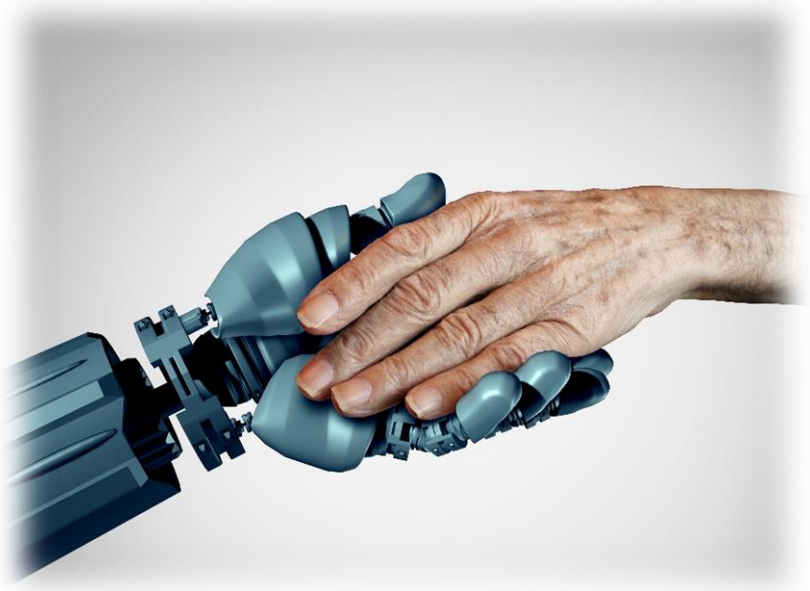
Good Privacy Practices for Developing and Marketing Social Support Technologies for Seniors



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

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. BACKGROUND

Senior citizens are an expanding population in much of the world. Consequently, companies that develop digital networked technologies are increasingly marketing these devices and applications to provide social support for seniors and their caregivers, in order to prolong a seniors' ability to live independently: that is, providing support for "aging in place".

For this study, the researchers held focus groups and workshops with seniors across Canada to collect the ethical concerns and privacy issues seniors have with using digital networked technologies both in current use and in prospective future use. Current devices in common use by seniors included:

- desktop and laptop computers,
- tablets,
- smartphones, and
- the Internet of Things (IoT), including devices like digital home assistants such as Amazon Echo and Google Home (less commonly).

Prominent tasks that these technologies are being pitched to perform for seniors include a range of social support functions:

- Facilitating social connections and activities to address social isolation;
- Monitoring for health and safety issues;
- Providing reminders, prompts and information retrieval, both in everyday use and more specifically to address short term memory loss or other cognitive ability reductions;
- Providing conversation and companionship to provide reassurance, encouragement, and entertainment, especially to address loneliness, depression and anxiety; and
- Providing a digital medium for family members to monitor and encourage seniors' social activities as caregivers.

Accomplishing these tasks generally requires the devices and applications to collect, use and sometimes share personal data either actively or passively provided by the senior user.

These "Good Privacy Practices for Developing Social Support Technologies for Seniors" were co-created with the seniors who participated in focus groups and workshops in research project "Involving Seniors in Developing Privacy Best Practices: Toward Responsible Development of Social Technologies for Seniors" funded by the Office of the Privacy Commissioner of Canada's (OPC) Contributions Program. In gathering data about the concerns, limitations, and benefits that seniors perceive current and future technologies to present, the researchers focused especially on personal data protection. We sought to understand how seniors currently employ strategies to protect their personal information, and what knowledge, tools, and support they would need in order to consider expanding their current practices to new functions or devices.

II. PRIVACY BEST PRACTICES FOR EVERYONE

Seniors are in most ways just like all other adults: so data protection principles that businesses must abide by of course apply just as much to businesses developing technologies for seniors.

The OPC has many resources for businesses that provide information on their obligations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In particular, the "Privacy Toolkit" guide for businesses and organizations is an excellent resource outlining data protection obligations, which can be downloaded here.

In short, businesses that develop and market social support technologies for seniors must abide by the PIPEDA's 10 Fair Information Principles:

1. Be accountable
2. Identify the purpose for collecting personal information
3. Obtain valid and informed consent
4. Limit collection to only what is necessary
5. Limit use, disclosure and retention to only what is necessary
6. Make sure data collected is accurate
7. Use appropriate safeguards
8. Be transparent about your data practices
9. Give individuals access to their own information
10. Provide recourse for complaints

While businesses developing and marketing social support technologies for seniors must abide by these principles in general, there are some particular challenges to doing so specific to the senior demographic. The following sections set out some of the challenges of designing privacy best practices for seniors, common myths and over-generalizations that should be avoided, and good privacy practices as suggested by the seniors who participated in this study.

