AGE-WELL Standard Submission

RATE

Journal of Rehabilitation and Assistive Technologies Engineering
Volume 7: 1–15

DOI: 10.1177/2055668320950195
journals.sagepub.com/home/jrt
SAGE

Protecting the privacy of technology users who have cognitive disabilities: Identifying areas for improvement and targets for change

Virginie Cobigo[1,2], Konrad Czechowski[1], Hajer Chalghoumi[1], Amelie Gauthier-Beaupre[3], Hala Assal[1], Jeffery Jutai[3], Karen Kobayashi[4], Amanda Grenier[5,6] and Fatoumata Bah[1]

Abstract

Introduction: Information Technologies (IT) may serve assistive roles that facilitate the interaction of people living with cognitive disabilities (CD) within their environments. However, there are some notable concerns related to privacy threats associated with the use of IT. The purpose of this study was to examine how assistive technology developers may best adapt over time to develop their IT to be resilient against threats to privacy. We therefore focused on the following areas: (1) developers' knowledge and practices related to privacy protection; (2) challenges when applying recommended practices, and; (3) preferred channels to acquire knowledge.

Method: We conducted semi-structured interviews with ten technology developers who are members of the AGE-WELL network undertaking research and development of assistive technologies to be used by people who have cognitive disabilities. We used an inductive-deductive method for the analysis of qualitative data to examine participant responses and generate themes related to the study goals.

Results: Principal themes that emerged from the data include practices specific to populations with CD, challenges to obtaining consent to use of information, and preferred channels to acquire knowledge.

Conclusion: We identify areas of focus for developing a knowledge mobilization strategy to improve relevant policies and practices.

Keywords

Privacy, technology development, implementation of change, cognitive disabilities, knowledge mobilization

Date received: 16 January 2020; accepted: 22 July 2020

Introduction

People who have cognitive disabilities may be at heightened risks where ethical issues, such as those relating to autonomy and privacy, are concerned. In using the term "cognitive disability" (CD), we refer to limitations that a person might have in their intellectual or cognitive functioning. CD includes cognitive and adaptive limitations with onset in childhood (*e.g.*, Down Syndrome). It may also result from brain injuries or a disease acquired later in life, such as dementia.[1] Cognitive disabilities exist in all age groups, but become more prevalent in later life with nearly one quarter of adults 65 years-old and older living with a

[1] School of Psychology, University of Ottawa, Ottawa, Ontario, Canada
[2]Children's Hospital of Eastern Ontario Research Institute, Ottawa, Ontario, Canada
[3]Interdisciplinary School of Health Sciences, University of Ottawa, Ottawa, Ontario, Canada
[4]Department of Sociology, University of Victoria, Victoria, British Columbia, Canada
[5]Factor-Inwentash Faculty of Social Work, University of Toronto, Toronto, Ontario, Canada
[6]Baycrest Hopsital, Toronto, Ontario, Canada

Corresponding author:
Virginie Cobigo, University of Ottawa, 136 JJ Lussier, Ottawa, ON K1N 6N5, Canada.
Email: Virginie.Cobigo@uottawa.ca

cognitive disability.[2,3] People who have CD may experience challenges in their daily living and barriers to social inclusion due to limitations in their abilities to process and recall information, or communicate with others.[4,5]

Information Technologies (IT) enhance participation in areas such as community integration, education, and recreation and leisure[6] and facilitate the interaction of those living with CD within their environments.[7,8] Persons with CD perceive the benefits of IT use and want to use them in their daily life.[9–12] However, there are some notable concerns related to privacy threats associated with the use of IT.

People with CD are among the most vulnerable to privacy threats, such as cyberbullying, and financial and sexual exploitation.[10,11,13,14] We define privacy as including the "right of individuals to determine if, when, how and to what extent data about themselves will be collected, stored, transmitted, used and shared with others".[15] We consider privacy to revolve around personal control of one's information and a right that enables individuals to have personal autonomy and independence.[16] Some of the aforementioned vulnerability may be explained by a difficulty to transfer their knowledge of privacy protection and threats to the abstract context of IT use.[10,11,14] For example, older adults with CD may misunderstand the information conveyed and/or important aspects such as who has access to the information recorded by the technology.[9,11,14]

IT developers and researchers in the field agree that security and privacy protection mechanisms negatively affect the usability of the technology, especially for people who have disabilities.[17] Technology developers report having limited knowledge of the challenges faced by people with CD, especially when protecting their personal information, leading to ill-informed practices.[17] For instance, the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is considered to be an efficient mechanism to increase the security of the interface being accessed. However, the cognitive demand associated with understanding instructions and identifying the relevant information to be reproduced is high.[17] IT developers may even choose to add distortions that further increase the security level, but "impose [...] a high cognitive load" on users.[17]

In addition, when targeting users who have CD and their caregivers, IT developers often overlook privacy concerns, or consider them too late in the technology development process.[18] In fact, technology development often aims to address caregivers' concerns about the safety of individuals who have CD or to support professionals' clinical assessment. Although these goals are legitimate and useful, they often supersede privacy considerations, leading to complex ethical dilemmas.[19,20] For instance, using tracking devices for safety reasons appears benevolent and useful,[21] but such ITs may be a source of intrusion to privacy through surveillance, and may cause stigma associated with tagging.[22]

Current practices, as reported by technology developers, call for an effective knowledge mobilization strategy that leverages scientific, practical and experiential knowledge, and translates it into improved policies and practices.[23,24] For instance, Balebako et al.[18] found that many developers they surveyed lacked awareness of privacy measures and were found to often make privacy-related decisions in an ad hoc manner. Transforming ill-informed practices requires knowledge mobilization strategies; however, the traditional way of transferring knowledge to technology developers has proven ineffective in changing practices and behaviours.[18] In fact, private sector (commercial) technology developers tend not to seek information from guidelines published by governmental agencies, but rather seek advice from their social networks or specialists within their company,[18] and from websites and trade magazines designed for product developers.[25,26] It is therefore advisable to be proactive at making knowledge available to them through their own channels of information.[27]

Current study

It is crucial to tailor knowledge mobilization strategies to technology developers' needs and contexts. Technology developers are often on the receiving end of knowledge mobilization strategies that aim to inform technology development practices to adequately protect privacy. To this end, our study was designed to explore developers' perceptions and understanding of issues related to privacy protection. Our qualitative study aimed to: 1) describe the current state of knowledge and practices of a sample of technology developers regarding the protection of the privacy of users who have CD; 2) examine the challenges they face when applying recommended practices; and 3) identify their preferred channels and mechanisms to acquire knowledge in the area.

