Digital privacy of smartphone camera-based assistive technology for users with visual disabilities

Hyung Nam Kim

North Carolina A&T State University,
Greensboro, NC 27411, USA
Email: hnkim@ncat.edu

Abstract: Smartphone users with visual disabilities often use camera-based assistive technology applications such as Seeing AI, BeMyEyes, and TapTapSee apps in identifying people and objects. As personal information could be shared, digital privacy issues are critical to those with visual disabilities. However, little is known about user perspectives on digital privacy issues – e.g., the degree to which those with visual disabilities understand user privacy policies and the degree to which they intend to adopt those apps. To address the knowledge gap, this study conducted interviews with a convenience sample of 30 participants with visual disabilities. The results indicate that those with visual disabilities had a lack of knowledge about privacy policies and potential risks of privacy and security breaches of personal information. The results contributed to forming a conceptual framework that contains a list of facilitators and barriers to user adoption, which could serve as a knowledge foundation for many other researchers and professionals to support and enhance users' privacy awareness, accessible to users with visual disabilities.

Keywords: visual impairment; blindness; user privacy; assistive technology; smartphone camera.

Reference to this paper should be made as follows: Kim, H.N. (2023) 'Digital privacy of smartphone camera-based assistive technology for users with visual disabilities', *Int. J. Human Factors and Ergonomics*, Vol. 10, No. 1, pp.66–84.

Biographical notes: Hyung Nam Kim is an Assistant Professor in the Department of Industrial and Systems Engineering at the North Carolina A&T State University. He earned his PhD in Industrial and Systems Engineering from Virginia Tech. His research interests include human factors, safety, health informatics, and human-computer interaction.

1 Introduction

1.1 Smartphone camera-based assistive technology applications

Today, a great number of users with visual disabilities gain benefits from mainstream technologies using assistive technologies. We should not ignore them or merely consider them as minorities in cyberspace. In 2015 a survey report (Anderson, 2015) uncovered that 68% of general populations in the USA have a smartphone, while a national survey (Morris et al., 2016) in 2016 found that 71% of Americans with disabilities have a

smartphone. Facebook users with visual disabilities actively engage in online social networking (e.g., posting status updates, comments, and likes), which is not significantly different from sighted users, and receive more feedback (i.e., comments and likes) from other users (Wu and Adamic, 2014). Smartphone users with visual disabilities often rely on camera-based assistive technology applications; for example, Seeing AI, TapTapSee, and BeMyEyes apps are the mostly commonly used camera-based assistive technology apps among people with visual disabilities (Dockery and Krzystolik, 2020). They use those apps for navigating spaces, identifying objects or colour, recognising faces or facial expressions, and reading documents. The apps rely on automated systems (e.g., a computer vision equipped with machine learning) or human-powered systems equipped with real human assistants (e.g., online volunteers). Those camera-based apps should be working effectively when users successfully capture a high-quality photo with ample lighting and the correct angle and position. As people with visual disabilities would be challenging to aim the camera onto a target object correctly due to vision loss, several researchers have made effort to address the challenge such that the apps could automatically guide users to proper lighting, angle, and position (Adams et al., 2013; Jayant et al., 2011; Vázquez and Steinfeld, 2014). The Seeing AI app, for example, is equipped with artificial intelligence (AI) such that users with visual disabilities can readily use the camera to identify people, text, colour, barcode, currency, scene, and any objects in real time. The TapTapSee app is powered by the image recognition application programming interface (API) that recognises, captions, and classifies the details of an image within seconds. In addition to the camera, the TapTapSee app requires a built-in screen reader (e.g., VoiceOver) so that it can take a picture (or video) of anything and identify it out loud for users with visual disabilities. Users with visual disabilities can also obtain real-time assistance from online volunteers who are virtually connected through the BeMyEyes app. Users with visual disabilities can use the smartphone camera to show objects to volunteers in real time – those who are untrained volunteers for a free service – and then the volunteers identify objects on behalf of the users.

1.2 Privacy concerns

People with visual disabilities are concerned about privacy. They typically ask family and friends for help to read texts, recognise objects, and better understand surroundings. Yet, they would often be hesitant due to privacy issues even though those helpers are their close allies (Hayes et al., 2019). As technology advances today, people with visual disabilities use a variety of emerging technologies to obtain help even from non-allies (including computing systems) (Kim, 2018, 2021; Wong, 2018). People with visual disabilities may happen to share personal information (tax documents, medical records, and financial statements) via live videos or photos. As much as they obtain help, the likelihood of a data breach is also increasing. For example, visual malware programs (e.g., *PlaceRider*) enable remote attackers to conduct a virtual theft via a phone camera by targeting a phone user's personal information (Templeman et al., 2012). Users with visual disabilities are more vulnerable to cyber-attacks because they have limited access to visual cues and software support systems that help users to be aware of potential cybersecurity threats (Inan et al., 2016). Inan et al. (2016) surveyed 20 people with visual disabilities, 80% of whom reported they were 'concerned' or 'very concerned' about cybersecurity threats and privacy. Their concerns include "someone stealing private information about me and my family (70%)", "someone gaining access to my financial

information (65%)", and "my personal information being made public (65%)". It is not uncommon today to be heard of data breaches, e.g., cybercriminals have stolen the usernames and passwords of 3 billion Yahoo users (Larson, 2017a), financial information of 143 million Americans from Equifax (Gressin, 2017), private data of 57 million Uber users (Larson, 2017b), 530 million Facebook users (Bowman, 2021), and 538 million Weibo users (Cimpanu, 2020). A national survey of 6,000 Americans (Ablon et al., 2016) found that 44% of respondents recalled receiving a data breach notification in their lives and 26 % did so in the 12 month-period prior to the survey, which were associated with credit card details (49%), health information (21%), social security numbers (17%), and user account information (13%).

