SoK: Evaluating Privacy and Security Concerns of Using Web Services for the Disabled Population

Alisa Zezulak, Faiza Tazi, and Sanchari Das
InSpirit Lab, University of Denver, Colorado; Emails: {Alisa.Zezulak, Faiza.Tazi, Sanchari.Das}@du.edu

***Abstract*—The online privacy and security of the disabled community is a complex field that has implications for every user who navigates web services. While many disciplines have separately researched the disabled population and their online privacy and security concerns, the overlap between the two is very high but under-researched. Moreover, a complex relationship exists between the disabled population and web services where the interaction depends on several web service developmental factors, including usability and accessibility. To this aid, we explored this intersection of privacy and security of web services as perceived by the disabled community through previous studies by conducting a detailed systematic literature review and analysis of 63 articles. Our findings encompassed several topics, including how the disabled population navigates around authentication interfaces, online privacy concerns, universal design practices, and how security methods such as CAPTCHAs can be improved to become more accessible and usable for people of all needs and abilities. We further discuss the gap in the current research, including solutions such as the universal implementation of inclusive privacy and security tools and protocols.**

***Index Terms*—Disabled Population, Privacy and Security, Web Services, Literature Review.**

I. Introduction

The Covid-19 pandemic has necessitated people worldwide to adapt to new ways of doing things [1]. With billions of people forced to conduct their daily activities online, including attending school, working from home, grocery shopping, banking, and other critical tasks [2]–[7], the move to a fully digital world has been an inconvenience for some. Unfortunately, this drastic shift to online services has left many behind, particularly those who rely on usable, accessible, and inclusive services [8]–[12]. While the vulnerabilities of the disabled population have always existed, this sudden move to digital services has exacerbated existing problems [8], [13], including privacy and security since vulnerable populations cannot use privacy and security tools and protocols successfully due to the disparities in usability and accessibility levels. Furthermore, these tools often fail to meet the specific requirements of the disabled population, even in fundamental areas such as authentication techniques [11], [14], [15].

Along with the usability and accessibility concerns, there are many data security and privacy concerns present, such as critical data access, smart home technology data usage, and inadequate authentication protocols. Additionally, the disabled population uses medical technology more than their non-disabled counterparts, but many of these tools and protocols are not accessible to users with different needs and abilities [16]. This makes accessing personal health records, and user accounts difficult for many users. Furthermore, the disabled population faces many difficulties online relating to authentication methods such as CAPTCHAs [17], [18]. Most CAPTCHAs require a user to enter an alphanumeric code, which can be difficult or impossible for visually impaired users. This raises questions about if privacy and security tools are designed with different user populations in mind.

To provide a comprehensive understanding of the research undertaken in this area, we conducted a systematic literature review of $2,352$ research articles on the privacy and security of web services and the disabled populations. We screened these articles by title, abstract, and full text, selecting 63 papers that focused on the privacy and security of web services as they relate to the disabled population. We then conducted a detailed thematic analysis of these papers, uncovering valuable solutions to address some privacy and security concerns of the disabled population. However, our analysis also revealed significant gaps in the research, highlighting the need for future work in this area. As far as we know, this is the first Systematization of Knowledge (SoK) paper to focus on the privacy and security challenges faced by the disabled community while accessing web services.

II. Related Work

While still a relatively new and developing field, a growing collection of literature focuses on the privacy and security of people with disabilities using web services.

A. Differing Tool Usage Perceptions: Web Services

Both on and offline, the general population and disabled population have vastly different needs and abilities. As technology advances, many adults increasingly use online services such as banking, social media, email, and healthcare [19]–[25]. As a result of this increase in technology use, many of these users have privacy and security concerns related to web services and how their data is being used [26]–[28]. While these web services can benefit users greatly, researchers such as Mentis et al. have found that they also create various privacy and security risks for vulnerable populations. In addition, many adults who use these services have mild cognitive impairment and other disabilities that make it difficult to understand the implications of sharing personal information online, the importance of password management, and recognizing scams [29]–[34]. While these web services should make technology more accessible to all users, our SOK demonstrates

that we need to perform an in-depth study to understand the needs of understudied populations.

B. Privacy and Security Concerns

When trying to understand more about how tool usage differs amongst these populations, the topic of authentication and CAPTCHA completion was at the forefront of six [17], [35]–[39] research papers. Authentication protocols are a hallmark of online privacy and security [40]–[43], necessary for all users to complete to gain access to their accounts or personal information. However, some authentication methods, such as CAPTCHAs, can be difficult or impossible for disabled users to complete since they rely heavily on visual outputs [44]–[47]. Therefore, Fuglerud et al. proposed a talking mobile one-time-password client that would provide users with both auditory and visual outputs [36]. This tool creates an environment where various types of users can complete authentication mechanisms without being overlooked based on their needs or abilities. However, our research reveals a scarcity of authentication tools and designs tailored to address the requirements of disabled populations.

III. Methods

Through this study, we aim to answer the following research questions (RQs):

- *RQ1: What are the privacy and security concerns related to the disabled community when interacting with web services?*
- *RQ2: How can CAPTCHAs/authentication be improved to protect the privacy and security of people with disabilities for online communication?*
- *RQ3: How can universal design, design for privacy, and inclusive privacy and security be implemented in different web services?*

To answer these questions, our literature review included several steps: (i) database search, (ii) title screening, (iii) duplicate removal, (iv) abstract screening,(v) full-text screening, and (vi)thematic analysis. Papers were included if they meet the following criteria: (1) Published in a peer-reviewed publication, (2) Published in English, (3) Technology discussed focuses on privacy and/or security of web services, (4) Target population includes a significant portion of individuals with disabilities. The exclusion criteria includes: (1) The technology discussed in the research work was not used primarily by people with disabilities, (2) The papers did not include a direct discussion of the privacy and security of users with disabilities for web services, (3) The paper was an abstract, poster, work-in-progress, or otherwise not a full paper, (4) The full-text of the papers were not available even after searching through multiple databases or after contacting the authors. Our methodology was adapted from prior works by Stowell et al. [48], Das et al. [49], Tazi et al. [50], [51], Noah and Das [52], and Shrestha et al. [53], [54].