Methods

Study context

The current study is part of a broader project that aims to develop an Implementation of Change process[28] for technology developers to develop technologies that are ethically sound for users with CD and their caregivers. An Implementation of Change process[28] implies a

collaborative approach with key knowledge users who help to tailor knowledge mobilization messages and tools to their information needs. Having an impact on practices is the result of a complex process and must be guided by existing frameworks that help structure the activities and identify barriers to knowledge use.[29] Grol and Wensing[28] proposed a 7-step process to implementing change in practices that is based on the critical review and evaluation of several theories of change. Step 1 involves the development of a proposal for change, which includes understanding the policy and legal context of the issue and reviewing existing scientific evidence. This step was completed as part of a previous project.[30] Step 2 consists of analyzing knowledge users' actual performances and identifying areas for improvement and targets for change. Steps 3-7 include the development of strategies to change a practice, execution of a plan, and integration of changes to create sustainable change. Step 2 was the focus of the research described in this paper.

Participants

Ten developers involved in the development of technology to be used by people who have CD took part in this study and were recruited from two sources: eight were based in universities and two (participants 1 and 2 in Table 1) were not. Participants reported a range of types of technologies they had experience developing that may be used by people with CD (see Table 1). Participants have been involved in a range of projects throughout their careers and were thus at various stages of their current projects at the time of interview.

We used a convenience and subsequently snowball sampling strategies to recruit participants who were knowledgeable about technology development for people with CD. Potential participants were identified by the authors of this paper, within the AGE-WELL (Aging Gracefully across Environments using Technology to Support Wellness, Engagement and Long Life NCE Inc.) network. The AGE-WELL network was launched in 2015 through a federally-funded Networks of Centres of Excellence (NCE) program in Canada. AGE-WELL NCE is a pan-Canadian network of caregivers, researchers, and 380 industry, government and non-profit partner organizations that aims to develop and deliver technology-based solutions to improve quality of life for older adults and caregivers.[31]

We recruited during targeted conferences, by posting information on relevant websites and in newsletters, and by sending emails to individuals who were known to have the expertise we sought to participate in this project. Prospective participants were informed that the aim of the study was to "examine AGE-WELL members' considerations toward privacy and security in the development and commercialization of technologies for which the target market includes persons with cognitive disabilities." Prospective participants were asked if they could suggest additional participants. Those who agreed to participate in the study responded positively to an invitation email to which all relevant information and consent details regarding study participation were attached. Trained research assistants confirmed participants' consent and conducted interviews over the phone, via Skype, or in-person. The third, fourth, and fifth authors conducted the interviews. Interviews that were held in person were held at an AGE-WELL conference in 2018. Participants were not compensated for the interviews. Ethical approval was granted by the University of Ottawa Research Ethics Board (Date of approval: 08/01/2018; Ethics File Number H-11-17-40).

Data collection. Data were collected by means of semi-structured interviews between August and November 2018 (See Appendix 1 for the interview guide). Participants were asked about: (1) the products they developed that may be used by people with CD and their targeted users' characteristics; (2) their knowledge about and practices for protecting users' privacy and obtaining consent for the collection of information

Table 1. Participant background and experiences.

Participant number	Type of technology developed	Targeted users
1	Application (mobile device)	Any cognitive disability
2	Application (mobile device)	Mild cognitive disability (eg, early dementia)
3	Applications (mobile device)	Head injury, Alzheimer's disease, Schizophrenia, Intellectual disability
4	Application (web-based)	Cognitive disability associated with aging
5	Alert service and digital games	Dementia (older adults)
6	Applications (web-based)	Dementia
7	Communication assistive technology	Early onset dementia
8	Sensors	Dementia
9	Digital game Sensors	Dementia or mild cognitive disability (older adults)
10	Applications (mobile device)	Any cognitive disability (older adults)

throughout the research and development process, particularly when targeting users with CD; and (3) their need for information on these matters and preferred means through which they may obtain this information. Each interview lasted approximately 60 minutes. Interviews were audio-recorded and transcribed verbatim by trained undergraduate students. Transcripts were then verified against the recordings by a senior research assistant.

Data analysis. After interviews were transcribed and checked for accuracy, they were imported into NVivo qualitative analysis software. Each transcript was coded for each of four themes of interest, which included: (1) practices for protecting the privacy of people with CD; (2) the extent to which technology developers are knowledgeable about Canadian privacy laws; (3) challenges related to protecting the privacy of and developing technology for people with CD; and (4) developers' information needs and preferred ways to receive training or information. These themes were chosen based on a review of literature and consistent with subject matter covered in the interviews.

Next, a cross-case matrix display[32] was developed where rows represented participants and columns represented each of the four themes of interest. Two researchers worked together to review codes and began this process by filling the rows for three participants. Researchers then conferred with the research team and based on overall impressions of the data and the contents of the matrix at that point, created subheadings within columns to further organize the data. The first three completed rows were then re-organized to conform to the new structure, and researchers then proceeded to fill the rest of the matrix for all remaining participants using the codes and transcripts.

The analytic process included a second cycle coding process[32] that allowed us to condense the data into smaller analytic units, as we moved from our four themes of interest to their sub-categorizations, and then to the patterns we observed across participants. We subsequently collapsed our second (knowledge about privacy laws) theme into the third (challenges applying recommended practices), leaving us with three themes after completing our analysis. Throughout this process, researchers remained open to the possibility of discovering new themes as they conducted analysis, employing a process of deductive qualitative analysis based on the original four themes of interest, while allowing for themes to emerge directly from the data using an inductive process.[33] Our findings are thus organized by upper-level or more general themes derived from our research questions and by lower-level sub-themes derived inductively from our multiple readings of the data.[34]

We took a number of steps to ensure the quality of the analysis when testing and confirming findings. First, we maintained methodological and analytic documentation throughout the whole process, allowing for steps to be retraced and evaluated on an ongoing basis (often referred to as an *audit trail*[35,36]) Second, the team met regularly to discuss decisions related to analysis and impressions of the data, as well as emerging themes. Third, employing a method of constant comparison of the data, researchers frequently went back and forth between the original transcripts and the cross-case matrix display to confirm emergent themes. Throughout this process, interpretations of the data were regularly discussed at group meetings and in occasional instances where there were differing interpretations of the data, researchers went back to original transcripts to come to a mutually agreed upon interpretation.

Findings

In this paper we primarily discuss three of the original four themes, integrating the material on the extent to which technology developers are knowledgeable about privacy laws with the theme examining challenges. The next section outlines three themes, as follows, including verbatim quotes from the interviews: (1) Users' privacy protection (knowledge and practices), (2) challenges when applying recommended practices; and (3) preferred channels and mechanisms to acquire knowledge. Each theme is divided by its sub-themes.

