Involving Seniors in Developing Privacy Best Practices:
Toward Responsible Development of Social Technologies for Seniors

BEST PRACTICE GUIDELINES

Dr. Andrea Slane, Dr. Isabel Pedersen, and Dr. Patrick C. K. Hung
Ontario Tech University

March, 2020

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

I. TAKE AWAYS FOR PRIVACY BEST PRACTICES:

In general, privacy best practices for seniors track closely with privacy best practices for all consumers. However, some modifications were suggested both via the themes in the participants' responses in the focus group interviews and in the workshops. The following take-aways emerged:

1. Seniors require **clear, simplified instruction** on what their data protection options are in the course of choosing whether to use a device for a specific function.
    - Instruction should come from a trusted source.
    - Instruction should come with live support to see seniors through the process.

2. Seniors should have access to **clear, simplified guides** that help them explicitly reason through the benefits, burdens, and risks associated with using a device or application for a particular function.
    - Guides should come from trusted sources.
    - Guides should come with live support to assist seniors through the reasoning process.

3. Seniors should be **recognized as autonomous individuals, with their own particular affinity level for technologies, and their own privacy risk tolerance.**
    - Seniors should not be assumed to share a uniform orientation toward the use of social support technologies, nor to the risks associated with using them.
    - Materials developed for seniors should allow for a user to reflect and self-identify their own privacy profile.

4. **Seniors do not all reason along the same lines when it comes to how best to approach privacy protection**.
    - Most seniors conform to dominant privacy protection principles that encourage transparency of data handling practices and meaningful choices for users to provide or withhold consent.
    - Some seniors foreground clearer rules about what the limits are to reasonable data handling practices for devices and applications aimed at senior users, which would alleviate some of the burdens of needing to understand and make active choices.

5. Seniors, like others, are influenced by **both idealized visions of what technology can do, as well as by disquieting news stories about privacy breaches and violations**.
    - Materials addressing how to protect privacy should acknowledge these influences and help seniors to reflect on them and what impact they might have on their decision-making.

6. **Seniors are often cast as a particularly vulnerable demographic** in cultural representations, which are often reinforced by younger family members who do not trust them to make wise decisions about privacy protection.
    - Materials for seniors should avoid reinforcing disempowering narratives.

The remainder of this document sets out the methodology for the workshops that contributed to these take-aways, and the findings gleaned from those workshops. While the workshops aimed to gather targeted input from seniors regarding privacy best practices, the means of gathering this input from seniors proved difficult to design. Nonetheless, when read in conjunction with the focus group findings report, the study has provided empirical substantiation for the above take-aways.

II. METHODOLOGY

Upon completion of the focus group phase of this project[1], we held two exploratory workshops aimed to elicit more specific input from seniors about privacy best practices. The workshops mirrored the conceptual design of the focus groups, with the first half exploring privacy concerns and solutions in relation to present day anthropomorphic social support technologies (digital assistants, but with more complex scheduling and coordination capabilities). The second half then focused on future anthropomorphic social support technologies (personal robots, imagined as capable of sophisticated human-like conversation). While in the focus groups we showed participants promotional videos for personal robots currently or soon-to-be on the market, given the limitations of these current robots we chose to explore seniors' attitudes toward more idealized future possibilities. This method enabled participants to delve more deeply into how they envisioned both the benefits and drawbacks of future social support technologies.

Two workshops were held in January/February 2020 at two of the Ontario senior centres that had hosted focus groups in summer, 2019. Eleven (11) participants took part in the workshops, all of them women, with a median age of 70. Five (5) of those participants had previously taken part in the focus groups. This meant that roughly half of the participants had discussed social support technologies in the extended focus group format, and had also seen the promotional videos, albeit six months earlier. The other 6 participants were new to the project and had not had an opportunity for much discussion of these technologies, nor had they seen the promotional videos.