A. Database Search and Title Screening

We conducted our search by exploring five digital databases, namely:IEEE Xplore [1], SSRN [2], Google Scholar [3], Science Direct [4], and ACM Digital Library [5]. The data collection spanned from May to July 2021 and included any paper published before July 2021. We collected 14 papers from IEEE Xplore, 3 papers from SSRN, 1000 papers from Google Scholar, 991 papers from Science Direct, and 344 papers from ACM Digital Library. The keyword search for IEEE Xplore, SSRN, and Science Direct was "disability + privacy + security," and the "research articles" filter was applied. For ACM Digital Library, the keyword search used was "disability" AND "privacy," AND "security" with the "full text" filter applied. We used the Publish or Perish [55] software to review Google Scholar articles. The keyword search used in Publish or Perish was "privacy and security" + "disabled people." This search was limited to 1000 results by the software. We reviewed a total of $2,352$ article titles from all five databases. A paper was at this point deemed pertinent if the title discussed web services for people with disabilities, including those with specific impairments like visual, hearing, or motor impairments. Additionally, the title was required to describe a study investigating privacy and security concerns of using web services for the disabled population or the usage of web services in general about privacy or security. A paper was also only considered if it met the inclusion requirements. After duplicate removal, our corpus consisted of 138 articles.

B. Abstract and Full Text Screening

We manually reviewed the abstracts of all 138 papers in the research collection for relevance to our RQs. We removed 27 papers during abstract screening, leaving 111 papers for full-text screening. On these 111 papers, we conducted a full-text screening where we reviewed the methods, findings, analysis, and discussions. After the full-text screening, 63 relevant papers remained for the detailed thematic analysis.

C. Data Extraction and Thematic Analysis

For all 63 papers remaining in our corpus, we extracted quantitative and qualitative findings to assess the web services' privacy and security perspectives on the disabled population-focused research conducted by prior studies. The extracted data included population samples, user experience, study design characteristics, and type of technology used (web services for our research). The results, discussion, and conclusion data from each paper were analyzed and coded according to themes identified by the first and third authors. The inter-coder reliability score for the coding was 89.4%. In places where the two authors could not agree, the second author decided. A random sample of 12 papers was taken where the abstracts,

[1]https://ieeexplore.ieee.org/Xplore
[2]https://www.ssrn.com
[3]https://scholar.google.com/
[4]https://www.sciencedirect.com/
[5]https://dl.acm.org/

methods, results, and discussions were reviewed. This resulted in themes such as:

- Type of disability: visual impairments, Down Syndrome, cognitive disabilities
- Type of participant: some studies include both disabled and non-disabled people, while other studies include only disabled people
- Difficulty using authentication interfaces
- CAPTCHA completion can be hard or impossible for those who are blind, have low vision, or have a learning disability (dyslexia, ADHD.)

The remaining papers were then evaluated by going through each and generating a complete codebook. This process yielded a codebook that consists of 33 overarching codes, which were themed into seven overarching themes including,“ Authentication Interface Issues ”, “ Privacy Concerns as Reasons for Non-Use ”,“ Critical Data Access ”,“ Online Vulnerability ”,“ Solutions to authentica ”,“ Universal Design ”and“ Usability of Security Tools and Protocols ”.

IV. Findings and Discussions

In this section, we report on our findings while addressing the RQs mentioned in the previous section.

A. RQ1: Privacy and Security Concerns of Disabled People for Web Services

Our first research question addresses the privacy and security concerns of people with disabilities when interacting with web services. We addressed this RQ by analyzing the different papers within the themes related to this specific research question which are four, namely:“ Authentication Interface Issues ”, “ Privacy Concerns as Reasons for Non-Use ”,“ Critical Data Access ”,“ Online Vulnerability ”. Table I provides the snapshot of the distribution of the papers which cater to RQ1. In the following subsections, we will provide more details about these themes.

Themes	Number of Papers
Authentication Interface Issues	4 (6.35%) [13], [17], [37], [38]
Privacy Concerns as Reasons for Non-Use	27 (42.86%) [16], [39], [56]–[80]
Critical Data Access	7 (11.11%) [81]–[87]
Online Vulnerability	14 (22.22%) [8], [29], [88]–[99]

TABLE I
The Distribution of Papers Across Themes Answering the RQ1

1) Authentication Interface Issues: Authentication is a basis of security standards and protocols for web services. While CAPTCHA completion and authentication steps are often easy for non-disabled users, the disabled population faces countless difficulties accessing their online services. While analyzing papers on security concerns for people with disabilities, we found that issues with authentication interfaces were a common theme discussed. We found underlying sub-themes, such as difficulty using authentication due to technical hindrances and how each disability can affect a user's capability to complete authentication mechanisms. Four papers from the 63 in our corpus [13], [17], [37], [38] relating to this category. One such paper discusses the success of CAPTCHA completion depending on the disabilities; for most non-disabled users, CAPTCHA completion and other forms of authentication are an almost unnoticeable part of using web services.