Users' privacy protection: Knowledge and practices

Participant views of what should be kept private. Participants gave a range of responses about their interpretations of 'what constitutes' private information, depending on the nature of the data they were working with. One participant said that they collect "pictures from [users'] homes or pictures from their work settings. It's pictures of them and work colleague[s] ... so technically since it is all theirs I would say all those data are private" (P10). Another participant spoke of "real-time data about [users'] movements and activities, that was being collected by sensors in the home" (P6) to be private. Further, another participant spoke of how some users may not make their diagnosis "public in terms of their workplace" (P7) adding that since many users had not "disclosed their diagnosis or that they have any sort of dementia to their employers or to their co-workers," it is essential that the information be kept confidential. Exceptionally, one participant, when asked about what they considered to be private to users, responded by saying "anything beyond their name and address" (P2). This is the only case where a participant's view

of what constituted private information contrasted with the views of others, given that a name and address are directly identifying information that were generally considered private by the rest of the sample.

There was consensus that private information generally refers to information that is collected from the user, illustrated by one participant who collects data about daily habits, who said "in fact, all" (P3) when asked what data they consider private. In their responses, participants did not distinguish between levels of privacy (i.e., that some information may be more private), with the exception of a developer of games that measure cognitive functioning, technology that measures driving ability in cars, and wandering alert sensors at home for people living with dementia, who spoke of the importance of context when considering how (or whether) data ought to be considered private:

> [if] somewhere it says that [a user's] number is a hundred and twenty-four, it's not private because it doesn't mean anything. If it said, my haemoglobin value is a hundred and twenty-four, now that means, that's a medical piece of information, and that has, you know, that value and its personal value because it's a number of both my health and then I say well this is something that needs to be protected (P9).

Practices for maintaining privacy and data security. When asked about protection measures, half of the sample explicitly referred to password protection and/or encryption, a method they employed to ensure their data is appropriately safeguarded when stored. For example, one participant said she stores data using cloud storage software "Dropbox, but [the data are] all protected by a password" (P4) and another who stores data on "internal encrypted hard drives" (P8). One participant, a developer who was working to develop technology for people living with early onset dementia said that the data he works with always undergoes a process of anonymization before his team can work with it: "So we get all the data which is analyzed and it's anonymized so we, we don't really get the full transcripts, it's just the data that will be useful in terms of the probe questions towards tech development" (P7).

Participants were also asked to describe how they store confidential data in a way that maintains users' privacy, while allowing their apps to function and their teams to do their jobs. For example, Participant 2 discussed how his team was faced with the challenge of limiting access to user details while allowing IT personnel to backup this data:

> So, you run into a challenge with how do you protect the data if the IT person is just doing an IT job. You know? For example, the person who backs up the data. That would be one example. So, you know, is there a way using technology that [IT personnel] can't see the data but still back it up? So, you do that through encryption. (P2)

We found that participants reportedly stored their data either on their own servers, "we store it on our computer so on our server" (P3) - or "data goes to the cloud, and, it's stored in the cloud" (P9). One participant said he stores data on both a server and cloud: "[data] it is going to be stored out in the cloud as we say [. . .]. We will create back-ups that we will keep locally just in case the cloud does go down" (P1).

Practices specific to users who have CD. A developer said he believes users with CD may experience challenges related to understanding privacy policies to which users need to adhere. Despite this, he explained that they do not take any extra measures to assist the users with CD in understanding the policy, based on their lawyers' advice that the law does not require them to do so. He explained, "Lawyers don't want you to be a pioneer, because you would get tested and [the outcome] could be negative from a commercial point of view" (P2). This respondent was speaking to a risk-averse context where they were advised not to take any additional measures to assist users in understanding the privacy policies, fearing it may impede the process of commercializing the product.

One developer who works with people with dementia to develop assistive technology described an additional step taken in instances where the user is judged to not have the capacity to consent on their own, using a *substitute decision maker* in their place. He described that because their users "have dementia . . . they cannot consent so we have a substitute decision maker. So, they consent on behalf of the participant" (P8).

Some participants who work with users whose cognitive capacity may be declining spoke of the process of re-documenting consent. One participant, a developer experienced in developing applications for people living with dementia described a process of re-confirming consent he was considering implementing, given that he works with a population whose cognitive capacity is expected to decrease over time:

> A challenging question given we are dealing with people whose cognitive abilities are deteriorating over time . . . [it is] a very interesting question given that we're dealing with people whose cognitive ability is declining over time. So, we are also considering having re-consent processes over the time because as

> I said our case studies are over the period of two years so very important for us to re-document the consent and actually make the person who is using the product made aware of what they're using and that their data is being collected so there will be a re-consent – not only a consent but a re-consent. (P6)

This sentiment was echoed by another participant, also working with a population experiencing cognitive decline over time, expressing that:

> Re-documenting the consent is one important part that we have to consider that again because a person might not know what their, their privacy are or what information they're sharing that might also change over time so re-documenting the consent is a part of that. (P7)

Re-documentation of consent was generally described as a more formal process where consent may be re-documented the same way it was originally (i.e., by signing a paper confirming consent). When asked about re-confirmation of consent, one participant, who worked with people living with dementia experiencing cognitive decline over time, discussed more informal ways of first checking whether the re-confirmation of consent is necessary:

> Theoretically, every time [users] come, they have the opportunity to give consent or at least assent to say yes last time I did this and I read all the papers and I agreed with it all and today I still agree [. . .] And confirming what I said last time was good. But theoretically, if they say, 'No no, I don't know why I'm here, show me that protocol again, I wanna read it all again, I wanna know why you're collecting this data again.' Fine right, technically we should be getting consent every visit. So, we usually have sort of an informal way of checking that they're still able to give consent. (P9)

This individual spoke of how they look for verbal cues from users (e.g., indicating confusion) that may indicate that redocumentation (and, importantly, re-confirmation) may be warranted. This quote is illustrative of the concerns some participants expressed about the need for re-documentation of consent with populations whose cognitive capacities may be declining. They made clear that with such populations, it is not immediately clear if consent given previously can still be considered valid (and informed) given potential cognitive decline.

Challenges when applying recommended practices

Obtaining consent to personal data collection. We asked participants about their practices for obtaining consent to personal data collection at any stage of the research and development process, i.e., including data collection for conceptualizing or testing a product, defining its market or commercialization strategy, and after commercialization. Procedures for confirming consent as described by our participants were fairly consistent, often describing a number of challenges associated with the process. In instances where participants had in-person interactions with people who have CD, they generally confirmed consent in person, having them sign a consent form. As outlined by one participant developing a model to identify factors that increase the chance a person with dementia may get lost:

Interviewer: So, when do you ask for user's consent?

> Participant 5: At the beginning of the well, yeah, at the beginning of the first interview . . . So, we explained the research by phone, we didn't ask for any personal information there, and when we got to their homes for the first interview, we explained everything and we asked for their, for their consent.