A. Exercise 1: Fictional Character Creation.

Participants in the first workshop engaged in a short exercise to devise a fictional senior citizen who would serve as the character to keep in mind when providing views on privacy and data protection related to social support technology use. The group constructed a female character in her 70s, with mild forgetfulness, mild dementia, and occasional days with arthritic pain. For social support, the character had daily phone calls from family or friends, and at least monthly in-person visits, with family living within a few hours' drive. The character also is somewhat socially engaged, leaving her home at least once a week for an activity. The purpose of creating this fictional character was to get the workshop participants to think at least roughly about a person with common needs and circumstances, rather than the broader range of possibilities that came from participants responding based on their own current situation, as they had in the focus groups. Workshop 2 participants then were given the same fictional character attributes on whom to base their thinking as they went through the exercises.

B. Exercise 2: Benefit and Comfort Level Ranking Exercise.

Exercise 2 involved filling out a form ranking benefits of specified functions and ranking comfort level with related data processing practices. In the Digital Assistant (Scheduler) exercise, four types of scheduling and reminders were proposed:

- Medical Appointments.
- Social Support Coordination.
- Social Activity Coordination .
- Daily Exercise.

[1] See Focus Group Findings report for this study.

In the Personal Robot (Conversationalist) exercise, four types of conversational purposes were considered:

- Companionship.
- Encouragement.
- Reassurance.
- Safeguarding.

The forms for the Digital Assistant (Scheduler) provided examples of the type of information that would need to be collected in order to perform the function, and what the user would get in return (e.g. coordination of best time to call a relative; or tracking for lack of out of house activity). For comfort level, participants were given information about where the data would come from (e.g. input directly from the user, a caregiver, service provider or internet search).
The forms for the Personal Robot (Conversationalist) similarly provided examples of the type of information collected (e.g. interests, family photographs, recordings of life stories, recurring concerns), as well as sources of that information.
Participants were told that they could assign the same benefit rank to more than one type of function (1 being most beneficial, 4 least beneficial); and the same comfort level (1 being most comfortable, 4 least comfortable).

C. Exercise 3: Benefits/Burdens/Risks Exercise.

Participants were given a stack of colored sticky notes and tasked first with writing down any benefits that fictional character could gain from using a Digital Assistant for the above complex scheduling, tracking, and reminders. In the second half of the workshop, participants did the same exercise with regard to personal robots used for the four types of conversation purposes (companionship, encouragement, reassurance, and safeguarding).

D. Exercise 4: Privacy Concept Bank Exercise.

Participants filled out forms answering yes/no questions and identifying reasonable information processing practices related to the specific functions for both Digital Assistants (Scheduler) and Personal Robots (Conversationalist), according to the four categories of functions for each established in Exercise 2. The forms aimed to cross-reference the following concepts:

- ***Three major privacy principles:***
  - Transparency
  - Meaningful consent
  - Reasonableness (in the absence of choice)
- ***Six major personal data handling loci:***
  - Personal information processing
  - Personal information sharing
  - Primary and secondary purposes
  - Security
  - Retention
  - User Support

III. LIMITATIONS

The workshop format proved difficult to conceptualize, insofar as the workshops hoped to elicit more concrete input on privacy best practices. The two scenarios for a fictional character approach (present and future - or more accurately, near future and far future) have potential to produce complex data about how seniors perform and imagine how a somewhat vulnerable senior would or should think specifically about data protection issues. However, these are complex concepts that require a fair bit of understanding about both privacy principles and data handling practices. We debated allowing time for discussion rather than individualized forms. We settled on forms because of the formal nature of what we were looking for, and feared that open discussion would lead to less specific feedback. We adapted the forms between the first and second workshops in order to test if they could produce more consistent outcomes. Further testing would be necessary to determine which forms worked best. The following limitations were evident:

- The stamina of participants to engage in conceptually difficult work varied widely.
- Some participants moved far more quickly through the exercises than others.
    - However, speed did not necessarily correlate with carefully reasoned responses.
- Some participants expressed their lack of familiarity with the concepts, or even the terminology.

A contingency plan would have been appropriate, for instance getting a Research Assistant to act as a scribe if a participant grew weary. Nonetheless, given that many of the participants had no previous knowledge of data protection principles and concepts, all participants at least tried to get through the exercises and provide valuable input.