However, users with any level of disability or impairment can find these same tasks to be difficult or impossible, as Helkala explains [17]. Through their work, Helkala explores how users with vastly different disabilities like Parkinson's disease, dyslexia, vision impairment, and upper extremity disabilities all experience different issues with CAPTCHA completion based on their abilities. In addition, this research raises important questions about how current authentication methods, such as static PIN codes, textual passwords, and one-time codes, can be altered better to fit different populations' needs and abilities. Another equally important code within this theme is the difficulty of using authentication due to technical hindrances; these difficulties discussed were at the conceptual and adoption levels. This was detailed by Bayor et al. in their research analyzing interest in using social media amongst users with intellectual disabilities. Their findings suggest that a lack of accessible authentication methods for disabled users often hinders this interest. The authors also note that voice search, auto-login, and password retrieval protocols could be already-existing solutions for this user population [13]

2) Privacy Concerns as Reasons for Non-Use: In reviewing research papers on the privacy and security concerns of the disabled population when using web services, we found that an overwhelming majority of users cited privacy concerns as reasons for non-use. Every user wants their account and data to be protected from social media sites to healthcare technology. Some of the most prevalent sub-themes related to non-use were found in connection to medical technology in smart homes and concerns about health information technology used frequently by people with disabilities. If a user feels that their health information needs to be adequately protected, it was found that they often choose not to use the service at all. There are 27 papers related to this theme, as detailed in table I. One such paper analyzes the privacy and security concerns of disabled people regarding medical technology used in smart homes.

Ziefle et al. researched the attitudes of disabled users towards a video-based monitoring system in the smart home environments of elderly or disabled people. They found that users would only feel comfortable with this system in their homes if strict privacy protocols were followed, including anonymity in transferring medical data, password protection, discretion, and avoidance of stigmatization [64]. Furthermore, many health information technologies are becoming popular amongst users, especially smartphone apps and websites that access medical data. Onyeaka et al. discuss how it may be difficult for some user populations, such as those with disabilities or mental health conditions, to use these smartphone apps and websites. The researchers found that many users with disabilities would withhold crucial medical information from their healthcare providers because of privacy and security concerns about

how their data was being used by the healthcare apps and websites [88]. Concerns exist that these privacy and security issues could lead to further stigmatization and non-use by the disabled population.

3) Critical Data Access: We classified papers within " Critical Data Access" if they discuss data sharing, specifically medical data, and the privacy and security concerns of disabled people over their critical data. Through these papers, we determine that users have privacy and security concerns related to sharing personal health records with caretakers, healthcare providers, insurance companies, researchers, and governments. In particular, many people with disabilities feel there are privacy trade-offs in emergency situations when they do not have control over who has access to their personal medical data. Seven papers from our corpus were included in this theme [81]–[87]. One of these papers; Beach et al. discuss how technology aimed at enhancing independent living for people with disabilities is a growing field. However, there are still a lot of privacy and security concerns to consider. This is particularly relevant because the researchers found that users with disabilities are significantly more accepting of the sharing and recording personal medical information than non-disabled people [82]. This raises concerns about how disabled people are more at risk of privacy and security failures than their non-disabled counterparts. On the other hand, Solanas et al. propose m-Carer, a smart mobile device that monitors patients' movements. The researchers hope to provide a way to track and find disabled users who become lost, disoriented, or need emergency medical attention [81]. Although this new technology could help users in emergencies, it raises concerns about patient privacy invasions and how the tracking data is stored and transmitted.

4) Online Vulnerability: we classified papers that examine online vulnerabilities, particularly those that affect individuals with disabilities, as " Online Vulnerability". More than 22% of the papers in our corpus fall under this theme, making it a prevalent one. [8], [29], [88]–[99]. Many disabled users are unaware of the ever-changing nature of online privacy and security issues, and must rely on the assistance of a caregiver or family member to safeguard themselves. This raises concerns about the trade-offs between autonomy and privacy when disabled people use digital services. According to Chalghoumi et al., many disabled users are unaware of technology and web services' privacy and security concerns. The researchers found that the opinions of caregivers and family members of the disabled participant were significantly influential on the user's behavior toward online privacy [99]. This raises questions regarding how much of a disabled user's web services experience can be autonomous if caretakers substantially impact them.

B. RQ2: Improving CAPTCHA/authentication

The second RQ focuses on how CAPTCHAs/authentication can be improved to protect the privacy and security of people with disabilities when using web services. Some disabled users can find authentication completion impossible and are consequently unable to access their accounts. Six papers [35], [100], [101] from our corpus focus on solutions to improving authentication and CAPTCHAs. Table II provides the snapshot of the distribution of these papers.

Theme	Number of Papers
Solutions to authentication/CAPTCHA Issues	3 (4.76%) [35], [100], [101]

TABLE II
THE DISTRIBUTION OF PAPERS ACROSS THEMES ANSWERING THE RQ2

Some papers relating to this theme provided the solution to authentication problems; one such solution is using passtones instead of passwords, as researched by Brown and Doswell. Rather than remembering alphanumeric sequences, Brown and Doswell propose a password alternative where users would remember a sequence of sounds [100]. The researchers explain how this tool has already been implemented using photos, but using auditory passwords would improve the experience of users with visual disabilities. While explicitly a solution for visually impaired users, this solution could be widely implemented and used by people of all different needs and abilities. Similarly, accessible password managers are another solution to issues with authentication that many users face. Barbosa et al. describe their implementation of UniPass, an accessible password manager for visually impaired users on a smart device. This tool includes features such as reading prompts and messages aloud, buttons and other graphical elements are avoided, and the device vibrates to signify the need for user input [101]. The researchers found that password managers are a promising solution for the difficulties visually impaired users face with authentication mechanisms. A different way to enhance the authentication experience of disabled users when interacting with web services is Spoken CAPTCHA. Shirali-Shahreza et al. discuss how most CAPTCHA methods currently only use visual patterns, making it impossible for blind users to complete them. The researchers propose a new CAPTCHA method, Spoken CAPTCHA, where users would hear a short sound clip asking them to say a word. The user will then respond in a speech file that can be checked not to be computer generated [35]. This solution focuses on the visually impaired population and provides a way to improve authentication methods for all types of users.