A range of cases have been reported associated with the privacy risks for users with visual disabilities. For example, people with visual disabilities are vulnerable to aural and visual eavesdropping when they use screen readers and magnifiers (Wang et al., 2019). People with visual disabilities use a screen reader that often reads out loud enough for bystanders to overhear what users read (or type) (Ahmed et al., 2015; Azenkot et al., 2012). Those with visual disabilities are also concerned that somebody could hack their smart technologies with cameras to sneak a look at them (Kim, 2021). With regard to the camera-based assistive technology apps, those with visual disabilities may not review and screen out the contents of videos/photos before sharing with online volunteers and/or computing systems as they cannot see. Gurari et al. (2019) also studied the degree to which people with visual disabilities are vulnerable to being exposed to privacy risks. They examined over 40,000 images taken by people with visual disabilities while using a smartphone camera-based assistive technology. They found that over 10% of the images contained personal information (e.g., medical, financial, login credentials, and faces of other people). They also reported that over 50% of privacy leaks occurred when those with visual disabilities compromised their privacy to obtain help with understanding information that is not accessible to them. In addition to users with visual disabilities, bystanders (e.g., their family and friends) were subject to privacy issues as users with visual disabilities could capture faces of bystanders while using the camera-based apps (Ahmed et al., 2018). Higher security assurances are necessary with regard to the use of assistive technology. Akter et al. (2020) conducted a survey study to explore the degree to which people with visual disabilities feel comfortable with using camera-based assistive technologies. Akter et al. found that those with visual disabilities were concerned about the privacy of bystanders as they might unintentionally capture and share bystanders' personal information with others. Those with visual disabilities were also concerned about their own personally identifiable information being targeted for identity theft. As compared to those with residual vision (or low vision), those with blindness were found to be less concerned about their privacy issues. Akter et al. argued that those with blindness might be more likely to compromise their privacy because their vision was severely visually impaired, leading to no other option but heavily relying on assistive technologies for independent living. It infers that independent living may be more critical than privacy protection among those with blindness.

Privacy issues could also be caused by human agents working between users and computing systems. For example, the BeMyEyes app is operated with assistance from volunteers who will virtually connect with users and help to read texts, identify objects, and so on via a phone camera. Yet, as the volunteers are not professionally trained but just random people online, users with visual disabilities are likely to be vulnerable to privacy issues. More specifically, the BeMyEyes app is powered by crowdsourcing-based

systems. There are many other applications running on crowdsourcing-based systems where other individuals are willing to identify things on behalf of users through a computer vision/camera such as VizWiz (Bigham et al., 2010), Chorus:View (Lasecki et al., 2013b), Legion:Scribe (Lasecki et al., 2012), Soylent (Bernstein et al., 2010), Legion:AR (Lasecki et al., 2013a), adrenaline (Bernstein et al., 2011), and chorus (Lasecki et al., 2013c). Yet, there are several reports indicating privacy problems that occurred to people with visual disabilities using the crowdsourcing assistive technologies (Ahmed et al., 2016; Gurari et al., 2019). Lasecki et al. (2014) demonstrated the vulnerability of existing crowdsourcing practices to personal information extracting and manipulating threats caused by volunteers online.

Although digital privacy issues are critical to those with visual disabilities, little attention has been paid to those with visual disabilities. Ahmed et al. (2015) conducted a systematic literature review and suggested that a research study by Azenkot et al. (2012) was one of the first to pay attention to the privacy risks toward mobile device users with visual disabilities, and it has been only ten years. Wang (2017) pointed out that there are three waves for research and development (R&D) in the field of user privacy and security. The first wave was to focus on system enhancements, while the second wave was to focus on usability since the 70's in which human factors and usability were recognised as a key factor contributing to effective security and privacy mechanisms. The newly emerging third wave focuses on 'inclusive security and privacy' where security and privacy issues are set to equally consider the needs of people with various abilities/disabilities (Wang, 2017). This third wave is centred around considering human abilities/disabilities as core system requirements to meet a range of different human needs, ultimately leading to 'inclusive designs for all' regardless of human characteristics, identities, and values.

1.3 Digital privacy literacy

Privacy policies are a set of legal agreements that describe to users what personal information is gathered, how it is collected, where they are stored, how it is used, and how it is shared. Many users tend to pay less attention to digital privacy policies before and even when using technology applications. A national survey by the Pew Research Center (Smith, 2014) found that half of online Americans do not know what a privacy policy is. Many users are aware that digital privacy is important and should be protected; however, they do not know in detail about it. It is well documented that privacy policies are often difficult for users to understand because the privacy policy statements are too technical (Kelley et al., 2010; Krumay and Klar, 2020; Meiselwitz, 2013; Schaub et al., 2017). This study pays attention to the concern that users with visual disabilities may be unable to easily find the webpage containing the privacy policies; encounter accessibility problems in reading the privacy policy statements; have difficulty in understanding them; and/or be unsure how the policies are exactly applied to their actual uses, all of which are associated with digital privacy literacy (Park, 2013). Wang and Price (2022) argued that many end-user privacy tools tend to be inaccessible to users with visual disabilities, such that those users often encountered challenges with managing their privacy. Inan et al. (2016) examined security awareness in people with visual disabilities and found a negative correlation of their awareness with 'cybersecurity concerns' as well as with "the frequency of internet activities". It suggests that those with a lower level of cybersecurity knowledge and skills are more likely to suffer from cybersecurity threats and be afraid of

using digital technologies, probably leading to technology abandonment and digital divide among people with disabilities. The latest research by Stangl et al. (2022) reviewed user privacy policy statements of companies that provide services to people with visual disabilities – e.g., Facebook, Apple, Amazon, Adobe, Microsoft, Google, screen readers, and camera-based assistive technologies. They found that the privacy policy statements were inadequately designed in informing users with visual disabilities about how user data are collected, retained, used, and disseminated. Yet, the study of Stangl et al. (2022) was based on an archival research method without directly interviewing users with visual disabilities, which has motivated the present study to make an effort to obtain much deeper understanding of how users with visual disabilities perceive, understand, and apply the user privacy policies of the camera-based assistive technologies.

This study aims to address the knowledge gap by conducting interviews that include people with visual disabilities who use the camera-based assistive technology apps and prospective users who have not used the apps but are interested in using them in the future. In addition, this study makes an effort to observe the degree to which those with visual disabilities change their tendency to adopt the apps after being educated on user privacy policies (e.g., safety measures and potential risks).

