Data privacy

Notes from 2 presentations:

UX Scotland conf presentation (Sage Bionetworks) + one webinar from SiteImprove about data privacy vs personalisation

https://sage-bionetworks.github.io/DesignSystem/just-in-time-permission.html

https://go.siteimprove.com/watch-now-privacy-vs-personalization

Privacy vs Personalisation – Siteimprove webinar

3 main steps:

- identify what you own *(for us: what partners own, and Company House too? Other stakeholders?)*
- assess its purpose
- be transparent about it

Identify your digital footprint

- Domains
- Personal data
- Files
- Pictures
- Cookies
- 3rd party scripts (GA)
- Share widgets
- forms

Gain control

- Why is it there?
- Do we still have a reason to keep that data?
- Do we have a permission to keep and use that data
- Can we do it in a better way using less
- Do we know when to delete that data
- Is it collected on a secure site with a certificate

Be transparent

- Let visitors make informed choice
- Use cookies banners
- Cookie notice or privacy policy
- No prechecked boxes when using forms
- State what data will be used for
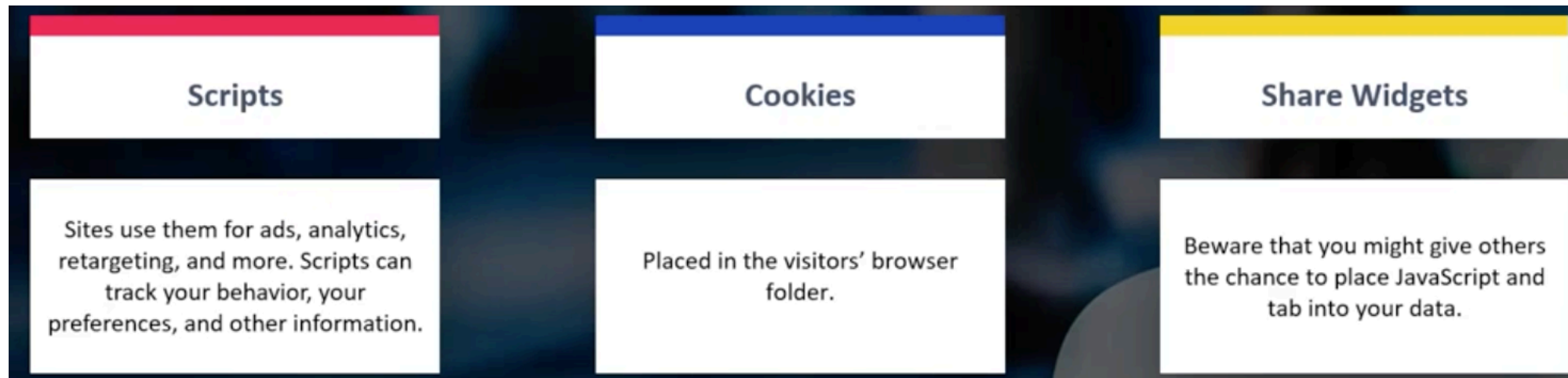- Use a language that you will understand yourself

Step 1:

Get the full overview to identify the vulnerabilities around data privacy

- Collecting lists and getting an overview is the right way to do it.
- Get an overview of all your domains

Check your 3rd parties:

Who else is tabbing into your visitors' data

Scripts	Cookies	Share Widgets
Sites use them for ads, analytics, retargeting, and more. Scripts can track your behavior, your preferences, and other information.	Placed in the visitors' browser folder.	Beware that you might give others the chance to place JavaScript and tab into your data.

What you should consider:

Avoid leaks	Third Parties	Forms
• Control access to subscriber data • Have processes in place to avoid manual uploads of files with personal data	• Why? • Do you need consent? • What data do you need? • How long do you need it for? • Did you inform the user?	• Consent needed? • No pre-checked boxes • How long will you keep the data? • Who is it shared with? • HTTP or HTTPS – is the site secure?

Consent:

- Positively Opt-in
- No pre-ticked boxes
- Clear, plain language
- Make it easy to withdraw consent

What you should consider:

- **Make data available**: anyone should be able to get access to their data and get it removed within 30 days

- **Third parties**: cookie banner, privacy notice

- **Forms**: make it easy to make a decision as a user. Most are willing to share their data if you're honest *(might not be true for SE users)*

Tracking and personalisation:

- Increase transparency

- Consider data privacy from all aspects

- Understand visitor behaviours

- Keep unnecessary third parties out

UX Scotland presentation (Sage Bionetworks)

This is based on research they have done specifically for their portal, when individual join a digital study. They work in biomedical research but what they found could be re-used for other contexts like MyAccount.