C. RQ3: Universal Design, Design for Privacy, and Inclusive Privacy and Security in Web Services

The third RQ focuses on how universal design, design for privacy, and inclusive privacy and security can be implemented in different web services. These inclusive concepts provide design tools and protocols to make web services more accessible for various user populations, regardless of needs and abilities. We have gleaned two themes pertaining to this research question," Universal Design "and" Usability of Security Tools and Protocols ". Table III provides the snapshot of the distribution of the papers which caters to the RQ3.

Theme	Number of Papers
Universal Design	6 (9.53%) [102]–[107]
Usability of Security Tools and Protocols	2 (3.17%) [36], [108]

TABLE III
THE DISTRIBUTION OF PAPERS ACROSS THEMES ANSWERING THE RQ3

1) Universal Design: The Universal Design concept describes how the design of all products and environments should be usable by all people without the need for adaptation or specialized design. Inclusive privacy and security and privacy by design are closely related to the overarching theme of universal design. Six papers [102]–[107] were included in this theme. These papers discuss the current privacy and security protocols that are most widely used and why they do not consider the needs and abilities of under-served populations such as children, older adults, people with disabilities, and people from non-Western populations. Wang et al. discuss the implementation of inclusive privacy and security tools, and protocols would prioritize the design of mechanisms that are inclusive to people with various characteristics, abilities, needs, and values [103]. Similarly, we considered papers on privacy by design and how designers and technologies must put inclusive privacy and security tools/protocols at the forefront of their design. One of the most practical ways these designers can implement privacy by design is to increase digital citizen awareness surrounding consent for data processing and usage. O'Connor et al. discuss how users must have the information they need to make informed decisions about how their data is being used [105].

2) Usability of Security Tools and Protocols: The usability and accessibility of security tools and protocols are essential to the overarching theme of universal design. While the previous theme describes the theory of universal design, this theme explores implementations of the theory. The two papers related to this theme [36], [108] present inclusive password management and two-factor authentication solutions for various user populations across two related papers. Password protection is a hallmark of online security tools and protocols. However, complicated authentication procedures to access web services can be cumbersome, especially for people with disabilities or the elderly. According to Fuglerud et al., a secure and accessible multi-modal authentication method using a one-time password client could solve this problem. Users with impairments affecting their ability to complete authentication steps now have access to auditory and visual outputs from the password client [36]. This allows all users equal access to password management tools and protocols. The second paper by Han et al. describes how current 2FA solutions all require some form of user effort, with can negatively impact the experience of disabled users or the elderly. Therefore, the researchers propose a new type of mobile 2FA, Proximity-Proof, that does not require user interactions and defends against the powerful man-in-the-middle attack [108]. According to the authors, Proximity-Proof is as secure as other 2FA methods and provides innovative ways for 2FA techniques to become more usable and accessible for all users.

V. FUTURE WORK AND LIMITATION

In this paper, we conducted a systematic analysis to evaluate the research articles and peer-reviewed papers published in the field of security and privacy of web services for the disabled population. We collected papers from five digital databases and limited the papers to ones available in English. As such we might have missed papers not available in these databases. However, our extensive literature review provides a detailed overview of the current research on security and privacy of web services for the disabled population. And while this gives a broad understanding of the current research and methods used, there is limited in-depth research on individual user groups within the disabled population. For example, five of the six papers relating to solutions for authentication issues were only solutions for visually impaired users. Future analyses of privacy and security concerns of the disabled population can provide valuable research into more specific subsections of the population, such as those with cognitive disabilities, mental illnesses, and different types of physical impairments.

VI. CONCLUSION

For many disabled users, information technology and web services can be a way to enhance their autonomy and discover new interests or communities. However, disability can make the internet a challenging place, seeing as many disabled people have trouble writing, reading, and comprehending text information, making it hard for them to understand and use basic security and privacy measures such as passwords and passwords CAPTCHAs. To that regard, we conducted a systematic literature review on 63 papers focused on the privacy and security of web services for the disabled population. Our findings reveal valuable solutions to privacy and security concerns of the disabled population, focused on universal design and inclusive privacy and security methods. Universal design, in particular, provides a way to create inclusive, accessible, and usable tools and protocols to protect the privacy and security of both the disabled and general populations online. These solutions would address issues such as authentication improvement, critical data access, online vulnerability, and usability of tools and protocols. However, our findings reveal gaps in the current research, such as a lack of implementation of these universal design methods and how solutions must focus on more subsections of the disabled population.

VII. ACKNOWLEDGEMENT

We would like to thank the Inclusive Security and Privacy focused Innovative Research in Information Technology (INSPIRIT) Laboratory at the University of Denver. This research has been funded by the Faculty Research Fund (FRF) at the University of Denver. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors and not of the organization or the funding agency.

REFERENCES

[1] E. Beaunoyer, S. Dupéré, and M. J. Guitton, "Covid-19 and digital inequalities: Reciprocal impacts and mitigation strategies," *Computers in human behavior*, vol. 111, p. 106424, 2020.