IV. WORKSHOP FINDINGS

The workshops were designed to elicit responses from participants to specific data protection issues that arise in the course of considering whether to use technology for social support, now or in the future. We experimented with the methodology, made adjustments to the format between Workshops 1 and 2, and given the small sample size and pilot approach, the findings are very provisional and exploratory.

The main insights are:

- Participants think about privacy orientations according to a range of Privacy Profiles across present and future devices;
- Benefit/Comfort Level consensus indicators were variable, but tended toward the high benefit and high comfort level with data collection and sharing;
- The Benefits/Burdens/Risks identified often cut across present and future devices but were somewhat more positive about the benefit of robots;
- Transparency and Meaningful Consent tend to show a high level of consensus indicators across present and future devices signaling strong privacy protective stances;
- Reasonableness consensus indicators also tend to cut across present and future devices, but reflect different patterns of reasoning.

A. Privacy Profiles Across Devices.

Some participants displayed more privacy protective orientations than others. Three prominent profiles were:

1. **Risk Averse** – High level of privacy sensitivity. If designating a function as highly beneficial, then also requiring a high level of privacy protection.
2. **Cautious** – Makes distinctions between low, medium and high benefit functions and assigns a level of required privacy protection differentially – though mostly in the medium-high range.
3. **Trusting** – Many functions deemed highly beneficial and lower levels of privacy protection required. Higher level of trust placed in companies.

B. Benefit/Comfort Level Consensus Indicators Across Devices.

Consensus indicators were very rough in the data. Some functions showed clear consensus about the benefit, and others showed no consensus among participants - which may be for a variety of reasons, most likely: Flaw in the study design -- ranking options forced some variations; Profiles -- reflect different ways of thinking - elaborated in the privacy profiles above; and Actual -- true differences of opinion.

1. Digital Assistant (Scheduler)

- **Medical Appointment reminders:** high benefit, and high comfort with input by users. No consensus for input by others.
- **Social Support Coordination:** high benefit to reminders to call family/friends after a pre-set amount of time; no consensus on the benefit of tracking or coordinating social contact frequency, and no consensus on comfort with how required info would be inputted or monitored.
- **Social Activity Coordination:** high benefit for suggestions of activities and adding to the calendar; no consensus for benefit of tracking for lack of out of house activity. High to Medium comfort level with user input, internet searches, and monitoring of not leaving the house.
- **Daily Exercise:** high benefit to prompting to exercise if no exercise noted, and medium benefit to tracking exercise history; no consensus on prompting for a user to input reasons. Medium comfort level for user input of exercise, logging that input and sharing with designated others; low comfort with monitoring directly by camera.

2. Personal Robot (Conversationalist)

- **Companionship:** high benefit to providing stimulating conversation and learning new things, no consensus on entertainment; medium to the high comfort level on searching Internet for new material and retaining records of previous conversations, no consensus on retaining conversation logs.
- **Encouragement:** high benefit to receptive listening (even if repetitive), no consensus on prompting to tell and records life stories or memories; High and medium comfort level on input from a user or user's family members, searches on Internet for life story prompts, and sharing recordings with designated recipients; no consensus on comfort level with recording life stories.

- **Reassurance:** high benefit for receptive listening to concerns, offer to report concerns to designated people, and provide information to assuage concerns; high comfort level with recording concerns and sharing them with the designated recipient, as well as providing present information to address repetitive concerns; no consensus on searching internet for helpful information (e.g. scam checker).
- **Safeguarding:** High benefit for monitoring for falls, lack of movement, lack of verbal response; high comfort with sending alerts to designated recipients if no response and to medical service if instructed or if no response.

In sum:

- Many participants designated both a high benefit to be had from using devices for the specified social support functions, and a high or medium-high comfort level with the information gathering and sharing that would need to take place to perform that function.
- Where there was no consensus, this tended to be because certain participants consistently signaled less comfort with data sharing with others (family, medical service providers) or for allowing the device to search the Internet (in other words, participants with risk averse privacy profile).
- While we caution against drawing too much from the limited data, it is interesting to note that the **comfort level for collecting and storing information on a personal robot was somewhat higher than on a digital assistant.** This finding would merit further inquiry to verify and probe the reasons for this distinction:
    - Lack of trust in current companies offering digital assistants as compared to imagined future companies offering personal robots.
    - Idealized conception of future personal robots, versus more realistic conception of current digital assistants?