2 Methods

2.1 Participants

Inclusion criteria were English speaking, 18 years old or older, visual acuity 20/70 or poorer (World Health Organization, 2008), and user experience with Seeing AI, BeMyEyes, and TapTapSee apps. Participants were recruited with support from community organisations, e.g., community centres and a public library for people with visual disabilities. They informed their community members about the opportunity to participate in this study. Potential participants who were interested in this study contacted the research team. A convenience sample of 24 individuals with visual disabilities was invited to this study by phone. In addition, this study invited six individuals with visual disabilities as prospective users who have not used any of the three apps but were interested in using them. Thus, a total of 30 participants with visual disabilities contributed to this study (see Table 1). Verbal informed consent was obtained from each individual participant.

Table 1 Characteristics of the participants

Participants	*(n = 30)*
Visual acuity	
Between 20/200 and 20/400	9
Between 20/400 and 20/1200	4
Less than 20/1200, but has light perception	15
No light perception at all	2
Duration of vision loss (years)	17.63 ± 23.11

Note: [a]Participants with early-onset of vision loss had lost their sight before 11 years of age

Source: Voss et al. (2004)

Table 1 Characteristics of the participants (continued)

Participants	*(n = 30)*
Onset of vision loss (years)a	
Early onset	9 (0.4 ± 1.26)
Late onset	21(45.81 ± 17.13)
Age (years)	59.7 ± 17.84
Gender	
Male	13
Female	17
Race/Ethnicity	
African American	13
European American	15
Others	2
Education	
High school or equivalent	12
Associate	7
Bachelors	5
Masters	6
Seeing AI user	7
BeMyEyes users	11
TapTapSee users	6
Prospective users	6

Note: [a]Participants with early-onset of vision loss had lost their sight before 11 years of age

Source: Voss et al. (2004)

2.2 Materials

A handful of user privacy policy statements were extracted from each app's homepage. Those privacy policy statements were distinctively different from each other as they were located under the distinctive headings of user privacy policies in each app's homepage. Thus, seven policy statements were selected for the Seeing AI app, 13 statements were for the TapTapSee app, and 22 statements were for the BeMyEyes app. The policy statements were converted into true-or-false quizzes. Samples of the true-or-false statements include: "If you register through a third party account like Facebook or Google, then we will collect the information that you allow us to collect via the controls offered by your account with that provider", "We may analyze stored video streams and provide copies of video streams to other companies that are working to develop products and services that may help the visually impaired or other members of the general public", and "We may transfer information that we collect about you, including personal information across borders and from your country or jurisdiction to other countries or jurisdictions around the world." In addition, seven inquiries to assess the participants' tendency to adopt the apps (i.e., technology adoption questionnaire) were adopted from

the work by Gao et al. (2011). The inquiries were related to the privacy issues; for example, “I could use the system if the system protects the privacy of its users”, “I could use the system if I feel confident that I can keep the system under control”, and “I could use the system if it is safe to use the system”. Participants would respond to each inquiry on a seven-point Likert type scale from ‘strongly disagree’ to ‘strongly agree’.

2.3 Procedures

An interviewer read out loud each privacy quiz question to participants, and participants chose true or false in response to each question. After completing the quiz, the interviewer reviewed the answers along with participants, i.e., the opportunity to educate them about user privacy policies. Participants were instructed to respond to the adoption tendency inquiries before and after quiz, which could help to examine how much the understanding of online privacy policies would influence the future use of the apps. All participants were asked to complete all the quizzes of user privacy policies that were assigned to not only the target app but also the other apps. For example, the user group of the TapTapSee app was assessed on the degree to which they were knowledgeable about the TapTapSee app’s user privacy policies, but also the user groups of the other apps (Seeing AI and BeMyEyes apps) were assessed on their knowledge about the TapTapSee app’s user privacy policies. The prospective user group was also assessed about the TapTapSee app’s user privacy policies. By doing so, this study was able to comprehensively assess and compare the level of the target user group’s knowledge from various aspects.

2.4 Data analysis

2.4.1 Quiz

- *Quiz scores between users of each app (i.e., target users)*. Each user group of the three apps (Seeing AI, BeMyEyes, and TapTapSee apps) completed the quiz that was set to assess the knowledge level of each target app’s user privacy policies. In this study, each user group was named as ‘target users’. The mean values of the quiz scores between each target user group were compared via Kruskal-Wallis tests, followed by a post-hoc analysis with Mann-Whitney tests.
- *Quiz scores between the target users, the users of the other apps, and the prospective users*. While the quiz for a particular app’s privacy policies was completed by its target user group but also the other user groups (i.e., those who did not use the particular app but the other apps). Thus, we were able to investigate the effect of ‘indirect experience’ (i.e., use of similar camera-based apps) on the knowledge level of the particular app’s user privacy policies. In addition, the quiz for a particular app’s privacy policies was completed by prospective users (i.e., those who did not use the app but would like to use it in the future), such that we were able to investigate the effect of ‘non-experience’ on the knowledge level of the particular app’s user privacy policies.
- *Quiz scores to assess user understanding of the target app’s user privacy policies*. The quiz scores were also used to assess the degree to which the target users understand the user privacy policies of the target app. As no norm exists to determine

whether their knowledge level is good or poor, we relied on a quartile that helps to measure the spread of observed values from the mean score. A quartile divides data into three points, i.e., the lower quartile, median, and upper quartile. In this study, the quiz scores under the lower quartile were considered to represent poor understanding of the user privacy policies.

2.4.2 Adoption tendency questionnaire

The quiz was set to not only evaluate participants' knowledge level of user privacy policies but also inform participants about their quiz scores and educate them. Thus, participants' responses to the technology adoption questionnaire were analysed to assess whether there was a significant difference before and after the quiz, which was accomplished using Wilcoxon Signed Rank tests.

2.4.3 Content analysis

The present study relied on the inductive content analysis that focuses on the process of exploring a phenomenon. The interview transcripts were thus analysed by conducting open coding, axial coding, and selective coding. Another coder was invited to assess the inter-rater reliability using Cohen's kappa statistic. There was substantial agreement among the raters as the inter-rater reliability was found to be $\kappa = 0.93$ (95% CI: .80 to 1.06).