[2] J. Daniel, "Education and the covid-19 pandemic," *Prospects*, vol. 49, no. 1, pp. 91–96, 2020.

[3] A. Aristovnik, D. Keržič, D. Ravšelj, N. Tomaževič, and L. Umek, "Impacts of the covid-19 pandemic on life of higher education students: A global perspective," *Sustainability*, vol. 12, no. 20, p. 8438, 2020.

[4] F. Tazi, S. Shrestha, D. Norton, K. Walsh, and S. Das, "Parents, educators, & caregivers cybersecurity & privacy concerns for remote learning during covid-19," in *Chi greece 2021: 1st international conference of the acm greek sigchi chapter*, 2021, pp. 1–5.

[5] V. Reddington, K. Haring, S. Das, and D. Pittman, "Development and evaluation of virtual reality classrooms through user-centered design during covid-19," *Proceedings of the SSPXR*, 2022.

[6] C. Monroe, F. Tazi, and S. Das, "Location data and covid-19 contact tracing: how data privacy regulations and cell service providers work in tandem," *arXiv preprint arXiv:2103.14155*, 2021.

[7] S. Karmakar and S. Das, "Understanding the rise of twitter-based cyberbullying due to covid-19 through comprehensive statistical evaluation," in *Proceedings of the 54th Hawaii international conference on system sciences*, 2021.

[8] M. Scanlan, "Reassessing the disability divide: unequal access as the world is pushed online," *Universal Access in the Information Society*, pp. 1–11, 2021.

[9] S. Das, A. Kim, S. Mare, J. Streiff, and L. J. Camp, "Security mandates are pervasive: An inter-school study on analyzing user authentication behavior," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2019, pp. 306–313.

[10] S. Das, R. S. Gutzwiller, R. D. Roscoe, P. Rajivan, Y. Wang, L. Jean Camp, and R. Hoyle, "Humans and technology for inclusive privacy and security," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 64, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 2020, pp. 461–464.

[11] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards implementing inclusive authentication technologies for older adults," *Who Are You*, 2019.

[12] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. Camp, "A qualitative study on usability and acceptability of yubico security key," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, 2018, pp. 28–39.

[13] A. Bayor, F. Bircanin, L. Sitbon, B. Ploderer, S. Koplick, and M. Brereton, "Characterizing participation across social media sites amongst young adults with intellectual disability," in *Proceedings of the 30th Australian Conference on Computer-Human Interaction*, 2018, pp. 113–122.

[14] S. Furnell, K. Helkala, and N. Woods, "Disadvantaged by disability: examining the accessibility of cyber security," in *Universal Access in Human-Computer Interaction. Design Methods and User Experience: 15th International Conference, UAHCI 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part I*. Springer, 2021, pp. 197–212.

[15] S. Das, A. Dingman, and L. J. Camp, "Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key," in *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22*. Springer, 2018, pp. 160–179.

[16] H. Liang, Y. Xue, and Z. Zhang, "Understanding online health information use: The case of people with physical disabilities," *Journal of the Association for Information Systems*, vol. 18, no. 6, p. 2, 2017.

[17] K. Helkala, "Disabilities and authentication methods: Usability and security," in *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, 2012, pp. 327–334.

[18] S. Das, S. Mare, and L. J. Camp, "Smart storytelling: Video and text risk communication to increase mfa acceptability," in *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2020, pp. 153–160.

[19] L. Gitlow, "Technology use by older adults and barriers to using technology," *Physical & Occupational Therapy in Geriatrics*, vol. 32, no. 3, pp. 271–280, 2014.

[20] S. Das, J. Goard, and D. Murray, "How celebrities feed tweeples with personal and promotional tweets: celebrity twitter use and audience engagement," in *Proceedings of the 8th International Conference on Social Media & Society*, 2017, pp. 1–5.

[21] T. L. Mitzner, J. B. Boron, C. B. Fausset, A. E. Adams, N. Charness, S. J. Czaja, K. Dijkstra, A. D. Fisk, W. A. Rogers, and J. Sharit, "Older adults talk technology: Technology usage and attitudes," *Computers in human behavior*, vol. 26, no. 6, pp. 1710–1721, 2010.

[22] K. Walsh, F. Tazi, P. Markert, and S. Das, "My account is compromised-what do i do? towards an intercultural analysis of account remediation for websites," in *Proceedings of the Sixth Workshop on Inclusive Privacy and Security (WIPS 2021): In Association with the Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021.

[23] H. R. Marston, M. Kroll, D. Fink, H. de Rosario, and Y. J. Gschwind, "Technology use, adoption and behavior in older adults: Results from the istoppfalls project," *Educational Gerontology*, vol. 42, no. 6, pp. 371–387, 2016.

[24] S. Das, T. Ahmed, A. Kapadia, and S. Patil, "Does this photo make me look good? how posters, outsiders, and friends evaluate social media photo posts," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW1, pp. 1–32, 2021.

[25] J. Dev, S. Das, and L. J. Camp, "Privacy practices, preferences, and compunctions: Whatsapp users in india." in *HAISA*, 2018, pp. 135–146.

[26] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and security concerns in iot-based healthcare systems," in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*. Springer, 2021, pp. 105–134.

[27] P. McCole, E. Ramsey, and J. Williams, "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns," *Journal of Business Research*, vol. 63, no. 9-10, pp. 1018–1024, 2010.

[28] P. Markert, A. Adhikari, and S. Das, "A transcontinental analysis of account remediation protocols of popular websites," *arXiv preprint arXiv:2302.01401*, 2023.