Another participant who works in an environment where consent is obtained in person presented a challenging situation regarding privacy protection of a non-consenting individual. The developer described their work on a project that involved recording residents and staff members at a facility that sought consent from both residents and staff prior to video recording them. However, staff who did not consent were reportedly recorded nonetheless, and then on a monthly basis, video data was reviewed and footage that captured non-consenting staff members was deleted from the server:

> . . .in case there are, there are one or two staff who have not consented for various reasons so we have to delete that video data to preserve their privacy . . . we are made aware of it so on a monthly basis we remove that data from our servers. (P8)

It is unclear whether the participant's REB has approved their protocol, or if non-consenting staff members consent to this method of privacy protection, given that the participant did not provide more contextual information.

On the other hand, in instances where consent for the gathering of personal information needed to be confirmed electronically, participants described the process often requiring participants to click an *OK* button in acknowledgement of the privacy terms and conditions before using the product. As one developer working on an app to assist people with CD with daily activities, they confirm "[users'] consent when they install the application. It's a standard protocol for all apps that you download either in the iPhone store or from the Android store" (P2). Another developer,

working on the same app simply described the process as involving "an online document [users] read and they accept which is a fairly standard process for applications of this type" and they went on to describe that "legally, we are being informed that that is an acceptable approach" (P2).

Challenges related to privacy laws. Our analysis identified some challenges participants reported when endeavoring to learn about or follow privacy laws. However, some participants had no knowledge of laws, reporting that ensuring practices comply with laws was not their role, but that of others (e.g., a lawyer). Multiple participants discussed having difficulties understanding the law, understanding the similarities and differences between different laws (e.g., across different provinces), and identifying the specific laws that they have to comply with when building their applications. One developer described challenges related to navigating inter-provincial certification requirements:

> It's really difficult [to get a certification in Quebec]. And in some cases, some of the items are written by [policy people] who don't understand current technology. I'll give you an example, I don't have it in front of me but I could go look it up. In Quebec, there's certification, one requirement says your data centre must have a glass front on it so that you are able to see what the employees are doing. Well, in a cloud-based environment where you're paying a vendor to do this, it doesn't really apply, right? It's not an applicable thing but it's still one of the requirements so...(P2)

In addition, as discussed earlier, participants were sometimes faced with challenges where they had to make privacy-related decisions in the absence of explicit guidelines for their particular situations. Our participants expressed the need for overarching guidelines or *privacy 101* resources for all the team members:

> I think the content can be at various levels, again, I think there needs to be information that is pertaining to the different stages of a project [...] Certainly, it would be very useful to have some very simple guidelines that people can look at, [...] so a simple privacy 101 document which would help people to understand the sorts of things they need to be doing at those different phases [research and commercialization] and then with supporting documentation or links to where they can find out more, you know, resources or links to organizations that provide this sort of help and support that they need to do. (P6)

Preferred channels and mechanisms to acquire knowledge

Despite reported challenges, participants left an impression that they were willing to learn more about best practices related to privacy protection and relevant laws, such as one developer who identified time constraints as a barrier: "If [training] could be one not more than two hours, [...] it would be ideal [...] because you can squeeze it in your lunch break." (P4). Another identified a lack of access to relevant resources as a barrier to further developing their knowledge:

> Interviewer: so, I am not sure if you're aware of those laws, have you taken any steps yet to learn about [privacy] laws?

Participant 5: No and maybe I would be interested for you to send me the [resources regarding laws in Canada that you told me about before].

As part of our data analysis, we identified participants' preferred channels of knowledge acquisition to inform future knowledge mobilization initiatives for technology developers that address the importance of protecting the privacy of users with CD. We found that developers rely on different sources of information regarding privacy and the law.

Sources and accessibility of information. The different sources of information relied upon by developers complement each other and provide different outlooks on privacy. Some sources that participants discussed considered privacy from a more user-centric perspective, while others focused on the legal or the technical aspects of privacy protection.

One developer mentioned that they contact advocacy groups that include members who live with CD, as well as gain information about any specific considerations for protecting their privacy. Although we did not ask this question explicitly, this is the only participant who mentioned consulting prospective users with CD about privacy.

> We should also mention at this point that part of the development of the [name of the system] is a sub-study that specifically explores the ethical and legal issues associated with the release of personal information via the [name of the system]. We've interviewed twenty people so far from across Canada, and representation from persons living with dementia, care partners, advocacy organizations, support organizations, police as well as search and rescue organizations. (P5)

Another emphasized the importance of availability of information, raising that they first consult the internet: " me personally, I would look for websites because I am always on the web like for my job" (P4) and subsequently consult documents they expect will contain the information they seek, "I like to have documents [to consult]" (P4). However, regarding more complex or specific information, this participant expressed appreciation for a lawyer they are able to consult: "But I also like to have like a lawyer, or someone you can contact if you have a really specific question and you don't wanna go through like 50 pages of a document" (P4).

This case was illustrative of participants' preference for easily accessible resources by first conducting an online search or asking a colleague for advice – participants reported they appreciate when they are able to find the information they seek more readily than having to schedule a meeting with the organization's lawyer or an advocacy group. This sentiment was reflected by another participant who appreciated in-person consultations, "A face-to-face review would be the best … because then we would have the chance to analyze it in detail, we would be able to ask questions, and clarify anything that was unclear" (P2).

Another participant preferred to immediately consult their privacy officer and only search online if the privacy officer is inaccessible:

> We're in a hospital, so we actually have a privacy officer here. So, I'm spoiled, right? I can pick up the phone and go [name of privacy officer], help me out here. But yeah, so I mean that, that's what I would do. I mean otherwise obviously I just go online and you know, look it up myself, if it was off hours, I'm not gonna call her at home at 9pm [. . .] I'll go online and search it myself. (P9)

Responsibility for privacy. Most participants aimed to meet a threshold of compliance when it came to privacy protection determined either by their Research Ethics Board protocol or the law and did not indicate that they had taken or considered additional steps related to protecting the privacy of users. For instance, one participant reported he refers to, and relied on, his organization's ethical or legal departments to ensure their practices comply with Canadian privacy laws:

> Usually, we start with the jurisdictions, they publicize information well. It may be difficult to understand sometimes but they do publicize it. If comes to something that is very close [. . .] to requiring a legal opinion, then we would go to a lawyer. (P2)

Similarly, another participant reported that he did not consider privacy issues prior to commercialization of his product: "I've never had to deal with [privacy issues] personally because I've never commercialized this type of product myself" (P6). Indeed, when asked about privacy-related matters, some participants reported they were not able to comment because they had either not commercialized their product yet or did not collect data from users. In both cases, participants implied that they did not need to be well versed in matters relating to privacy protection until product commercialization or until data collection. Further, some expressed it is not their role on the team to be concerned with privacy. For instance, a developer with experience in adapting existing technologies used by caregivers to people who are ageing to the Canadian context said, "I am not aware of the laws so I might have to read them to make sure … we usually have like, the lawyer" (P4). Developers working in a university context often deferred to their Research Ethics Board or designated colleagues on their research team, as one developer who works with people with dementia using sensors and physiological activity to develop assistive technology said, "we have an ethics board here, we have a research coordinator, she has experience in, you know, in all these ethics reviews so she has good, good, good knowledge of [user privacy]" (P8).

