



ukgovcamp

Session: 1

Room: Committee Room 3&4

Session title :threat models

Session leader : Jonathan

Volunteer to continue conversation after :

Notes taken by : Raj

Notes

Chatham house rules

Definition - what do people understand as a threat model?

Group had a brief discussion, thinking about how we define threats to our systems. Who wants access, to what, and how might they do it?

Group talked about mechanisms for reducing data being vulnerable - both less collection, and also models like those in *Platformland* that give the user more authority about data being shared.

Group reflected on how we balance the value of data and the potential risks. Eg. knowing how many drug users are in an area allows us to think about business cases for better addiction prevention...but equally there's a risk that a bad actor could use that data to persecute them. At the end of the day, what does society think about the balance/trade-off of more data for better services? Example of Tesco clubcard was pointed out, where you might trade data for 50p off a sandwich!

Similarly personalisation and digital ID: group talked about how they felt about government being able to identify when you've proved your age in a sex shop, for example.

Group touched on the potential for an authoritarian or populist government (regardless of political leaning) to use over-collected data for 'bad purposes'. Legal frameworks can be constructed by the government with relative ease, so do we have a duty to build only those services that meet the immediate need? No easy answer here - civil servants serve the government of the day, and can't just 'not' do things.

Are there tools and systems to reduce risk to citizens and ourselves