[29] H. M. Mentis, G. Madjaroff, and A. K. Massey, "Upside and downside risk in online security for older adults with mild cognitive impairment," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–13.

[30] S. Shrestha, D. Thomas, and S. Das, "Secureld: Secure and accessible learning for students with disabilities," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 66, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 2022, pp. 465–469.

[31] S. Das *et al.*, "Sok: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review," in *Proceedings of the workshop on usable security and privacy (USEC)*, 2022.

[32] S. Das, A. Kim, B. Jelen, L. Huber, and L. J. Camp, "Non-inclusive online security: older adults' experience with two-factor authentication," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2020.

[33] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Why don't older adults adopt two-factor authentication?" in *Proceedings of the 2020 SIGCHI Workshop on Designing Interactions for the Ageing Populations-Addressing Global Challenges*, 2020.

[34] S. Das, J. Streiff, L. L. Huber, and L. J. Camp, "Why don't elders adopt two-factor authentication? because they are excluded by design," *Innovation in Aging*, vol. 3, no. Supplement_1, pp. S325–S326, 2019.

[35] S. Shirali-Shahreza, H. Abolhassani, H. Sameti, and M. Hassan, "Spoken captcha: A captcha system for blind users," in *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, vol. 1. IEEE, 2009, pp. 221–224.

[36] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 27–34, 2011.

[37] J. Yan and A. S. El Ahmad, "Usability of captchas or usability issues in captcha design," in *Proceedings of the 4th symposium on Usable privacy and security*, 2008, pp. 44–52.

[38] Y. Ma, J. Feng, L. Kumin, and J. Lazar, "Investigating user behavior for authentication methods: A comparison between individuals with down syndrome and neurotypical users," *ACM Transactions on Accessible Computing (TACCESS)*, vol. 4, no. 4, pp. 1–27, 2013.

[39] T. Kumar, A. Braeken, A. D. Jurcut, M. Liyanage, and M. Ylianttila, "Age: authentication in gadget-free healthcare environments," *Information Technology and Management*, vol. 21, no. 2, pp. 95–114, 2020.

[40] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review," *arXiv preprint arXiv:1908.05901*, 2019.

[41] J. M. Jones, R. Duezguen, P. Mayer, M. Volkamer, and S. Das, "A literature review on virtual reality authentication," in *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15*. Springer, 2021, pp. 189–198.

[42] R. Duezguen, P. Mayer, S. Das, and M. Volkamer, "Towards secure and usable authentication for augmented and virtual reality head-mounted displays," *arXiv preprint arXiv:2007.11663*, 2020.

[43] R. Majumdar and S. Das, "Sok: An evaluation of quantum authentication through systematic literature review," in *Proceedings of the Workshop on Usable Security and Privacy (USEC)*, 2021.

[44] A. Patrick, A. Burris, S. Das, and N. Noah, "Understanding user perspective in a university setting to improve biometric authentication adoption," in *9th Mexican International Conference on Human-Computer Interaction*, 2022, pp. 1–10.

[45] Z. Zhang, J. Abbott, and L. J. Camp, "Building an authentication infrastructure—designing a two factor authentication hardware token with form factor that encourages engagement," *Available at SSRN 4177411*, 2022.

[46] J. McLeod, R. Majumdar, and S. Das, "Challenges and future directions in the implementation of quantum authentication protocols," in *Computational Science–ICCS 2022: 22nd International Conference, London, UK, June 21–23, 2022, Proceedings, Part IV*. Springer, 2022, pp. 164–170.

[47] K. Jensen, F. Tazi, and S. Das, "Multi-factor authentication application assessment: Risk assessment of expert-recommended mfa mobile applications," *Proceeding of the Who Are You*, 2021.

[48] E. Stowell, M. C. Lyson, H. Saksono, R. C. Wurth, H. Jimison, M. Pavel, and A. G. Parker, "Designing and evaluating mhealth interventions for vulnerable populations: A systematic review," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–17.

[49] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing: Exploring user research through a systematic literature review," *arXiv preprint arXiv:1908.05897*, 2019.

[50] F. Tazi, S. Shrestha, J. De La Cruz, and S. Das, "Sok: An evaluation of the secure end user experience on the dark net through systematic literature review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 2, pp. 329–357, 2022.

[51] F. Tazi, J. Dykstra, P. Rajivan, and S. Das, "Sok: Evaluating privacy and security vulnerabilities of patients' data in healthcare," in *International Workshop on Socio-Technical Aspects in Security*. Springer, 2022, pp. 153–181.

[52] N. Noah and S. Das, "Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review," *Computer Animation and Virtual Worlds*, vol. 32, no. 3-4, p. e2020, 2021.

[53] S. Shrestha, E. Irby, R. Thapa, and S. Das, "Sok: a systematic literature review of bluetooth security threats and mitigation measures," in *International Symposium on Emerging Information Security and Applications*. Springer, 2022, pp. 108–127.

[54] S. Shrestha and S. Das, "Exploring gender biases in ml and ai academic research through systematic literature review," *Frontiers in artificial intelligence*, vol. 5, 2022.

[55] A.-W. Harzing, *The publish or perish book*. Tarma Software Research Pty Limited Melbourne, 2010.

[56] N. Kordzadeh, J. Warren, and A. Seifi, "Antecedents of privacy calculus components in virtual health communities," *International Journal of Information Management*, vol. 36, no. 5, pp. 724–734, 2016.

[57] T. Ermakova, B. Fabian, S. Kelkel, T. Wolff, and R. Zarnekow, "Antecedents of health information privacy concerns," *Procedia Computer Science*, vol. 63, pp. 376–383, 2015.

