Panel 1: How developers use data

The impact of AI

- AI is a game changer, but who controls the data? AI will bring benefits - fear of missing out (FOMO) effect.
- Already great, but still in many ways very limited. Limited in handling the data. AI works in a similar way compared to human brain - limitations.
- Risks in larger ill-minded deployment of generative AI are in the fields of automations and system level operations rather than conventional Nigerian letter type of scams.

Face recognition technology

- How and when will this be deployed in Finland?
- With dozens and hundreds of surveillance cameras – who owns the data?
- In countries like China, they deploy and utilise data for other governmental purposes – data is collected and stored, then used when an appropriate situation arises.

Regulation

- A strict European approach to regulation might hinder innovation compared to a US approach that is more market-driven.
- Simply making software work isn't enough. Regulations must be considered, which will require resources. This presents a challenge for smaller developers.

The end user perspective

- The end user has no easy way to estimate the security of a web page or any application.
- Cookies across websites are accepted by default by the end user.
- From an end user perspective, there needs to be more control rather than simple actions like ‘Allow’. Who has the actual motivation to set up a negative selection as default on various user interfaces (Google is about to update its Chrome browser on this functionality.)

How to best develop solutions

- When building new software solutions, there are technical ways to limit access, enable transparency and give power to control the data.
- Securing the network should be prioritised over individual computers/devices.
- Complexity will simply complicate things unless security is incorporated in design.

Panel 2: Being regulation-compliant

Getting to know your regulations

- Learning standards and regulations will enable you to develop a solution in a feasible direction.
- Also be weary of the “other stuff” – understand the regulations of specific industries such as health care or the banking sector.
- GDPR and other standards and regulations are friends. They are benefitting solutions on the business side as well as customers.

Trusting the big tech giants

- For developers that work with services such as AWS, we inherently trust that these giant organisations are complying with the regulations.
- Whilst this a positive consequence, we should be weary. Are we also handing over part of a business opportunity to services like AWS? If we have data hosted on these giant systems, does that make us a bigger target for criminals?

Legal and standards expertise

- There is a lack of expertise in certain areas of regulation.
- Should developers be talking to lawyers more to ensure that what they are doing is by the book?

Cookies and privacy statements

- Cookies are not some force of nature, they are simply used based on the money to be earned.
- Privacy statements must be available on solutions, regardless of the deployment of cookies.
- GDPR can also be used to reason with various stakeholders when discussing projects.

Questions we should be asking when developing solution?

- If a data owner requests to see the usage of their date with multiple simultaneous requests, can automation functionalities provide a solution?
- Can we develop solutions where scripts are not collecting data? There would be practical implementation challenges, including the loss of useability. However, this could still be an opportunity for someone.
- Given the Chromebook approach with its security motivation, do we need to move away from browser-based apps?
- Native apps are less controlled (whereas browsers are constantly tested) – does this make them less secure inherently?