3 Results

This study found significant differences in the quiz scores (i.e., participants' knowledge level of user privacy policies) and the adoption tendency levels before and after the quiz-based education session. The qualitative interview data analysis yielded a deep understanding of the participants' user experience with those apps and their perspectives on trust and concerns about digital privacy. The details are presented below.

3.1 Quiz

3.1.1 Quiz scores between users of each app (i.e., between target users)

Kruskal-Wallis tests found that there were significant differences in the quiz scores between the Seeing AI, BeMyEyes, and TapTapSee target user groups (see Table 2). A post-hoc analysis with Mann-Whitney tests found that the quiz score of the TapTapSee target user group was significantly lower than that of the other target user groups (i.e., Seeing AI and BeMyEyes target user groups).

Table 2 Quiz scores compared between target user groups of each app

	Quiz scores		*Kruskal-Wallis tests*		
	Mean	*SD*	χ^2	*df*	*p*
Target users of Seeing AI app	0.82	0.39	13.92	2	< 0.01
Target users of BeMyEyes app	0.85	0.36			
Target users of TapTapSee app	0.65	0.48			

Table 2 Quiz scores compared between target user groups of each app (continued)

Post-hoc pairwise comparisons	*Mann-Whitney tests*		
	U	*z*	*p*
TapTapSee vs. Seeing AI	1,600.50	–2.00	< 0.05
TapTapSee vs. BeMyEyes	7,614.00	–3.70	< 0.01
Seeing AI vs. BeMyEyes	5,746.50	–0.50	0.59

3.1.2 Quiz scores between the target users, the users of the other apps, and the prospective users

Kruskal-Wallis tests found a significant difference in the quiz scores, with regard to the *TapTapSee app's privacy policies*, between the three user groups – the TapTapSee target user group, the user group of the other apps, and the prospective user group (see Table 3). A post-hoc analysis with Mann-Whitney tests found that the quiz score of the TapTapSee target user group was significantly lower than that of their peer groups (i.e., the user group of the other apps and the prospective user group), although the TapTapSee user group was one who had actual experience with the TapTapSee app.

Table 3 Quiz scores compared within each app

	Quiz scores of target users		*Quiz scores of users of the other apps*		*Quiz scores of prospective users*		*Kruskal-Wallis tests*		
	Mean	*SD*	*Mean*	*SD*	*Mean*	*SD*	χ^2	*df*	*p*
Seeing AI app	0.82	0.39	0.78	0.41	0.76	0.43	0.43	2	0.81
BeMyEyes app	0.85	0.36	0.81	0.39	0.89	0.31	4.33	2	0.12
TapTapSee app	0.65	0.48	0.78	0.41	0.85	0.36	8.64	2	<0.05

Post-hoc pairwise comparisons	*Mann-Whitney tests*		
	U	*z*	*p*
Target users of the TapTapSee app vs. Users of the other apps	7,956	–2.26	<0.05
Target users of the TapTapSee app vs. Prospective users	2,457	–2.77	<0.01
Users of the other apps vs. prospective users	8,544	–1.22	0.22

3.1.3 User privacy policies

The lower quartile (Q1) was found to be 0.67. As shown in Table 4, among the Seeing AI target users, one of 7 quiz questions (14%) was scored below Q1; among the BeMyEyes target users, two quiz questions (9%) were scored below Q1; and among the TapTapSee target users, 11 quiz questions (85%) were scored below Q1.

Table 4 User privacy policies indicating a lower level (Q1) of knowledge by each app's target users

App	*Category*	*User privacy policy*
Seeing AI	How to access and control your personal data	You can also make choices about the collection and use of your data by Microsoft. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law.
BeMyEyes	How we use and share information	If we ever use a third party to help us provide our services and if that third party needs access to your personal information in order to help us provide the service, we will share the information with them.
		We may share your contact information with non-profit organisations that advocate for or support people who are visually impaired ('support organisations') that may use the information to contact you or make you aware of the services they offer.
TapTapSee	Information we collect	We use third-party analytics tools to help us measure traffic and usage trends for the service. These tools collect information sent by your device or our service, including the web pages you visit, add-ons, and other information.
		When you visit the TapTapSee, we may use cookies and similar technologies to collect information about how you use the TapTapSee. We may ask advertisers or other partners to serve ads or services to your devices, which may use cookies or similar technologies placed by us or the third party.
		When you use our TapTapSee, our servers automatically record certain log file information, including your web request, your internet protocol ('IP') address, your browser type, referring / exit pages and URLs, number of clicks and how you interact with links on the Service, domain names, landing pages, pages viewed, and other such information. We may also collect similar information from e-mails sent to you, which then help us track which e-mails are opened and which links are clicked by recipients.
		A device identifier may deliver information to us or to a third-party partner about how you browse and use the service and may help us or others provide ads.
	Sharing of your information	We may share your information as well as information from tools like cookies, log files, and device identifiers and location data (such as usage data, referring/exit pages and URLs, platform types, number of clicks, etc.), with organisations that help us provide the service to you ('Service Providers').
		We may license the image data of yours to outside companies or organisations for their internal use. No user IDs or any other personally identifying metadata will be attached along with the images though.

Table 4 User privacy policies indicating a lower level (Q1) of knowledge by each app's target users (continued)

App	*Category*	*User privacy policy*
TapTapSee	Sharing of your information	If we sell or otherwise transfer part or the whole of TapTapSee or our assets to another organisation (e.g., in the course of a transaction like a merger, acquisition, bankruptcy, dissolution, liquidation), your information (such as name and e-mail address, user content and any other information collected through the service) may be among the items sold or transferred.
	How we store your information	The images taken by you are stored indefinitely.
		Your information collected through the service may be stored and processed in the USA or any other country in which TapTapSee, a company in the same group of companies as TapTapSee or Service Providers maintain facilities.
		TapTapSee may transfer information that we collect about you, including personal information across borders and from your country or jurisdiction to other countries or jurisdictions around the world.
	Your choices about your information	TapTapSee may retain information and User Content for a commercially reasonable time for backup, archival, and/or audit purposes.