[58] A. E. Roberts, T. A. Davenport, T. Wong, H.-W. Moon, I. B. Hickie, and H. M. LaMonica, "Evaluating the quality and safety of health-related apps and e-tools: Adapting the mobile app rating scale and developing a quality assurance protocol," *Internet Interventions*, vol. 24, p. 100379, 2021.

[59] D. B. Lafky and T. A. Horan, "Personal health records: Consumer attitudes toward privacy and security of their personal health information," *Health Informatics Journal*, vol. 17, no. 1, pp. 63–71, 2011.

[60] W. Yao, C.-H. Chu, and Z. Li, "The adoption and implementation of rfid technologies in healthcare: a literature review," *Journal of medical systems*, vol. 36, no. 6, pp. 3507–3525, 2012.

[61] B. Maqbool and S. Herold, "Challenges in developing software for the swedish healthcare sector." in *HEALTHINF*, 2021, pp. 175–187.

[62] B. Kaplan and S. Ranchordás, "Alzheimer's and mhealth: Regulatory, privacy and ethical considerations," in *Everyday Technologies in Healthcare*. CRC Press, 2019, pp. 31–52.

[63] D. B. Lafky and T. A. Horan, "Prospective personal health record use among different user groups: results of a multi-wave study," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. IEEE, 2008, pp. 233–233.

[64] M. Ziefle, C. Rocker, and A. Holzinger, "Medical technology in smart homes: exploring the user's perspective on privacy, intimacy and trust," in *2011 IEEE 35th Annual Computer Software and Applications Conference Workshops*. IEEE, 2011, pp. 410–415.

[65] T. Tantidham and Y. N. Aung, "Emergency service for smart home system using ethereum blockchain: System and architecture," in *2019 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)*. IEEE, 2019, pp. 888–893.

[66] A. El Husseini, A. M'hamed, B. El Hassan, and M. Mokhtari, "Trust-based authentication scheme with user rating for low-resource devices in smart environments," *Personal and ubiquitous computing*, vol. 17, no. 5, pp. 1013–1023, 2013.

[67] P. Novitzky, A. F. Smeaton, C. Chen, K. Irving, T. Jacquemard, F. O'Brolcháin, D. O'Mathúna, and B. Gordijn, "A review of contemporary work on the ethics of ambient assisted living technologies for people with dementia," *Science and engineering ethics*, vol. 21, no. 3, pp. 707–765, 2015.

[68] N. Vasco Lopes, "Internet of things feasibility for disabled people," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3906, 2020.

[69] M. Hadian, T. Altuwaiyan, X. Liang, and W. Li, "Efficient and privacy-preserving voice-based search over mhealth data," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. IEEE, 2017, pp. 96–101.

[70] J. Pacheco, C. Tunc, P. Satam, and S. Hariri, "Secure and resilient cloud services for enhanced living environments," *IEEE Cloud Computing*, vol. 3, no. 6, pp. 44–52, 2016.

[71] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72 469–72 478, 2018.

[72] R. Ramli and N. Zakaria, "Privacy issues in a psychiatric context: applying the isd privacy framework to a psychiatric behavioural monitoring system," *AI & society*, vol. 29, no. 2, pp. 203–213, 2014.

[73] Y. Wang, "Intelligent medicine system prototype of the internet of things," 2012.

[74] C. Ifrim, A.-M. Pintilie, E. Apostol, C. Dobre, and F. Pop, "The art of advanced healthcare applications in big data and iot systems," in *Advances in mobile cloud computing and big data in the 5G Era*. Springer, 2017, pp. 133–149.

[75] L. M. Dang, M. Piran, D. Han, K. Min, H. Moon *et al.*, "A survey on internet of things and cloud computing for healthcare," *Electronics*, vol. 8, no. 7, p. 768, 2019.

[76] A. Hussain, T. Ali, F. Althobiani, U. Draz, M. Irfan, S. Yasin, S. Shafiq, Z. Safdar, A. Glowacz, G. Nowakowski *et al.*, "Security framework for iot based real-time health applications," *Electronics*, vol. 10, no. 6, p. 719, 2021.

[77] M. Anisha, J. Francis Felix Sindhuja, C. Jim Elliot, R. Lijia Rani, J. Durga Devi, K. Monal, P. Chezhiyan, A. Abdul Majeeth, and U. Shalini, "Automated assistive health care system for disabled patients utilizing internet of things." *Journal of Engineering Science & Technology Review*, vol. 13, no. 4, 2020.

[78] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law & Security Review*, vol. 41, p. 105528, 2021.

[79] P. Mohan and M. Singh, "Security policies for intelligent health care environment," *Procedia Computer Science*, vol. 92, pp. 161–167, 2016.

[80] S. M. Ahmed and A. Rajput, "Threats to patients' privacy in smart healthcare environment," in *Innovation in Health Informatics*. Elsevier, 2020, pp. 375–393.

[81] A. Solanas, A. Martinez-Balleste, P. A. Perez-Martinez, A. F. de la Pena, and J. Ramos, "m-carer: Privacy-aware monitoring for people with mild cognitive impairment and dementia," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 19–27, 2013.

[82] S. Beach, R. Schulz, J. Downs, J. Matthews, B. Barron, and K. Seelman, "Disability, age, and informational privacy attitudes in quality of life technology applications: Results from a national web survey," *ACM Transactions on Accessible Computing (TACCESS)*, vol. 2, no. 1, pp. 1–21, 2009.

