should be leading the way: we should not simply comply but make the effort to be fully transparent and explain to citizens in simple terms what happens to their personal information when they use the library.”* | 10min |
| Slide 23. | **RFID privacy notice**  Example of a privacy notice for RFID.  Refer to the BIC RFID privacy in libraries toolkit. Explain what privacy risks related to RFID the BIC working group identified and what their recommendations are. | 20min to slide 30 |
| Slide 24. | **Information we collect about citizens**  *“We should regularly review what information about citizens we collect and keep. We should ask ourselves:*  *- When / by what system is potentially personally-identifiable information collected?*  *- How long is that data stored?*  *- Why is it kept for that duration?*  *- What is it used for?*  *- How long is it actually used?*  *- How long is it realistically needed to deliver the service?*  *- Is there a way to securely anonymise the data?*  *- Are you giving citizens a choice regarding the duration their data is kept for?”*  Go through the questions using an example (when citizens join the library, when they borrow items…) |  |
| Slide 25. | **Data retention**  *“This is a non-exhaustive list of the areas to review…*  *We should use our review or GDPR information audits as an opportunity to actively take a stand to better protect citizens’ information. This means making sure that we do not collect information that isn’t necessary and that we do not keep it longer than we need. It’s a chance to create or update data retention policies.*  *For these areas on the list, how long should we actually keep this information? What’s stopping us from reducing that amount of time?”* |  |
| Slide 26. | **Threat modelling**  *“You can use threat modelling for the library service as well. It should help you understand what you need to protect and what options you may have.”*  Comment the example on the slide. |  |
| Slide 27. | **Suppliers**  *“Your systems and resources suppliers will likely pop up in your threat models. It’s worth speaking to them about the security basics you expect and the privacy features you would like to see.”* |  |
| Slide 28. | **Auditing supplier products**  *“It’s best practice to also audit your current systems. US-based librarians Alex Caro and Chris Markman have developed a quick assessment using these questions.”*  Read out the questions (you might like to adapt the vocabulary to UK terms when you read them).  *“As you see, for us some of these will be covered by GDPR compliance. But it’s always worth asking!”* |  |
| Slide 29. | **Library computers**  Give examples of privacy tools to offer on library computers (staff and public). Obviously these tools should be familiar to participants from the first part of the workshop… |  |
| Slide 30. | **Events for citizens**  *“Another aspect of what we can do is explain the issues to citizens and give them the knowledge and skills to protect their own privacy. You might choose to run events like CryptoParties, hold one-to-one digital skills session on privacy and security, incorporate privacy in your basic getting online courses, hold talks and film screenings…”*  Explain what CryptoParties are.  Mention working in partnership with citizens (e.g. members of the Open Rights Group, your local tech scene) to facilitate events, using materials like Tactical Tech’s Me and My Web Shadow resources (in hand-out) to help plan events content…  Idea of film screening: [Nothing to hide](https://www.youtube.com/watch?v=M3mQu9YQesk) documentary (available under a Creative Commons BY-NC-ND licence). |  |
| **What next** | | 20min |
| Slide 31. | **What next?**  Switch from this slide to the first question on the *What next?* Mentimeter presentation. |  |
| Mentimeter | **What is the first thing you will do to better protect the privacy of citizens when you get back to your library?**  To take part in the poll participants will need to go to the website www.menti.com and type in the number that is displayed at the top of the facilitator’s screen.  Read out the question. Briefly comment the answers appearing. |  |
| Mentimeter | **Is there anything you think would be difficult to implement in your library?**  Switch to the second question of the *What next?* Mentimeter presentation.  Read out the question. Comment the answers appearing. Involve the other participants in trying to find solutions for those. |  |
| Slide 32. | **Handout**  *“Other things you could do next is learn more for yourself or look up some of the resources for library staff I mentioned today. This workshop was developed for the Carnegie UK Trust’s* Taking a stand for privacy *project so an obvious resource to read is the guide of the same name! It explains in more details topics we covered today in the part on what we can do for citizens in libraries.”*  Distribute the Information and resources handout. |  |
| Slide 33. | **Conclusion**  *“After this workshop and now you know more about the topic, I hope you will take a stand for citizens’ privacy and champion the issue among your colleagues, library stakeholders and citizens using your library’s services.”* |  |
| Slide 34. | **Keep in touch**  If you’ve had badges made: distribute them to participants for them to wear proudly, at work and outside of work!  Encourage people to stay in touch with you (if that’s ok, share your contact details) and with each other. If there are Twitter users among the participants, ask them to use the #libstaff4privacy hashtag to talk about what they’ve learnt, shout about what they’re doing around privacy in their libraries, share interesting resources and articles on privacy. |  |

Handouts

1. Threat modelling exercise (one sheet double-sided)
2. Information and resources (one sheet one-sided)

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?**

**Taking a stand for privacy**

Information and resources

**Learn more – as a citizen**

* Data Detox Kit | Tactical Technology Collective

<https://datadetox.myshadow.org/detox>

* Surveillance Self-Defense | Electronic Frontier Foundation

[https://ssd.eff.org](https://ssd.eff.org/)

* Open Rights Group (UK)

[https://www.openrightsgroup.org](https://www.openrightsgroup.org/)

* Our data our selves | Tactical Technology Collective

Data and activism <https://ourdataourselves.tacticaltech.org/projects/data-and-activism>

**Do more – in your library**

* Choose Privacy Every Day | American Library Association

Resources <https://chooseprivacyeveryday.org/resources>

* Data Privacy Project − training course for library staff

Project by Brooklyn Public Library and partners [https://dataprivacyproject.org](https://dataprivacyproject.org/)

* Introduction to privacy − training for staff | Newcastle Libraries

Session materials on Newcastle Libraries' GitHub.

Short link <https://frama.link/ToonLibsPrivacyTraining>

* Leading the way | Carnegie UK Trust

Guide accessible via[https://www.carnegieuktrust.org.uk](https://www.carnegieuktrust.org.uk/)

* Libraries for privacy | Scottish PEN

“A digital security and privacy toolkit”, including ideas and tools.

<https://issuu.com/scottishpen/docs/libraries_for_privacy_toolkit_digit>

* Library Freedom Project − resources, information and advice

[https://libraryfreedomproject.org](https://libraryfreedomproject.org/)

* Me and my Shadow | Tactical Technology Collective

Training curriculum <https://myshadow.org/train>

* *Measuring library vendor cyber security: seven easy questions every librarian can ask*

by Alex Caro and Chris Markman

Published in Code{4}lib Journal, 2016 <http://journal.code4lib.org/articles/11413>

* RFID privacy in libraries | Book Industry Communication (BIC)

<http://www.bic.org.uk/161/RFID-Privacy-in-Libraries>

* Taking a stand for privacy | Newcastle Libraries

Workshop materials https://frama.link/TakingAstand

* Security Education Companion | Electronic Frontier Foundation

[https://sec.eff.org](https://sec.eff.org/)

* UK Information Commissioner's Office

<https://ico.org.uk/for-organisations>