3.2 Adoption tendency questionnaire

As shown in Table 5, Wilcoxon Signed-Rank tests found that there were significant differences in the tendency to adopt the apps before and after the quiz-based education. Both user groups of the Seeing AI app and the BeMyEyes app showed greater tendency to adopt the apps after quiz. Yet, the user group of the TapTapSee app did not significantly change their tendency to adopt the app in that they always maintained the highest level of tendency to adopt the app both before and after quiz. The prospective users (i.e., individuals without actual user experience) did not show a significant change in their tendency to adopt the apps between before and after quiz. The results suggest that the privacy education may not be a significant determinant for prospective users to decide on whether to adopt the apps; however, the privacy education can be considered as a significant determinant for experienced users (users of Seeing AI and BeMyEyes apps, except users of TapTapSee app) to adopt the apps, leading to increased adoption tendency with trust in privacy.

Table 5 Participants' tendency to adopt the Seeing AI, the TapTapSee, and the BeMyEyes apps

	Tendency to adopt the app		*Wilcoxon tests*	
	Before quiz	*After quiz*	*Z*	*P*
	(Mean ± SD)	*(Mean ± SD)*		
Target users of the Seeing AI app	6.12 ± 0.57	6.53 ± 0.41	–2.20	0.03
Users of the other apps (BeMyEyes and TapTapSee)	6.84 ± 0.24	6.90 ± 0.16	–2.06	0.04

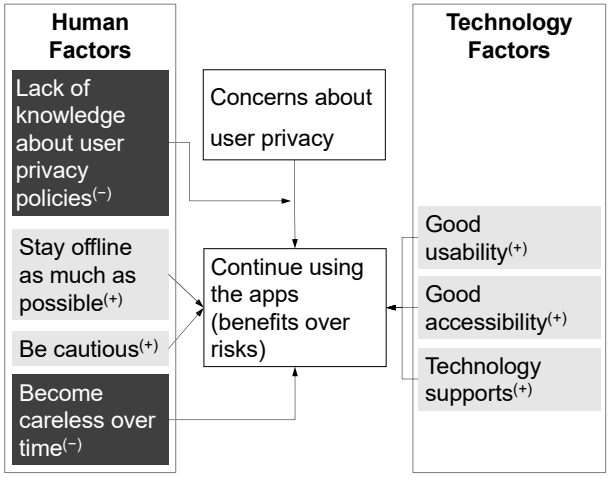
Table 5 Participants' tendency to adopt the Seeing AI, the TapTapSee, and the BeMyEyes apps (continued)

	Tendency to adopt the app		*Wilcoxon tests*	
	Before quiz	*After quiz*	*Z*	*P*
	(Mean ± SD)	*(Mean ± SD)*		
Target users of the BeMyEyes app	6.76 ± 0.26	6.84 ± 0.18	–2.06	0.04
Users of the other apps (Seeing AI and TapTapSee)	6.52 ± 0.61	6.75 ± 0.38	–2.21	0.03
Target users of the TapTapSee app	7.00 ± 0.00	7.00 ± 0.01	0.00	1.00
Users of the other apps (Seeing AI and BeMyEyes)	6.51 ± 0.50	6.72 ± 0.32	–2.97	< 0.01
Prospective users	6.67 ± 0.47	6.62 ± 0.93	0.00	1.00

3.3 Content analysis

The participants' exit interviews were analysed, resulting in nine themes. Approximately 63% of the participants' comments were associated with "personal interventions such as be cautious and stay offline as much as they can", 50% with "continue using the apps (benefits over risks)", 43% with "not easy to understand user privacy policy statements", 20% with "concerns about privacy and security", 13% with "good usability and accessibility required for trustworthiness", 7% with "feel scary and vulnerable", 7% with "good technology supports", and 3% with "becoming careless over time". As shown in Figure 1, their perspectives were visually presented as a framework explaining facilitators and barriers to user adoption.

Figure 1 Conceptual framework showing the participants' perspectives on user experience with the camera-based assistive technology applications: *facilitators (+) vs. barriers (–) to user adoption*



3.3.1 Concerns about user privacy

The participants explicitly expressed concerns about privacy issues with regard to the smartphone camera-based assistive technology apps. For example, they would like to use the apps that are safe from hackers stealing their personal information (P4, P11) but also, they did not want the app companies to share their personal information with any third-party organisations (P21, P22, P24). Another concern was that they were not comfortable with BeMyEyes volunteers seeing the password while they were typing (P1).

3.3.2 Lack of knowledge about user privacy policies

The quiz helped the participants to realise that they had a lack of understanding about the user privacy policies (P6, P9, P10, P18, P20, P21, P22, P24), e.g., "I did not know any of this stuff [user privacy policies] (P20)" and "Through the quiz, I have definitely learned in depth about what these privacy policies are. Now I understand why people should read them on their own, instead of taking other people's words for it (P6)". The participants also expressed their concerns that the privacy policy statements were not easy for them to understand, e.g., "I would make the statements [user privacy policy statements] much easier to understand (P14)", "It would probably be better if they [policy statements] were a little bit clearer about what information the app companies collect and how they use them (P21)". The participants were misinformed about the user privacy policies, e.g., P10 was introduced to the app by other people who informed P10 that no personal information would be stored or shared with any other organisations.

3.3.3 Continue using the apps, due to benefits over risks

The participants were aware of (or learned through the quiz) the risk of privacy breaches; however, they would like to keep using the apps (P4, P6, P7, P11, P12, P16, P18, P20, and P23). They believed that the benefits of using the apps would be greater than the potential risks, e.g., "The benefit I have gotten from the app has already far exceeded the risk of using the app (P7)", "I am okay with giving up those rights in order to use the apps (P20)", and "I would still keep using the app because the app is very helpful to me (being a blind person) to remain independent (P4)".

3.3.4 Good usability, accessibility, and technology supports

The participants would trust and adopt the apps if the apps could offer good usability and accessibility. For example, P9 stated "As long as you make them [the apps] accessible and easy to use, I would then confidently use them". The apps are designed to utilise the back camera in order to capture the data (e.g., people, texts, and objects that users intend to see). Thus, the participants felt safe to use the apps in that their face would not be captured unless they intentionally aim the camera onto their face. The participants stated "I would say that privacy is important. It is fairly safe because they [the apps] use the back camera (P8)" and "I like the fact that when the camera comes on, it is not facing me but the room. It does not see me. I like the fact that I am anonymous (P10)".