Privacy information needs. Developers reported seeking privacy information from a variety of sources which reflected the range of privacy information needs they described, from very general information about Canadian privacy laws to very specific technical details. For example, one participant mentioned referring to regulations by their local jurisdiction where they gain general information about the law (see previous P2 quote). On the other hand, participants also described consultations with other sources who had familiarity with privacy laws or knowledge of best practices participants could draw from to provide practical advice when addressing privacy considerations. Participants reported soliciting specific information about a specific regulation that they were required to follow or technical implementation advice. For example, a participant described that his source:

> Would be the university and the [name] company that we're working with because they have experience with actually dealing with real time data of the people or the consumers they're working with. So, the university and our collaborators, the company specifically would be my reference point. (P7)

Finally, one participant discussed the need for more practical guidelines throughout the software development lifecycle:

> So, issues around privacy extend beyond the technical aspects of data security and confidentiality. Privacy is also about how the data is used and whether the data is used in an invasive and intrusive way. It's very difficult to really judge what's being done at the moment because many of these systems that we're talking about are still at prototype level, the kind of guidelines about how these should be used in order. . ., even if the data is secure and confidential, and that there's no issues around how the data is used and by whom is still really open to question. (P6)

Discussion

Overall, participants noted the importance of adequate practices to maintain users' privacy but highlighted a number of challenge areas unique to working with users living with CD. Challenges principally included barriers to ensuring informed consent is obtained and maintained. Participants often spoke of consent as a theoretically challenging issue, but practically speaking, there is little evidence that most participants took additional measures to obtain and confirm consent. Some participants also identified issues related to the application of privacy laws, primarily related to a lack of clarity or access, particularly if they did not have access to legal advice.

Practices related to privacy protection

Our participants gathered a range of data from users including sensor information, private pictures from their homes, and directly identifying personal information such as names. They generally agreed that most (if not all) information gathered from users ought to be considered private. Participants' perceptions of what constitutes private information are generally consistent with the laws governing their use of personal information, such as the Personal Information Protection and Electronic Documents Act (PIPEDA), a federal Canadian statute governing the management of personal information. According to PIPEDA, what participants described as private would constitute *personal information*, which according to the statute ought to be safeguarded using appropriate measures. The definition of privacy we previously cited and use for this article, as the right of individuals to determine the extent to which data about themselves will be collected, stored, and shared with others,[15] underscores the agency of the user.

There was little indication in our findings that participants believed users who have CD require additional measures for privacy protection as compared to people without CD. Indeed, technologies should be designed so that users who have CD have as much protection as is given to other users. Developers should emphasize users' marginalization rather than their vulnerability.[37] Vulnerability refers to individual characteristics that make a person at a higher risk to be harmed, while marginalization refers to the treatment of an individual or group as less important than others. When focusing on users' vulnerability, developers may stigmatize them further by focusing attention on users rather than features of the research and development process and environment that present ethical challenges. Research and development processes would be improved if they were informed by a deeper understanding of aspects of the user's life that are associated with social marginalization. In this way, IT interventions could be better targeted to reach persons with CD through improved user-centred research and development.

One participant referred to a user's diagnosis of dementia as information that must be kept private, as uniquely important to working with the CD population. This is consistent with previous literature that suggested the stigma associated with dementia makes it particularly important that the information be kept confidential.[38] Indeed, diagnosis is considered *personal information* which according to PIPEDA ought to be safeguarded.[34] Given that people who have CD and their caregivers may seem misinformed and naïve regarding the risks for privacy breaches when using information technology,[9] it is particularly important that appropriate measures be taken to minimize the risk of a privacy breach and to ensure that data belonging to people who have CD is appropriately safeguarded.

Further, participants did not differentiate between type and risk of data collected when considering how it ought to be safeguarded. For instance, Czechowski, Sylvestre, & Moreau[39] developed a data handling framework that considers the type of data handled (the extent to which it is directly identifiable) and risk associated with a potential confidentiality breach when considering steps to securing personal data. Similarly, developers do not need to protect all personal information the same way. For instance, a developer does not need to take the same stringent steps to securing step count information collected by one application as a user's diagnosis; in both instances the information is *private* but the risk associated with a breach is far greater for the latter case. Participants in our study did not report considering type of data handled and risk associated with a confidentiality breach, but only

described some methods of safeguarding information (e.g., password protection).

Privacy by design. When discussing the safeguarding of private information, participants referred to the guidelines or requirements of their particular organization to describe various practices for secure storage of information, including password protection and encryption. Most discussion related to security measures to safeguard private information was about measures that can be taken during the course of a project (e.g., after data is already collected). Indeed, privacy is often overlooked as an innovative feature or considered too late in the development process.[18]

A Privacy by Design approach, a framework to proactively embed privacy protection directly into a technology's infrastructure by making privacy the default setting in the technology's design,[40,41] could be a possible solution. A Privacy by Design approach could mitigate some tensions between privacy and usability concerns, given that some privacy protection measures may affect usability for some people with CD.[42] Such an approach would ease some concerns participants expressed about considering privacy protection at various stages of development prior to commercialization. Implementation of a Privacy by Design approach, particularly if structured, may also serve to satisfy the need for guidance throughout the software development cycle, something at least one participant identified as a need.

Procedures for (re)confirmation of consent to personal data collection

Challenges cited by participants generally centred around ensuring that the user understands what they are consenting to and some have expressed doubt about whether or not consent should be re-confirmed. When asked about consent throughout the research and development process, participants generally spoke of two contexts in which consent was confirmed with users: in person and electronically. Challenges discussed and concerns raised were similar across both methods of confirmation of consent, and generally centred around how the process may be different for users with CD. Indeed, the capacity of people with CD to consent has been explored, particularly in the area of consent to participation in research, finding that people who have CD may benefit from additional accommodations when consenting to participation,[36,37] Our participants spoke from experience in the context of research and development of assistive technology, and concerns related to additional accommodations were reflected in their responses. Despite these concerns, participants did not identify additional measures they routinely take to ensure users' consent was sufficiently informed, with the exception of the use of a *substitute decision maker* to consent on a participant's behalf. The inconsistency between their acknowledgement that additional measures may be appropriate to ensure consent is adequately informed and the absence of such steps reflects a desire for best practices that participants currently do not have access to.

