Nov 29 2016 - Design Crit Notes (Privacy)

https://wiki.fluidproject.org/display/fluid/%28Floe%29+Privacy+Needs+and+Preferences

https://www.w3.org/TR/P3P11/

https://myshadow.org/

Is this contextual?

How would we enforce this?

- Can't enforce, but can inform user when prefs not being met
- Advocacy - allow user to create a machine-readable policy

Where would user come across this?

- Like first discovery? user-driven , ubiquitous
- Start with stories - which of these do you relate to?
- Nested circles at the centre
- Eg. sending email

- Timeline assumes we have access to this information
- Data that we explicity share vs. inferred data (derived from your activity) and sharing of inferred data
- Inference that is happening that is not transparent - about what the data will be used for
    - How do you get access to this?
    - How do you present this to the user?
- "We don't have access to that but our algorithms do" e.g. Amazon employees may not have access to your data, but algorithms can present you with suggestions etc.
- Who has access? What kinds of decisions are being made? Can we and/or do we need to surface this in the UI?
- Customer-based privacy maintenance
- Make it game-like, story-based
- Discrepancy hook - i want this, they are giving me that
- The tool has to have access to your personal data?
    - For timeline
    - For other granular choices
- Companies that will opt-in
    - Levels of participation
        - Just tell users we exist, link to us, somewhere in app/site
        - Offer us as an option whenever user is editing app/site's own prefs
        - Include us in notices of privacy policy changes
        - Show conformance/discrepancy whenever user logs in
    - No opt-in: we give a warning to user (incentive for app/site to opt in!)
    - Also considering what is possible in the future
    - Privacy to become a competitive advantage
- Aggregation of all the data in a timeline - could present security concern as a potential point of attack
    - Can we collect info about what you're protecting (or not protecting) but not the value itself?
    - Can we "aggregate" the data superficially (not actually)?
    - Can we take a kind of hypothetical approach like Me and My Shadow - if you are using these devices, making these choices etc then it is probably that this information is being tracked about you
    - 1. The richer and more specific your personal privacy policy is, the more sensitive it is e.g. if you are blocking medical information, it could be inferred that you have something to hide - and by making it less granular it could be limiting
    - 2. Is there a way to approach this differently such that the user doesn't feel that we are another place that is collecting data about them?
    - We are not actually collecting the data about the user?
- A partnership - with the provider - a speculative exercise - we don't want to aggregate data, we assume a balanced partnership
    - E.g. provider specifies a token rather than the actual data - the event not the value
- Could provide a rating for different sites etc re: privacy
- Once it's gone you can't get that data back
- A hypothetical approach - the tool reveals the policies of the services rather than specifically setting preferences?
- A game - create a persona and interact with services - experience what happens
    - "SimPrivacy"
    - Export the outcome as your privacy preference?
- Snapsets / settings of someone you know - sharing

Next Steps

- More of a first discovery-like approach
- Create a simple UI with the following:
    - Begin with generalised timeline OR hypothetical exercise/mapping, with links into
    - simplified preference setting tool/UI
        - Return to timeline or mapping to see changes based on prefs set
    - Beginnings of personal privacy policy output?
- Timeline could link into app-specific privacy settings? And from there, prompt to use preference-setting tool to avoid having to set app-specific privacy settings in the future?
- consider both the speculative (full, complex) design (like current wireframes with timeline etc) as well as the simplified / what is realistic today
- in simplified case - what is bare minimum? the bottom line? "5 things"
    - what does user want to "say" to provider (i.e. privacy preferences) - what can they opt-out of
    - what does user want to know from provider (i.e. what info is being used and why?)