3.3.5 Personal interventions

The participants acknowledged that the apps helped them to be independent in daily life; however, they would like to be careful to protect their privacy. They believed that their participation in the quiz-based education was helpful for them to learn in depth about user privacy and potential risks. The participants stated "It [the quiz-based education] was an eye-opener. There are obviously ways people can get information about my IP number and all that personal information, but I did not know these apps could do it. I am surprised they were collecting them (P17)" and "I think the apps are great to use. When I lost vision, these apps helped me to do all the things on my own. I would still use them, but I would think about it [user privacy] before jumping in and using the apps (P3)". The participants employed their own interventions; for example, they avoid using the apps to identify a person or read personal information, as stated "I am not overly concerned about the user privacy because I have never used the apps in identifying people or personal information (P8)" and "If any important materials are stored on my device [personal computer and phone], I use the device when not connected with the internet (P2)".

3.3.6 Become careless over time

While the participants consciously paid attention to the user privacy and tried to be careful while using the apps, they also found themselves becoming careless over time as they got used to the apps. For example, P6 stated "If I feel comfortable using the apps, it will then make it a no-brainer to use. Once I feel safe and comfortable to use the apps, I do not pay attention to it. I do not think twice, but just use it".

4 Discussions

Users of the three apps were individually assessed on the degree to which they were knowledgeable about their target app's user privacy policies. It was found that the knowledge level of the TapTapSee users was significantly lower than that of the Seeing AI users and the BeMyEyes users. Furthermore, the knowledge level was additionally compared between the target users of the TapTapSee app, the users of the other apps, and the prospective users. The comparison analysis found a consistent result that the TapTapSee users had a significantly lower level of knowledge. The quartile analysis contributes to better understanding about the lower level of knowledge in the TapTapSee users, as the quartile analysis uncovered that those users were less informed of almost all aspects (85%) of the TapTapSee app privacy policies compared to other users (only 9% and 14% for BeMyEyes and Seeing AI apps, respectively). It was interesting to observe that although the TapTapSee users were less knowledgeable about the user privacy policies, their tendency to adopt the TapTapSee app remained at the highest level 'before' and 'after' the quiz-based education, which were higher than the tendency of the other app users (Seeing AI and BeMyEyes app users). The results suggest that even after the TapTapSee users are well informed of the potential risks, they would still like to use the TapTapSee app without changing the way they have been using the TapTapSee app. Being well informed of the user privacy policies may not be the primary determinant causing the TapTapSee users to change their usage behaviour. It is well documented in the literature that despite being well informed of potential risks, users are less likely to

change their usage patterns. Gurari et al. (2019) examined images taken by smartphone camera-based assistive technology app users with visual disabilities. It was found that the images contained a number of personal information, and over 50% of privacy leaks occurred as those users compromised their privacy with the intention to keep using the assistive technology to live independently. Akter et al. (2020) also observed a lower level of privacy awareness among individuals with visual disabilities and argued that those individuals might have compromised their privacy to continue using the camera-based assistive apps for independent living. Based on the results of this study and the previous studies, a possible hypothesis is that TapTapSee users are willing to compromise their privacy if they feel they gain more benefits in return. Further research should be followed to examine thoroughly why TapTapSee users highly trust and intend to use the app continuously.

The Seeing AI users were less knowledgeable particularly about 'users' capability' to access and control their own personal data, while the BeMyEyes app users were less knowledgeable about "the app company's capability" to use and share users' information. The Seeing AI users did not know that their capability to access and control their own data is limited in some cases. Thus, the Seeing AI users would need to be properly educated that although the data are provided/created by the Seeing AI users themselves, the users may have, sometimes, no authority to access and control their data. On the contrary, the BeMyEyes app users would need to be educated that the app company could share their information with third-party organisations such that the third-party organisations may contact users or make them aware of various services they offer (i.e., consumer marketing). Similar results are found in the literature. For example, a survey study with 495 individuals (Waldman, 2017) found that 16.2% and 43% of the survey respondents 'never' and 'rarely', respectively, read user privacy policy statements. Nearly 60% had a poor understanding of user privacy policy statements. Stangl et al. (2022) reviewed user privacy policies of various assistive technologies, including camera-based assistive technologies. They found that the privacy statements were poorly written and difficult for users to understand. Participants in this study may have been affected by how the policy statements are designed as Waldman (2017) argued that users' ability to understand user privacy policy statements are likely to be affected by the degree to which the statements are readable and understandable. Derguech et al. (2018) examined the readability of user privacy policy statements by using the simple measure of Gobbledygook (also known as SMOG Index Readability Score). A set of 1139 policy documents were examined, over 44% of which were found to be readable only by people who have higher education (at least undergraduate and graduate levels in the USA). It infers that a large number of Americans (including those with visual disabilities) are less likely to comprehensively understand the user privacy policy statements.

Through the exit in-depth interviews, the participants expressed a range of concerns about user privacy issues, and furthermore, they were found to be unaware of, misinformed of, and/or had difficulty understanding the user privacy policies. Although they felt scared and vulnerable to privacy threats, they would still like to continue using the apps. They empathised that they have been relying on the apps to remain independent in everyday life such that they could not abandon those assistive technology apps because there are no other alternative options for them to replace those apps with. That perspective may explain why the TapTapSee users showed the greatest tendency to adopt the apps even though their knowledge level of privacy policies was lower but also even after they learned about the potential risks through the quiz-based education. A similar

result was also found in the literature that Hayes et al. (2019) observed their research participants expressing concerns about privacy and security issues associated with online transactions using their credit cards. Their research participants did not believe in existing privacy/security measures online as their credit card information may be stolen by others. They were also concerned that they might not easily notice the digital theft as they cannot see due to vision loss. Despite the limitations, they would still like to keep relying on such online transactions because that is a way for them to remain independent, i.e., the trade-offs between independence and privacy/security online.