Some spoke of the potential need, under certain circumstances, to re-confirm consent. This concept is not new; for instance, Cameron and Murphy[43] referred to it as *ongoing consent*, where they phoned their research participants with a range of learning and communication disabilities prior to each visit for their longitudinal study over a 4-month period. This is consistent with the approach to consent as a process, allowing for ongoing assessment of participants' comprehension of what they consented to and its implications.[44] Re-confirmation, in our study, was generally discussed in a context of cognitive decline (e.g., users diagnosed with dementia), but participants made clear this was a practice they rarely (if ever) employed. This may have largely been due to an absence of clear guidelines or best practices for re-confirmation of consent, despite some participants bringing it up as important under certain circumstances. Perry, Beyer, and Holm[22] argue that seeking consent in the context of assistive technology should not be a one-off activity; it should be regularly reviewed and users should have the ability to opt out at any point, despite financial and organizational inconveniences to a developer. Further, we note that practically speaking, one should consider the trade-off between a greater frequency of re-confirming consent (thus, increasing cognitive demand) and a resulting loss in cognitive accessibility.

Some participants described the use of a substitute decision-maker to confirm or re-confirm consent. Participants were not always clear about how they determined whether a substitute decision-maker was necessary. Bravo, Pâquet, & Dubois[45] surveyed various stakeholders including older adults and caregivers of adults who have CD and found that most respondents reported that, in the case of people with dementia, participation in research should involve a legal guardian only when higher levels of risk are associated with participation. Their study highlighted that risk should be an important factor when considering whether a substitute decision maker should be used. Moreover, the risks and benefits of including a third party or caregiver in the process of obtaining consent should be carefully considered, given that their inclusion may appropriately facilitate or inappropriately hinder (e.g., due to over-protection) the process depending on the circumstances.[44]

Dye et al.[46] argue for the need to move away from the traditional dichotomous categorization of consent and into a recontextualization that includes a risk and benefit analysis. Such a framework would consider the possible risks and benefits associated with participation when considering the level of capacity necessary to make a particular decision to consent. Our participants illustrated the challenges associated with obtaining consent, particularly in determining capacity to consent, the possibility of re-confirmation of consent, and in the involvement of substitute decision-makers. Despite their uncertainties and the challenges they expressed, they made clear they would benefit from and eagerly follow guidelines or best practices if they were available and accessible to them. Given that such guidelines do exist,[44] perhaps this is more of an issue related to knowledge mobilization in the process of developing resources/tools and awareness of available resources, at least for our participants.

Developing an effective knowledge mobilization strategy

One of the objectives of this study was to inform step two of a seven-step Implementation of Change[28] process. Step two consists of analyzing knowledge users' actual performances and identifying areas for improvement and targets for change. To identify targets for change, a portion of the interviews was dedicated to examining developers' information needs and how best to tailor knowledge mobilization strategies to them. Although findings from this study are too preliminary to be useful to designing a knowledge mobilization strategy on their own, they could be used to inform future studies that together with the present study, will be used to develop a knowledge mobilization strategy of sufficient detail.

Our participants relied on different sources for gaining information about privacy. These sources vary in their availability to participants and provide information that can vary in its level of details, and potentially accuracy. Participants described that they received direct advice and had the ability to discuss and ask follow-up questions. Participants valued the ability to have someone whom they can turn to when they have questions and referred to it as a "shortcut" to timely information when they do not have the luxury of reading long manuals.

They reported a need for practical guidelines. It is also important to acknowledge that frequently, software companies and developers' objectives for building applications are primarily to gain profit. Maintaining privacy and security is not without its cost, especially for companies that do not have security and privacy expertise and resort to hiring experts. Thus, developers should be introduced to the importance of privacy and security from the early stages of their software development training.

However, privacy consideration should be an ethical obligation, which should stem from both individuals' moral values, and regulations. Previous work showed that software developers are often motivated to address security when they understand the implications of security issues on their users and find that it aligns with their own values.[47] Similarly, privacy training should target developers' awareness and understanding of the implications of privacy breaches on users in general, and specifically on users with CD. With new technologies come new ethical problems and their implications ought to be assessed at an early stage of development.[48] Ongoing training is therefore necessary to ensure that developers remain updated on emerging and evolving privacy concerns.

With respect to regulations, our participants reported that regulations mandate privacy practices that are questionable in their ability to protect users' privacy, let alone the privacy of users who have CD. In addition, the advice provided to one of our participants by their lawyers and legal consultants against doing more than the bare minimum outlined by privacy laws is particularly worrying. They consider this as an unnecessary burden, the benefits of which do not outweigh the risk. This more broadly may require a culture shift away from viewing privacy protection as burdensome at this participant's workplace.

Limitations and future research

We identified a few limitations to this study. The findings were derived from a relatively small sample size (n=10) within the AGE-WELL network. A similar limitation resulted from the recruitment strategy; we used a convenience sampling strategy to recruit the participants via targeted conferences, online postings, newsletters, by sending emails to individuals, and a snowball sampling technique to recruit a few additional participants. We used these techniques in order to maximize the number of responses in the time allotted for the project from a population that proved to be challenging to reach and recruit from. This may have resulted in our sampling of more university-based technology developers instead of private-sector developers. The research completed in this project could be advanced by interviewing a larger population of technology developers in Canada, including a larger proportion of those who are not university-based. By having more participants, any differences related to age, seniority level (work experience, training received, etc.) or sector of practice (academic or private) could be highlighted and may produce additional insights

which would have the potential to guide the improvement of knowledge mobilization efforts to meet technology developers' needs in this area. Moreover, some developers whose work is overseen by a Research Ethics Board may have had their practices modified by recommendations from an ethics board that developers in other settings may not have been subjected to.

We also note that the cross-sectional nature of the data collection did not allow us to examine changes in attitudes or behaviours over time, nor what factors may have played roles in such changes. Further, participants were not asked about their awareness of specific published resources on privacy protection. We hope that future research (particularly of a quantitative design with larger samples) will identify published resources on privacy protection and survey developers to examine their familiarity with them.

As noted in the introduction, this study is situated within a larger project that lead to a better understanding of the knowledge mobilization process among technology developers. This study was meant as a step toward the development of a comprehensive strategy that will ultimately aim to increase technology developers' awareness of privacy and security regulations and policies, and knowledge of best practices when developing technology that is respectful of the privacy and security of people who have CD. Future research will build on this first step by further examining how such best practices ought to be identified and then disseminated to developers.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

This work was supported by AGE-WELL Networks of Centres of Excellence of Canada (NCE) under its Catalyst Program (April 2017) – *Implementing changes in technology development practices that protects users' security and privacy* (AWCAT - 2017- 109)

Guarantor

[Omitted for blind review]

Contributorship

The following is a list of authors in order of the magnitude of their contribution. All authors approved the final version of the manuscript.