III. CHALLENGES OF DESIGNING PRIVACY BEST PRACTICES FOR SENIORS

Some of the challenges of designing privacy best practices for seniors include:

- Sensitive Personal Information:
    - Some of the functions that are potentially most useful to seniors are also inherently privacy invasive (e.g. monitoring for adverse events like falls or not getting out of bed);
    - Voice assistants can be helpful for seniors, but they require the capacity to listen for activation words, which can result in unwanted monitoring;
    - Some social support technologies, like social robots with conversational abilities and facial recognition, require activation of cameras, microphones, and often access to cloud services, which can collect sensitive audio and video data for processing; and
    - Providing personalized content for entertainment and community engagement involves gathering potentially sensitive information about the senior's interests and circumstances.
- Seniors worry about security:
    - Seniors are often attuned to media reports of security risks, such as hackers getting access to home monitoring or digital assistant devices, businesses having poor data protection practices (e.g. social media platforms), banking and credit card information being compromised and misused, and seniors being manipulated by scammers. These reports make many seniors wary of using networked technologies.
- Some seniors lack confidence in their ability to use networked technology safely:
    - Some seniors opt to avoid using such technologies or use them only for limited purposes, instead of learning how to use privacy protections.
- Seniors are a widely variable population:
    - Seniors are not a uniform group, with the full range of opinions, perspectives and privacy risk tolerance levels of the general adult population.
- Seniors value their independence and autonomy:
    - It can be tricky to know whether a senior can give consent on their own behalf, or if a caregiver should be providing consent; and
    - Seniors are well aware that their health and cognitive capacity may decline over time. They often think about social support technology use as something they do not currently need, but may need if their health and abilities decline in the future.

IV. AVOID OVERGENERALIZATIONS ABOUT SENIORS

There are some commonly held and repeated generalizations about seniors as a population that should be avoided by any business that is developing and marketing social support technologies.

AVOID THESE OVERGENERALIZATIONS:

- Seniors are not tech savvy:
  - Some seniors are indeed not particularly tech savvy, but many are just as capable and interested in new technology as the general adult population.
  - Younger family members sometimes assume their elders cannot make wise decisions about privacy protection.
  - Materials for seniors should avoid reinforcing disempowering messages.
- Seniors are a vulnerable demographic:
  - While certainly there are seniors who are vulnerable to manipulation and deceit, seniors as a whole should not be assumed to be more vulnerable than other adults.
- Seniors are a uniform group:
  - Seniors do not all reason along the same lines when it comes to how best to approach privacy protection.
  - Most seniors espouse 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 too 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.

Our focus groups and workshops revealed that seniors engage in a complex reasoning process when deciding whether or not to use a device, platform or application for a particular function, weighing the benefits, burdens and privacy/security/safety risks. The reasoning process was similar across currently available devices and future devices (such as social robots).

Many seniors show great potential benefit in using technology for social support, but had varying levels of comfort with the data collection, use and sharing practices that using such technologies would entail.

V. GOOD PRIVACY PRACTICES FOR SENIORS

Many people, seniors included, complain about how difficult some applications make enabling privacy settings. Many complain about overly complicated, legalistic privacy policies that consequently tend to go unread. Some seniors face even greater barriers to understanding such procedures and policies, to the point where they opt out of using a device or application entirely.

In order to boost the confidence of seniors in using your device, platform, application or service, we recommend the follow good privacy practices for seniors:

1. Seniors value the data protection principle of **transparency.** Tell users exactly what information will be collected and why through a clear and abbreviated privacy policy.
    - An **abbreviated version** of the data handling practices of the device, platform, application or service that highlights the key points should be made for senior users.
    - The abbreviated version should **link to the relevant sections of the full privacy policy**, should the user wish to see the complete more complex version.
2. Seniors value the data protection principle of **meaningful consent.**
    - The OPC has issued Guidelines for Obtaining Meaningful Consent. The OPC stresses that while the complete privacy policy should be readily available, emphasis and attention should bring forward four key elements:
        - What personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to.
        - With which parties is personal information being shared.
        - For what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to.
        - Risks of harm and other consequences
    - The OPC has made similar recommendations for developers of mobile apps, where obtaining meaningful consent from app users can be challenging: see Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps.
3. 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 with **live support** to assist seniors through the reasoning process.
4. 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.

5. 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 and support** should be available for senior users, preferably via a means to talk to a live representative of the company.
6. Seniors are looking to companies to **proactively protect user privacy,** and so alleviate some of the burdens on seniors to have to constantly check and update their privacy preferences. Make privacy protection a key part of your business.

VI. Building Trust

Like most people, seniors prefer to deal with companies that they trust. Well-established companies tend to have an easier time maintaining the trust that has already been earned, while newer, smaller companies will have to build that trust. Building trust with seniors should follow from the above good privacy practices.

Seniors are often steady consumers of news media. When they have read a news item about a security breach or a poor privacy protection practice, they tend to lose trust in the company or its device. Whether trust or distrust carries over to a new device depends on how closely a senior considers the parallel with previous devices. In our study, many participants had heard about incidents with digital assistants of unwanted surveillance, unwanted transmitting of conversations, and hacking. Some of these concerns carried over in what they imagined would be privacy and security issues with social robots.

The marketing of new devices and applications for seniors tend to focus only on the benefits of adopting the device or application. Privacy and security concerns are often not addressed at all, or only superficially. Trust can be built by expressly addressing the privacy and security concerns of seniors, and what protections the senior user can access in order to mitigate risks and so feel more at ease with using the technology.