On the other hand, they were worried that although they know that they should be careful while using the apps and sharing personal information online, they often found themselves becoming careless and inattentive. A similar finding was also observed in previous research. For instance, Napoli et al. (2021) reported that computer users with visual disabilities often became unconcerned or overconfident while using computing systems online, resulting in increased risks of privacy/security issues. Those with visual disabilities in the study of Napoli et al. (2021) simply believed that safety measures were reliable such that they could use the online system without any concerns about privacy/security risks; but also, they believed in themselves that they could easily spot any risks/suspicious activities online. As those human behaviours are associated with human factors (e.g., human-enabled errors in cyber operation) (Nobles, 2018), appropriate educational interventions should be provided to help them to increase and/or maintain good privacy/security awareness. Thus, they could make informed decisions, leading to less unintentional privacy-invasive behaviour (Pötzsch, 2008).

This study might have been affected by a few research limitations. For example, due to the COVID-19 pandemic, the research team interacted with participants using a telephone. Therefore, participants were instructed to complete the quiz while the research team was reading it out loud instead of completing the quiz in writing. It might have been difficult for participants to understand and respond to the quiz over the phone. Yet, the research team repeated the quiz statements and questions as many as participants wanted. Further, there is a report (Rogowsky et al., 2016) revealing no significant difference in learners' comprehension levels when learners use different learning modalities, i.e., reading, listening, and both. Participants might also have used different versions of the apps depending on when they updated the apps, which would lead participants to perceive user privacy issues differently. Future research will include more participants to extend the validity of the results of this study.

5 Conclusions

This study contributed to advancing knowledge of how users with visual disabilities perceive camera-based assistive technology apps, especially associated with user privacy. People with visual disabilities have obtained a great degree of benefits using the assistive technology apps (e.g., identifying people, text, colour, barcode, currency, scene, and any objects in real time). They cannot stop using the apps even though they are aware of the potential risks as they have no other options to remain independent. A conceptual framework was accordingly formed to illustrate facilitators and barriers to user adoption. Researchers and professionals in assistive technology fields can consider the results of this study as a knowledge foundation to support and enhance users' privacy awareness,

accessible to people with visual disabilities (i.e., inclusive design approach in privacy awareness).

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 1831969.

References

Ablon, L., Heaton, P., Lavery, D.C. and Romanosky, S. (2016) *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, Rand Corporation, Santa Monica, California.

Adams, D., Morales, L. and Kurniawan, S. (2013) 'A qualitative study to support a blind photography mobile application', *Proceedings of the 6th International Conference on PErvasive Technologies Related to Assistive Environments*, Rhodes Greece, pp.1–8.

Ahmed, T., Hoyle, R., Connelly, K., Crandall, D. and Kapadia, A. (2015) 'Privacy concerns and behaviors of people with visual impairments', *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Republic of Korea, pp.3523–3532.

Ahmed, T., Kapadia, A., Potluri, V. and Swaminathan, M. (2018) 'Up to a limit? privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies', *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 2, pp.1–27.

Ahmed, T., Shaffer, P., Connelly, K., Crandall, D. and Kapadia, A. (2016) 'Addressing physical safety, security, and privacy for people with visual impairments', *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pp.341–354.

Akter, T., Dosono, B., Ahmed, T., Kapadia, A. and Semaan, B. (2020) ''I am uncomfortable sharing what I can't see': privacy concerns of the visually impaired with camera based assistive applications', *29th USENIX Security Symposium (USENIX Security 20)*, pp.1929–1948.

Anderson, M. (2015) *Technology Device Ownership*, Pew Research Center [online] https://www.pewresearch.org/internet/2015/10/29/technology-device-ownership-2015/.

Azenkot, S., Rector, K., Ladner, R. and Wobbrock, J. (2012) 'PassChords: secure multi-touch authentication for blind people', *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*, pp.159–166.

Bernstein, M.S., Brandt, J., Miller, R.C. and Karger, D.R. (2011) 'Crowds in two seconds: enabling realtime crowd-powered interfaces', *Proceedings of the 24th annual ACM symposium on User Interface Software and Technology*, pp.33–42.

Bernstein, M.S., Little, G., Miller, R.C., Hartmann, B., Ackerman, M.S., Karger, D.R., Crowell, D. and Panovich, K. (2010) 'Soylent: a word processor with a crowd inside', *Proceedings of the 23rd Annual ACM Symposium on User Interface Software and Technology*, pp.313–322.

Bigham, J.P., Jayant, C., Ji, H., Little, G., Miller, A., Miller, R.C., Miller, R., Tatarowicz, A., White, B. and White, S. (2010) 'Vizwiz: nearly real-time answers to visual questions', *Proceedings of the 23rd Annual ACM Symposium on User Interface Software and Technology*, pp.333–342.

Bowman, E. (2021) *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*, NPR [online] https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.

Cimpanu, C. (2020) *Hacker Selling Data of 538 Million Weibo Users*, ZDNET [online] https://www.zdnet.com/article/hacker-selling-data-of-538-million-weibo-users/.

Derguech, W., Zainab, S.S.E. and D'Aquin, M. (2018) 'Assessing the readability of policy documents: the case of terms of use of online services', *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, pp.247–256.

Dockery, D. and Krzystolik, M. (2020) 'The use of mobile applications as low-vision aids: a pilot study', *Rhode Island Medical Journal*, Vol. 103, No. 8, pp.69–72.

Gao, S., Krogstie, J. and Siau, K. (2011) 'Developing an instrument to measure the adoption of mobile services', *Mobile Information Systems*, Vol. 7, No. 1, pp.45–67.

Gressin, S. (2017) *Equifax Data Breach: What to Do Now*, CNN [online] https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html.

Gurari, D., Li, Q., Lin, C., Zhao, Y., Guo, A., Stangl, A. and Bigham, J.P. (2019) 'Vizwiz-priv: a dataset for recognizing the presence and purpose of private visual information in images taken by blind people', *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp.939–948.

Hayes, J., Kaushik, S., Price, C.E. and Wang, Y. (2019) 'Cooperative privacy and security: Learning from people with visual impairments and their allies', *Proceedings of the 15th Symposium on Usable Privacy and Security*, Santa Clara, California, pp.1–20.

Inan, F.A., Namin, A.S., Pogrund, R.L. and Jones, K.S. (2016) 'Internet use and cybersecurity concerns of individuals with visual impairments', *Journal of Educational Technology & Society*, Vol. 19, No. 1, pp.28–40.

