(Floe) Privacy Needs and Preferences

Project Description: Understanding, Discovering and Asserting Personal Privacy Preferences (UDAPPP)

Background

Individuals most vulnerable to the misuse of private information include persons with disabilities (e.g., denial of insurance, jobs, services), persons who are aging (e.g., senior's fraud) and other individuals who face discrimination, stereotyping, marginalization or exclusion. This diverse group also has the most to gain from smart services that respond to personal data. Any privacy strategy must consider this growing group of consumers.

Systems that request personal information generally ask the individual to either accept or reject a fixed privacy policy (e.g., as seen in service contracts, license agreements or surveys). Rejection entails rejecting the service or product. There is generally no opportunity for the individual to question or adjust what information is given to whom and for what purpose; or option to negotiate conditions, specify time limits, or modify the privacy policy as it applies to them.

The project provides individual privacy preference exploration, creation and editing tools, (co-designed by diverse community participants), to gain informed individual control over personal data. A community-generated list of possible personal privacy preferences is used to form the basis of a proposed International Standards Organization (ISO) privacy preference interoperability standard.

The resulting strategy supports a user-specific privacy policy that is compliant to Canadian privacy laws and addresses the requirements of both the organization seeking access to information and the individual providing informed consent.

Goals of the Project

- Design an interface exemplar for discovering, exploring and choosing privacy and identity management preferences
- Leverage ISO 24751* (Access for All) to discover, assert, match and evaluate personal privacy and identity management preferences
    - engage relevant stakeholders in developing a proposed privacy and identity management preference application profile as a New Work Item

*ISO 24751: a standard to support processes that match unique individual needs and preferences with resources that meet those needs and preferences

How it Will Work

- a single, personalized interface to understand and determine a privacy agreement that suits the function, risk level and personal preferences
- private sector companies would have a standardized process for communicating or translating privacy options to a diversity of consumers

Action Items

- implement a transparent online workspace to recruit input from stakeholders
- hold facilitated group discussions, co-design sessions and test scenarios to map out potential plans and evaluate feasibility of the plans

- draft a New Work Item (NWI) proposal to attach to ISO 24751
- create a prototype user experience exemplar

Working Documents

Inclusive Design for Privacy - Working Doc (Google Doc)

Key Points for Tool Introduction/Animation

DEEP 2016 Privacy Discussion Summary (Google Doc)

Privacy and Sharing Preferences List (Google Doc)

Brainstorming a Personal Privacy Policy (Google Doc)

Examples of Misuse of Personal Data (Google Doc)

PIPEDA and Privacy Preferences Design

- Original One Page Brainstorm

Privacy Preferences Information Model (Google Doc)

PIPEDA Audit

Meetings

Mar 28, 2017 Design Crit Notes (Privacy), based on the interactive prototype

Feb 17, 2017 Accessible Prototyping

Jan 31, 2017 Design Crit Notes (Privacy), based on these wireframes

Dec 21, 2016 Privacy Preferences Meeting

Dec 6, 2016 Design Crit Notes (Privacy), based on these wireframes

Nov 29, 2016 Design Crit Notes (Privacy), based on these wireframes

Sept 28, 2016 Privacy and Sharing Preferences Brainstorm

Sept 8 2016 Privacy Discussion Meeting Minutes

August 25, 2016 Brainstorm Session Notes

Deliverables

Deliverable 1: Feasibility Report

- Feasibility of Extending ISO 24751

Deliverable 2: New Work Item

- Privacy Preferences Information Model
- ISO 24751 New Work Item
- ISO 24751 Committee Draft

Deliverable 3: Co-designed Prototype

- User interface exemplar
- Inclusive Design for Privacy
- Early wireframes (showing Timeline and reflecting PIPEDA's Collect / Use / Disclose levels of privacy)
- Privacy Needs and Preferences List

Deliverable 4: Risk, Security and PIPEDA Assessment

- PIPEDA and Privacy Preferences Design Assessment
- Privacy Preferences Design: Risk and Security Assessment

Deliverable 5: Proposal for Next Steps

- Next Steps for Personal Privacy

Research and Resources

Building Consentful Tech - zine

Usable Privacy

Privacy by Design

Media Post April 26 2017 - Researchers say that a massive 47% of consumers are put off digital channels by privacy concerns.

Your Smartphone is a Civil Rights Issues - TED Talk

The Electronic Frontier Foundation

Me and My Shadow Project - Take Control of Your Data

Me and My Shadow - Tracking, So What?

Me and My Shadow - The 8-Day Data Detox Kit

The Glass Room NYC - Looking into Your Online Life

Office of the Privacy Commisioner of Canada - Web Tracking with Cookies

Understanding Cookies (Microsoft)

The Watchers augmented board game

http://uxmag.com/articles/privacy-and-personalization-can-coexist-through-good-design

http://catalogue.projectsbyif.com/

The Platform for Privacy Preferences Project (W3C)

Designing a Privacy Preference Specification Interface - A Case Study. Cranor, L.F.

User Interfaces for Privacy Agents. Cranor, L.F., Guduru, P. and Arjula, M.

Usable Privacy Policy Project

The Privacy Bird !

https://privacy.google.com/#

Anne Cavoukian U of T Alumni Presentation - Joseph's notes and link to Anne's slide deck

International Council on Global Privacy and Security by Design

Online security tips from Y Combinator

NYPR podcast: The Bookie, The Phonebooth, and the FBI

The Quantified Worker - Harvard University

Deceived by Design - How tech companies use dark patterns to discourage us from exercising our rights to privacy

The Internet of Things - Examples

Leon's - Project Smart Furniture

Amazon Echo Look

Examples of "Best Practices" for Protecting Users' Privacy

Questions (from initial brainstorming session)

We want to address the following three questions:

1. What are the possible privacy preferences someone might have?
2. How is private information being used currently?
3. Who are vulnerable in this context?

As part of answering these questions, we want to discuss:

- what constitutes private information,
- what is being gathered and for what purpose,
- what are the conflicts between privacy requirements and what is actually being done today, and
- are there constraints in fulfilling privacy wishes.