- VC: Supervision of all the activities as project lead, study conception, manuscript writing
- KC: Data analysis, manuscript writing
- HC: Study conception and design, data collection, data analysis, manuscript writing
- AGP: Data collection, manuscript writing
- HA: Data collection, data analysis, manuscript writing
- JJ: Study conception and design, critical revision
- KK: Study conception and design, critical revision
- AG: Study conception and design, critical revision
- FB: Data collection, drafting the manuscript

Acknowledgements

This work was supported by AGE-WELL NCE, a national network whose mission is to develop a community of researchers, older adults, caregivers, partners and future leaders that accelerates the delivery of technology-based solutions that make a meaningful difference in the lives of Canadians. AGE-WELL is a member of the Networks of Centres of Excellence (NCE), a Government of Canada program that funds partnerships between universities, industry, government and not-for-profit organizations.

ORCID iD

Virginie Cobigo https://orcid.org/0000-0001-8174-4770

References

1. Bohman PR and Anderson S. A conceptual framework for accessibility tools to benefit users with cognitive disabilities. In: *Proceedings of the 2005 international cross-disciplinary workshop on web accessibility* (W4A). pp. 85–89. New York: ACM, 2005.
2. Graham JE, Rockwood K, Beattie BL, et al. Prevalence and severity of cognitive impairment with and without dementia in an elderly population. *Lancet* 1997; 349: 1793–1796.
3. Plassman BL, Langa KM, Fisher GG, et al. Prevalence of cognitive impairment without dementia in the United States. *Ann Intern Med* 2008; 148: 427–434.
4. Kottorp A. Occupation-based evaluation and intervention : validity of the assessment of motor and process skills when used with persons with mental retardation, http://urn.kb.se/resolve?urn = urn:nbn:se:umu:diva-94111 (2003, accessed 30 November 2019).
5. Kottorp A, Bernspång B and Fisher AG. Activities of daily living in persons with intellectual disability: strengths and limitations in specific motor and process skills. *Aust Occup Ther J* 2003; 50: 195–204.
6. Hendricks DR and Wehman P. Transition from school to adulthood for youth with autism spectrum disorders: review and recommendations. *Focus Autism Dev Disabil* 2009; 24: 77–88.
7. Moser I. Disability and the promises of technology: technology, subjectivity and embodiment within an order of the normal. *Inf Commun Soc* 2006; 9: 373–395.
8. Rocheleau JN, Cobigo V and Chalghoumi H. Recognizing everyday information technologies as assistive technologies for persons with cognitive disabilities. In: Miesenberger K and Kouroupetroglou G (eds)

Computers helping people with special needs. Berlin: Springer International Publishing, 2018, pp.504–508.
9. Chalghoumi H, Cobigo V and Jutai J. Ethical issues related to IT adoption by elderly persons with cognitive impairments. *Stud Health Technol Inform* 2017; 242: 59–63.
10. Holmes KM and O'Loughlin N. The experiences of people with learning disabilities on social networking sites. *Br J Learn Disabil* 2014; 42: 1–5.
11. Löfgren-Mårtenson L. Love in cyberspace: Swedish young people with intellectual disabilities and the internet. *Scand J Disabil Res* 2008; 10: 125–138.
12. McClimens A and Gordon F. People with intellectual disabilities as bloggers: what's social capital got to do with it anyway? *J Intellect Disabil* 2009; 13: 19–30.
13. Didden R, Scholte RHJ, Korzilius H, et al. Cyberbullying among students with intellectual and developmental disability in special education settings. *Dev Neurorehabilitation* 2009; 12: 146–151.
14. Shpigelman C and Gill CJ. Facebook use by persons with disabilities. *J Comput Commun* 2014; 19: 610–624.
15. Cannon JC. *Privacy: what developers and IT professionals should know*. Boston: Addison-Wesley Professional, 2004.
16. Cavoukian A. Privacy by design in law, policy and practice. *White Pap Regul Decis-Mak Policy-Mak*, 2011 Aug.
17. Sauer AL, Parks A and Heyn PC. Assistive technology effects on the employment outcomes for people with cognitive disabilities: a systematic review. *Disabil Rehabil Assist Technol* 2010; 5: 377–391.
18. Balebako R, Marsh A, Lin J, Hong JI, Cranor LF. The privacy and security behaviors of smartphone app developers, 2014.
19. Melenhorst A-S, Fisk AD, Mynatt ED, et al. Potential intrusiveness of aware home technology: perceptions of older adults. *Proc Hum Factors Ergon Soc Annu Meet* 2004; 48: 266–270.
20. Wild K, Boise L, Lundell J, et al. Unobtrusive in-home monitoring of cognitive and physical health: reactions and perceptions of older adults. *J Appl Gerontol* 2008; 27: 181–200.
21. Stock SE, Davies DK, Wehmeyer ML, et al. Emerging new practices in technology to support independent community access for people with intellectual and cognitive disabilities. *NeuroRehabilitation* 2011; 28: 261–269.
22. Perry J, Beyer S and Holm S. Assistive technology, telecare and people with intellectual disabilities: ethical considerations. *J Med Ethics* 2009; 35: 81–86.
23. Graham ID, Logan MB, Harrison SE, et al. Lost in knowledge translation: time for a map? *J Contin Educ Health Prof* 2006; 26: 13–24.
24. Graham ID and Tetroe JM. Getting evidence into policy and practice: perspective of a health research funder. *J Can Acad Child Adolesc Psychiatry J Acad Can Psychiatr Enfant Adolesc* 2009; 18: 46.
25. August S. Integrating users into product development, https://faculty.washington.edu/wobbrock/press/useful.pdf (2004, accessed 5 August 2020).
26. The role of user experience in the product development process. UXmatters, www.uxmatters.com/mt/archives/2014/05/the-role-of-user-experience-in-the-product-development-process.php (accessed 30 November 2019).
27. Herold R. *Managing an information security and privacy awareness and training program*. Hoboken: Hoboken CRC Press, 2010.
28. Grol R and Wensing M. Effective implementation of change in healthcare: a systematic approach. In: Michel W, Richard G, Jeremy G (eds) *Improving patient care implementation of change health care*. United states: John Wiley & Sons Ltd. 2013, pp. 40–63.
29. Nilsen P. Making sense of implementation theories, models and frameworks. *Implement Sci IS* 2015; 10: 53.
30. Cobigo V, Chalghoumi H and Gauthier-Beaupré A. A scan of Canadian privacy laws and related information materials for technology developers, https://rise.articulate.com/share/Xc7_NcbXb9C3TGhguJLD919W4JLZyME- (2018, accessed 5 August 2020).
31. The Future of Technology and Aging Research in Canada, https://agewell-nce.ca/wp-content/uploads/2018/05/Booklet_8_Challenges_English_2019oct2_digital.pdf (2019, accessed 22 May 2020).
32. Miles MB, Huberman AM and Saldaña J. *Qualitative data analysis: a methods sourcebook*. 3rd ed. Thousand Oaks, CA: Sage, 2014.
33. Fereday J and Muir-Cochrane E. Demonstrating ZT. *Int J Qual Methods* 2006; 5: 80–92.
34. Thomas DR. A general inductive approach for analyzing qualitative evaluation data. *Am J Eval* 2006; 27: 237–246.
35. Corbin J, Strauss A. Basics of qualitative research: Techniques and procedures for developing grounded theory. CA, US: Sage Publications, 2008
36. Rogers BL and Cowles KV. The qualitative research audit trail: a complex collection of documentation. *Res Nurs Health* 1993; 16: 219–226.
37. Walker AK and Fox EL. Why marginalization, not vulnerability, can best identify people in need of special medical and nutrition care. *AMA J Ethics* 2018; 20: E941–E947.
38. Milne A. *The 'D'word: reflections on the relationship between stigma, discrimination and dementia*. Milton Park: Taylor & Francis, 2010.
39. Czechowski K, Sylvestre J, Moreau K. Secure Data Handling: An Essential Competence for Evaluators. *Canadian Journal of Program Evaluation* 2019; 34(1): 139–151.
40. Cavoukian A. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity Inf Soc* 2010; 3: 247–251.
41. O'Connor Y, Rowan W, Lynch L, et al. Privacy by design: informed consent and internet of things for smart health. *Procedia Comput Sci* 2017; 113: 653–658.
42. Chalghoumi H, Cobigo V, Dignard C, et al. Information privacy for technology users with intellectual and developmental disabilities: why does it matter? *Ethics Behav* 2019; 29: 201–217.
43. Cameron L, Murphy J. Obtaining consent to participate in research: the issues involved in including people with a