Jayant, C., Ji, H., White, S. and Bigham, J.P. (2011) 'Supporting blind photography', *The Proceedings of the 13th International ACM SIGACCESS Conference on Computers and Accessibility*, Association for Computing Machinery, Dundee, Scotland, UK.

Kelley, P.G., Cesca, L., Bresee, J. and Cranor, L.F. (2010) 'Standardizing privacy notices: an online study of the nutrition label approach', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp.1573–1582.

Kim, H.N. (2018) 'User experience of mainstream and assistive technologies for people with visual impairments', *Technology and Disability*, Vol. 30, No. 3, pp.127–133.

Kim, H.N. (2021) 'Characteristics of technology adoption by older adults with visual disabilities', *International Journal of Human–Computer Interaction*, Vol. 37, No. 13, pp.1256–1268.

Krumay, B. and Klar, J. (2020) 'Readability of privacy policies', *IFIP Annual Conference on Data and Applications Security and Privacy*, Springer, pp.388–399.

Larson, S. (2017a) 'Every single Yahoo account was hacked – 3 billion in all', *CNN Business* [online] https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

Larson, S. (2017b) 'Uber's massive hack: what we know', *CNN Business* [online] https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html.

Lasecki, W., Miller, C., Sadilek, A., Abumoussa, A., Borrello, D., Kushalnagar, R. and Bigham, J. (2012) 'Real-time captioning by groups of non-experts', *Proceedings of the 25th Annual ACM Symposium on User Interface Software and Technology*, pp.23–34.

Lasecki, W.S., Song, Y.C., Kautz, H. and Bigham, J.P. (2013a) 'Real-time crowd labeling for deployable activity recognition', *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, pp.1203–1212.

Lasecki, W.S., Thiha, P., Zhong, Y., Brady, E. and Bigham, J.P. (2013b) 'Answering visual questions with conversational crowd assistants', *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility*, pp.1–8.

Lasecki, W.S., Wesley, R., Nichols, J., Kulkarni, A., Allen, J.F. and Bigham, J.P. (2013c) 'Chorus: a crowd-powered conversational assistant', *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology*, pp.151–162.

Lasecki, W.S., Teevan, J. and Kamar, E. (2014) 'Information extraction and manipulation threats in crowd-powered systems', *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pp.248–256.

Meiselwitz, G. (2013) 'Readability assessment of policies and procedures of social networking sites', *International Conference on Online Communities and Social Computing*, Springer, pp.67–75.

Morris, J.T., Jones, M.L. and Sweatman, W.M. (2016) 'Wireless technology use by people with disabilities: a national survey', *Journal on Technology and Persons with Disabilities*, Vol. 1, pp.101–113.

Napoli, D., Baig, K., Maqsood, S. and Chiasson, S. (2021) 'I'm literally just hoping this will {work:'}'obstacles blocking the online security and privacy of users with visual disabilities', *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pp.263–280.

Nobles, C. (2018) 'Botching human factors in cybersecurity in business organizations', *HOLISTICA–Journal of Business and Public Administration*, Vol. 9, No. 3, pp.71–88.

Park, Y.J. (2013) 'Digital literacy and privacy behavior online', *Communication Research*, Vol. 40, No. 2, pp.215–236.

Pötzsch, S. (2008) *Privacy Awareness: A Means to Solve the Privacy Paradox?*, pp.226–236, IFIP Summer School on the Future of Identity in the Information Society, Springer, Berlin, Heidelberg.

Rogowsky, B.A., Calhoun, B.M. and Tallal, P. (2016) 'Does modality matter? The effects of reading, listening, and dual modality on comprehension', *SAGE Open*, Vol. 6, No. 3, pp.1–9.

Schaub, F., Balebako, R. and Cranor, L.F. (2017) 'Designing effective privacy notices and controls', *IEEE Internet Computing*, Vol. 21, No. 3, pp.70–77.

Smith, A. (2014) *Half of Online Americans Don't Know What a Privacy Policy Is* [online] https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ (accessed 4 December 2021).

Stangl, A., Shiroma, K., Davis, N., Xie, B., Fleischmann, K.R., Findlater, L. and Gurari, D. (2022) 'Privacy concerns for visual assistance technologies', *ACM Transactions on Accessible Computing (TACCESS)*, Vol. 15, No. 2, pp.1–43.

Templeman, R., Rahman, Z., Crandall, D. and Kapadia, A. (2012) 'PlaceRaider: virtual theft in physical spaces with smartphones', arXiv preprint arXiv:1209.5982, https://arxiv.org/pdf/1209.5982.pdf.

Vázquez, M. and Steinfeld, A. (2014) 'An assisted photography framework to help visually impaired users properly aim a camera', *ACM Transactions on Computer-Human Interaction (TOCHI)*, Vol. 21, No. 5, pp.1–29.

Voss, P., Gougoux, F. and Guillemot, J-P. (2004) 'Early-and late-onset blind individuals show supra-normal auditory abilities in far-space', *Curr. Biol.*, Vol. 14, No. 19, pp.1734–1738.

Waldman, A.E. (2017) 'A statistical analysis of privacy policy design', *Notre Dame L. Rev. Online*, Vol. 93, No. 1, pp.159–171.

Wang, R., Yu, C., Yang, X-D., He, W. and Shi, Y. (2019) 'EarTouch: facilitating smartphone use for visually impaired people in mobile and public scenarios', *Proceedings of the 2019 Chi Conference on Human Factors in Computing Systems*, Glasgow, Scotland, UK, pp.1–13.

Wang, Y. (2017) 'The third wave? Inclusive privacy and security', *Proceedings of the 2017 New Security Paradigms Workshop*, pp.122–130.

Wang, Y. and Price, C.E. (2022) *Accessible Privacy. Modern Socio-Technical Perspectives on Privacy*, Springer, Cham.

Wong, S. (2018) 'Traveling with blindness: a qualitative space-time approach to understanding visual impairment and urban mobility', *Health & Place*, Vol. 49, pp.85–92.

World Health Organization (2008) *Change the Definition of Blindness* [online] https://www.who.int/health-topics/blindness-and-vision-loss (accessed 4 October 2020).

Wu, S. and Adamic, L.A. (2014) 'Visually impaired users on an online social network', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Toronto, ON, Canada, pp.3133–3142.