Jan 31, 2017 - Privacy Design Crit Notes

Wireframes - Privacy Storybuilder

- create a story “based on you or someone you know” - perhaps change this wording so that it doesn’t convey the message that you are setting this up for someone else — perhaps change wording to “my situation”/“me” vs. “explore”
    - intention here is to allow the possibility of keeping it removed from personal experience if desired
- would be good to be able to trace directly back from your selections to the outcomes (mapping)
    - suggested possible way of mapping: https://docs.google.com/drawings/d/1S2plkB9GMibHyrqTJ6lBOzqfl4id0Np22VErZXRCDdk/edit?usp=sharing
- experience with seniors - they know what they’re concerned about already
    - some are using online services but are worried
    - some avoid online services because they’re worried
    - perhaps an alternate approach would be to focus on the concerns up front (e.g. browser history tracking, ID theft etc), or the specific activities (e.g. on-line banking, or on-line shopping)
    - we could also create multiple intro animations - each that addressed a different concern
    - based on your activities - these are some things you might be worried about
    - also they are very peer-expert oriented - what are those they trust doing? then they’ll do the same
- what about those who may be using other means to protect their privacy, like encryption? or ways of blocking political activism traces on FB
    - can we include links to other resources (e.g. things that aren’t covered by privacy preferences)
    - consider scenario where someone may be using full encryption at O/S level, but then goes to public computer and doesn’t have it available
    - perhaps this is where “backup” privacy preferences could help
- what do we mean by “public” - public computer vs. public wi-fi?
    - i.e. we need to be clear - “public computer” vs “public internet use”
    - what are the different concerns for using public wifi e.g. at Starbucks, vs using your data while at Starbucks? which is better?
- weighing the benefits
    - perhaps we could present typical minimum requirements for using various services
- what do we mean by “as-needed” re: location tracking? i.e. who decides?
    - in this case we were considering the existing setting (in iOS) that allows location tracking only when app is in use

Intro Storyboard

- we need to be clear about HOW the data is being used
    - in aggregate? anonymously?
    - can we make real-world comparisons/analogies? e.g. traffic counting (anonymous)
- cookies are just one mechanism by which our data is traced
- need to consider also that cookies don’t store the data, rather they provide a link from ID to data stored in a server, so deleting cookies doesn’t mean that the data is deleted
- consider Evercookie https://en.wikipedia.org/wiki/Evercookie - “By storing the same data in several locations that a client can access, if any of the data is ever lost (for example, by clearing cookies), the data can be recovered and then reset and reused.”
- how do we consider “value” of the data
    - value to service (not known, not transparent)
    - value to user
    - self-defined
- we talk about the users’ “right to be forgotten”, but does a service have a “right to remember” if the user has freely given the data
    - need to consider that most data is given unknowingly

Links Shared During Crit

Wireframes: https://files.inclusivedesign.ca/index.php/s/KkU4vnFur5H5WQ8#pdfviewer

Privacy Preferences List: https://docs.google.com/document/d/1zskKCkLVRHqLYgcWigMyu1i797tOr7x_JgACOGp6ZN0/edit?usp=sharing

Privacy Tips for Newbie Activists: https://news.ycombinator.com/item?id=13516116

Browser Fingerprinting https://www.reddit.com/r/privacy/comments/51nmve/a_solution_to_browser_fingerprinting/
Even if someone has taken precautions to control their privacy, their browser may be revealing unique information that could indentify them uniquely.

This is the EFF tool which tests your browser finger print: https://panopticlick.eff.org/