C. Benefits/Burdens/Risks Across Devices.

The table below compares the terms that Workshop participants used to describe the benefits, burdens and risks associated with the fictional character using either a Digital Assistant or a Personal Robot for the tasks set out in the previous exercise. Some terms were reclassified if they were written into the wrong category.

1. Benefits

- Shared benefits across both devices included **practical assistance** (e.g. reminders); additional practical assistance for robots included “can help you solve some problems” – implying intelligent interaction;
- Robot benefits included **more direct social support arising from conversational functions**: social engagement, psychological support, companionship, and mental stimulation.

2. Burdens

- **Shared burdens across both devices**: learning to use and maintain, the burden of entering information, technical challenges; lack of resources to purchase and maintain, and lack of trust.

3. Risks

- **Shared risks across both devices** included:
  - Over-reliance on technology (by both users and caregivers;
  - Technical concerns (e.g. not knowing how to fix errors, frustration);
  - Privacy and security concerns
    - **However, the list of privacy and security concerns was longer for digital assistants, especially with regarding to hacking, scams, unwanted surveillance**.
    - Future research should explore whether lower concern about such privacy breaches arises from the idealization of future robot devices.
  - Ethical concerns, such as replacing human contacts, accelerating rather than slowing cognitive decline.
- **Concerns unique to robots:**
  - Social and emotional attachment to the robot – risk of feelings of loss if removed or malfunctions, risk of misunderstanding needs/wants of user, risk of reducing a variety of social interactions and activities.

D. Transparency, Meaningful Consent and Reasonableness Consensus Indicators Across Devices

The Privacy Concept Bank exercise included Yes/No questions regarding transparency and meaningful consent, and either line drawing or option circling to point toward what data handling practices the participants considered reasonable.

1. Transparency.

- Phrased as a yes/no question about whether the fictional character needs to know how his/her information is being handled at each of the data protection loci elicited a strong trend toward **YES across all loci and across both devices.**
- A second yes/no question probed whether the fictional character would still use the device if they did not know or understand how their information was handled at the loci elicited a strong trend toward **NO across all loci and across both devices.**
- However, a few participants consistently diverged from this dominant norm, as discussed below.

2. Meaningful consent.

- Phrased as a yes/no questions about whether the fictional character needs to have choices regarding how his/her information is handled at the six data protection loci also elicited a strong trend toward **YES across all loci and across both devices.**
- A second yes/no question probed whether the fictional character would still use the device if they did not have choices about how their information was handled at the loci elicited a strong trend toward **NO across all loci and across both devices.**
- However, a few participants consistently diverged from this dominant norm, as discussed below.

3. Reasonableness.

- Participants were asked to draw a line or to circle the data handling options that they would consider to be reasonable for each of the data protection loci, in the absence of user choices: responses varied, but tended toward **strong user control of data handling practices.**

- Those that diverged from the highly privacy protective norms regarding transparency and meaningful consent, however, often were particularly privacy protective in answering replies regarding what would be reasonable in the absence of user choices.
- While reasons for diverging should be pursued in further studies**, this pattern appears to be related to privacy profiles, and indicated an alternative approach to reasoning about data protection that foregrounds reasonableness over transparency and consent.**

Overall, **there is no significant difference in reasoning between digital assistants and robots.** The findings show that even a participant who thinks differently about privacy protection -- that is, placing more weight on reasonable limits than transparency and choice -- there is little difference between the reasoning employed in relation to digital assistants, and that employed in relation to personal robots. Determination of what is reasonable in the absence of user choice is primarily privacy protective, however, with some recognition that function and process can determine what is reasonable. In future studies, individual follow up interviews would help verify the reasoning process with particular participants.