range of learning and communication disabilities. *Br J Learn Disabil* 2007; 35: 113–120.
44. Cobigo V, Potvin LA, Fulford C, et al. A conversation with research ethics boards about inclusive research with persons with intellectual and developmental disabilities. *Res Involv Particip Cogn Disabil Differ Ethics Auton Incl Innov* 2019; 185.
45. Bravo G, Pâquet M and Dubois M-F. Opinions regarding who should consent to research on behalf of an older adult suffering from dementia. *Dementia* 2003; 2: 49–65.
46. Dye L, Hendy S, Hare DJ, et al. Capacity to consent to participate in research – a recontextualization. *Br J Learn Disabil* 2004; 32: 144–150.
47. Assal H and Chiasson S. 'Think secure from the beginning': a survey with software developers. In: *Proceedings of the 2019 CHI conference on human factors in computing systems,* p. 289. New York: ACM, 2019.
48. Palm E and Hansson SO. The case for ethical technology assessment (eTA). *Technol Forecast Soc Change* 2006; 73: 543–558.

Appendix 1. Semi-structured interview guide

Section A: Introduction

At the beginning of each interview, we will remind participants about the topic of the interview:

> Thank you for agreeing to participate in this interview. As a reminder, we want to hear about your practices to protect the privacy of technology users, and especially those with cognitive impairments.

Next, we will review the participant's consent to record the interview and to participate in the project:

- Do you have any questions regarding the project and/or your participation?
- We would like to record the interview to ensure the accuracy of our data. Do we have your permission?
  - ○ Your name will be removed from the transcript.
  - ○ Only the research team on this project will have access to the audio recording and transcript of this interview.

(If affirmative, start recording)

- Do you agree to participate in this interview?
  - ○ Please note that you can stop at any time.
  - ○ You do not have to answer all our questions.

Section B: Questions about current practices

Demographics.

1. What is your professional title, related project and industry, province and country (if applicable)?
2. What types of products do you develop?
3. What platforms do you develop for?
4. In the survey, you told us that you have developed OR are developing any technologies for which the target market includes persons with cognitive impairments. Could you tell us more about the product(s)?

Note for the interview: adapt the following questions to focus on the product(s) described.

General.

1. In general, what steps do you take to protect users with cognitive impairments' privacy and security?
2. Do you consider potential privacy and security breaches when developing your products? If so, how does that impact your product development? And your product commercialization?

Data collection practices.

1. What data do you collect from users?
2. How do you decide what data to collect from users?
3. How does your business model drive what data you collect from users?
4. Which analytics or API do you use, if any?
   - ○ *Note: API stands for "Application Programming Interface". It is a code that allows two software to communicate with each other.*
5. What data does the analytic company collect from users through your app?
6. How do users know what information you are collecting?
7. What information that you collect could be considered "private" or "personal" by your users?
8. Do you think users would be surprised by any of the information you collect?

Compliance with Canadian privacy regulations recommendations.

1. Do you have a privacy policy? If so, how can users access it?
2. Do you provide just-in-time disclosures about data collected?
3. Do you participate in any trade association, self-regulatory program, or industry organization that provides guidance on privacy disclosures?

Trade-offs.

1. Have you ever decided not to collect certain information from users due to privacy concerns? If so, tell me about it.
2. Have you ever decided to collect more data from users than necessary due to business concerns? If so, tell me about it.

Resources.

1. Is there anyone that you turn to when you have questions about consumer privacy and security? (e.g. staff, lawyer, advice from other developers). If so, who?
2. Do you use any online resources (e.g., training, websites) to help make privacy and security decisions? If so, what resources do you use?
3. Do you use any tools (e.g. software development kits, apps, government resources, etc.) to help with privacy and security implementation or decisions? If so, what tools do you use?

Section C: Conclusion

We will conclude each interview session by doing the following:

- Offer to send the findings of the study to the participant if they are interested.
- Ask the participant if they have any feedback for improving the interview.
- Thank the interviewee for their participation and effort. Ask if we could contact them again to clarify the content of the interview if needed.
- Inform the participant about the next step in the project, and ask them if they would be interested in contributing:
- The next step of the project is to develop and embark in a process that supports technology developers in their efforts to respect and protect the privacy of users with cognitive impairments. Could we contact you again to tell you more about the next steps of the project, and ask if you would be interested to contribute?

If a participant would like to withdraw:

- If a participant would like to withdraw and does not want us to use the collected data, they can do so at any moment.