Note: this is an ongoing work, a lot of links don't work …

https://sage-bionetworks.github.io/DesignSystem/just-in-time-permission.html

Just-in-time permission

Apps usually bombard users with permissions screens requesting access to their camera, microphone and location data all at once.
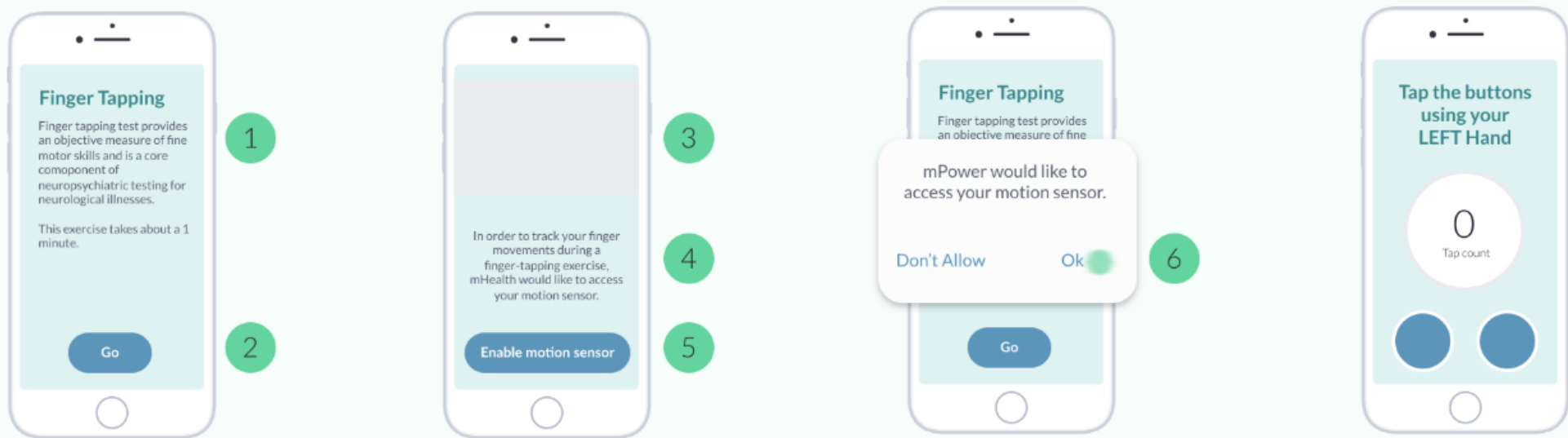
The appropriate access permissions should only be asked right before the user needs to complete a task requiring this type of data.

Just-in-time permission lays the groundwork for engagement.

The participant is provided with sufficient context to make an informed decision to allow / deny permission when it becomes required for an study-related task.

The just-in-time permission lays the groundwork for a long-term engagement by fostering mutual understanding and trust.

Best Practice: Just-In-Time Permission

Finger Tapping

Finger tapping test provides an objective measure of fine motor skills and is a core comoponent of neuropsychiatric testing for neurological illnesses.

This exercise takes about a 1 minute.

Go

1

2

In order to track your finger movements during a finger-tapping exercise, mHealth would like to access your motion sensor.

Enable motion sensor

3

4

5

Finger Tapping

Finger tapping test provides an obiective measure of fine

mPower would like to access your motion sensor.

Don't Allow   Ok

Go

6

Tap the buttons using your LEFT Hand

0

Tap count

---

1 Call out the to-do task to be completed, and explain why it is relevant to the research topic.

2 Show the permission request only after the participant decides to launch the task.

3 Show visual(s) of the task to be completed.

4 Name the the specific permission request and explain why it is required for the task.

5 Add a call-to-action button to lead the participant to willfully turn on the permission.

6 Pop up the actual permission dialog only after the walkthrough.

"I hear you. The finger-tapping test is used to assess the progression of my Parkinson's disease. It requires me to turn on the motion sensor to track my finger movements. The app explains it well so I would like to give such access. Cool, since now I understand what's happening, let's do some finger-tapping."

What to prepare?

Step 1   **Send just-in-time permission request only when a relevant tasks comes up.**

Place the permission request only at the moment when a participant wants to complete a relevant task. [iOS] -> consider that this could take place during the ('prepareForSegue')

Step 2   **Explain just-in-context how the permission is required for the task.**

Provide a walkthrough of what task the participant is required to accomplish, how the task connects to the scientific research, and why the permission must be turned on in order to gather the data.

Step 3   **Use texts and visuals to demonstrate a real example.**

For example, show a visual of the finger-tapping exercise and explain the application must have the permission to use the motion sensor in order to track finger movements.