[83] F. Hamidi, K. Poneres, A. Massey, and A. Hurst, "Using a participatory activities toolkit to elicit privacy expectations of adaptive assistive technologies," in *Proceedings of the 17th International Web for All Conference*, 2020, pp. 1–12.

[84] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong, "Password sharing: implications for security design based on social practice," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2007, pp. 895–904.

[85] F. Hamidi, K. Poneres, A. Massey, and A. Hurst, "Who should have access to my pointing data? privacy tradeoffs of adaptive assistive technologies," in *Proceedings of the 20th international acm sigaccess conference on computers and accessibility*, 2018, pp. 203–216.

[86] D. Grunwel and T. Sahama, "Delegation of access in an information accountability framework for ehealth," in *Proceedings of the Australasian Computer Science Week Multiconference*, 2016, pp. 1–8.

[87] V. Distler, C. Lallemand, and V. Koenig, "How acceptable is this? how user experience factors can broaden our understanding of the acceptance of privacy trade-offs," *Computers in Human Behavior*, vol. 106, p. 106227, 2020.

[88] H. K. Onyeaka, H. Wisniewski, P. Henson, and J. Torous, "Understanding the evolving preferences for use of health information technology among adults with self reported anxiety and depression in the us," *Journal of Behavioral and Cognitive Therapy*, vol. 30, no. 1, pp. 49–56, 2020.

[89] T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia, "Privacy concerns and behaviors of people with visual impairments," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 3523–3532.

[90] J. Lazar, L. Kumin, and J. H. Feng, "Understanding the computer skills of adult expert users with down syndrome: an exploratory study," in *The proceedings of the 13th international ACM SIGACCESS conference on Computers and accessibility*, 2011, pp. 51–58.

[91] K. Macmillan, T. Berg, M. Just, and M. Stewart, "Are autistic children more vulnerable online? relating autism to online safety, child wellbeing and parental risk management," in *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 2020, pp. 1–11.

[92] A. Jattamart and A. Leelasantitham, "Perspectives to social media usage of depressed patients and caregivers affecting to change the health behavior of patients in terms of information and perceived privacy risks," *Heliyon*, vol. 6, no. 6, p. e04244, 2020.

[99] H. Chalghoumi, V. Cobigo, C. Dignard, A. Gauthier-Beaupré, J. W. Jutai, Y. Lachapelle, J. Lake, R. Mcheimech, and M. Perrin, "Information privacy for technology users with intellectual and developmental disabilities: why does it matter?" *Ethics & Behavior*, vol. 29, no. 3, pp. 201–217, 2019.

[93] M. Hersh and B. Leporini, "Mobile recommender apps with privacy management for accessible and usable technologies," in *Harnessing the Power of Technology to Improve Lives*. IOS Press, 2017, pp. 630–637.

[94] E. Muñoz, S. Cáceres, and A. Marqués, "Providing secure mechanisms to protect personal data in a mobility platform," in *25th ITS World Congress, Copenhagen, Denmark, 17-21 September 2018*, 2018.

[95] G. A. Giannoumis, "Accessibility of anonymity networks: How can web accessibility policies promote the usability of darknets for persons with disabilities?" *First Monday*, 2018.

[96] M. Hersh, "Mobility technologies for blind, partially sighted and deafblind people: design issues," in *Mobility of visually impaired people*. Springer, 2018, pp. 377–409.

[97] J. King, "" becoming part of something bigger" direct to consumer genetic testing, privacy, and personal disclosure," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–33, 2019.

[98] N. Kim and A. Hong, "Conceptualizing blockchain technology in utilization of social welfare service for the disabled," *Sustainable Development Research*, vol. 1, no. 1, pp. p35–p35, 2019.

[100] M. Brown and F. R. Doswell, "Using passtones instead of passwords," in *Proceedings of the 48th Annual Southeast Regional Conference*, 2010, pp. 1–5.

[101] N. M. Barbosa, J. Hayes, and Y. Wang, "Unipass: design and evaluation of a smart device-based password manager for visually impaired users," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 49–60.

[102] J. Vales-Alonso, E. Egea-López, J. P. Munoz-Gea, J. García-Haro, F. Belzunce-Arcos, M. A. Esparza-García, J. M. Pérez-Manogil, R. Martínez-Álvarez, F. Gil-Castineira, F. J. Gonza *et al.*, "Ucare: Context-aware services for disabled users in urban environments," in *2008 The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*. IEEE, 2008, pp. 197–205.

[103] Y. Wang, "Inclusive security and privacy," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 82–87, 2018.

[104] ——, "The third wave? inclusive privacy and security," in *Proceedings of the 2017 New Security Paradigms Workshop*, 2017, pp. 122–130.

[105] Y. O'Connor, W. Rowan, L. Lynch, and C. Heavin, "Privacy by design: informed consent and internet of things for smart health," *Procedia computer science*, vol. 113, pp. 653–658, 2017.

[106] L. McRae, K. Ellis, M. Kent, and K. Locke, "Privacy and the ethics of disability research: Changing perceptions of privacy and smartphone use," *Second international handbook of internet research*, pp. 413–429, 2020.

[107] M. D. Medley, R. H. Rutherfoord, G. E. Anderson, R. W. Roth, and S. A. Varden, "Ethical issues related to internet development and research," *ACM SIGCUE Outlook*, vol. 26, no. 4, pp. 57–72, 1998.

[108] D. Han, Y. Chen, T. Li, R. Zhang, Y. Zhang, and T. Hedgpeth, "Proximity-proof: Secure and usable mobile two-factor authentication," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, 2018, pp. 401–415.