AI-based Assistive Technologies & People with Disabilities: Privacy at risk

Jasmine Madaan

A Thesis submitted to the Faculty of Graduate Studies in Partial Fulfillment of the Requirements for the Degree of Master of Laws

Osgoode Hall Law School
York University
Toronto, Ontario

September, 2024

Abstract

This thesis follows three research questions. First, it explores the potential privacy risks that people with disabilities (PWDs) face in the face of incorporation of artificial intelligence (AI) in assistive technologies (ATs). It then investigates reasons that exacerbate PWDs' vulnerability to such potential privacy risks. Since legal literature in the context of AI-based ATs is limited, this thesis adopts a combination of multidisciplinary and traditional legal doctrinal research by studying legal literature and empirical research in other disciplines. Lastly, the thesis reviews the current Canadian data protection legal framework to examine if there is any provision specifically addressing PWDs or vulnerable data subjects and highlight legislative gaps impacting PWDs.

Acknowledgments

I am extremely grateful to my supervisor, Professor Hengameh Saberi, for her guidance, support, and proactive-approach throughout the course of my research and thesis writing. Your expertise, feedback on my research and writing, and assistance in setting timelines have been instrumental in timely completion of this thesis.

I would also like to thank my supervisory committee members, Professor Ian Stedman and Professor Jonathan Penney. Your expertise, valuable suggestions, and constructive feedback helped me tremendously during my research journey.

Thank you to 2023-24 cohort of graduate students at Osgoode Hall Law School for thought-provoking discussions. I am also grateful to the Graduate Program team, including Professor Susan Drummond, Graham Sue, and Prina Wong, for their support.

A special thanks to Malcolm Katrak and Prina Wong for their support, thoughtful answers to my questions, and for being great seniors and friends.

I am beyond thankful to my family and friends for their constant encouragement and emotional support. Lastly, I thank York University for financial and administrative support, which made working on this thesis possible. I also acknowledge the land that precedes York University. It is located in Tkaronto, on the territory of Indigenous nations.

Table of Contents

List of Abbreviations

Abbreviation	Full form
AI	Artificial intelligence
AAC	Accessibility and Augmentative Communication
AAL	Active and Assisted Living Technologies
ACA	Accessible Canada Act
ADA	Americans with Disabilities Act
ADHD	Attention deficit hyperactivity disorder
ADL	Activities of Daily Living
AIDA	Artificial Intelligence and Data Act
AR	Augmented Reality
ASL	American Sign Language
ATs	Assistive Technologies
AVSR	Audio-Visual Speech Recognition
CIPL	Centre for Information Privacy Leadership
CJEU	Court of Justice of the European Union
CPPA	Consumer Privacy Protection Act
CRPD	Convention on the Rights of Persons with Disabilities
DPIA	Data Protection Impact Assessments
ECtHR	European Court of Human Rights
ETSI	European Telecommunications Standards Institute
EU	The European Union
FAQs	Frequently Asked Questions
FIPPs	Fair Information Practice Principles
FRT	Facial Recognition Technology
GATE	Global Cooperation on Assistive Technology
GDPR	General Data Protection Regulations
HCI	human-computer interface
HI	High impact
HRC	Human Rights Committee
IADL	Instrumental Activities of Daily Living

ICCPR	International Covenant on Civil and Political Rights
ICF	International Classification of Functioning, Disability and Health
ICT	Information and Communication Technologies
IPCO	Information Privacy Commissioner of Ontario
ISED	The Minister of Innovation, Science and Industry
LLM	Large Language Model
ML	Machine Learning
OECD	The Organization for Economic Cooperation and Development
OPC	Office of Privacy Commissioner
PC	Privacy Commissioner
PHIPA	The Personal Health Information Protection Act
PIAs	privacy impact assessments
PIDPTA	Personal Information and Data Protection Tribunal Act
PIPEDA	Personal Information Protection and Electronic Documents Act
PVI	People with Visual Impairment
PWA	People with autism
PWDs	People with disabilities
PWIDD	People with intellectual and developmental disabilities
SCC	Supreme Court of Canada
SDGs	Sustainable Development Goals
UN	The United Nations
US	The United States of America
VAT	Visual Assistive Technologies
VR	Virtual Reality
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WP29	Article 29 Data Protection Working Party
YADD	Young adults with developmental disabilities

List of Illustrations

1 Introduction

Valued at $21.95 billion in 2022, experts believe the global AT market will rise to $31.22 billion by 2030.[1] One major reason for this growth trend in the AT market is the incorporation of AI systems in ATs.[2] This AI incorporation will inevitably become deeply rooted in the AT space, a transformation similar to the one brought about by the internet in the 1990s. The functioning of these emerging AI-based ATs involves processing personal data, for instance, credit card details, health reports, and more. This processing of personal and sensitive data requires AI-based ATs to protect the information privacy of the data subjects. It is irrefutable that the use of AI-based ATs offers convenience and independence to PWDs in an unprecedented way, promoting access to the world.[3] Yet, one cannot deny that the growing trend of AI-based ATs will also increase potential privacy or data protection concerns for PWDs.[4]

By way of an example illustrating this point, while using an AT app with AI-based image recognition technology, people with visual impairment (PVI) take pictures with the camera on their phone. The AI system then converts the image into text or speech and assists PVI in interacting with the world. Often, PVI use this AT for personal and sensitive data. Since this AT uses AI, certain questions related to privacy protection arise here—Is this AI-based AT storing this data? If so, is the service provider using cloud storage? Do any third parties have access to the stored data? Is this data being used for training of this or any other AI model? What happens with the collection of incidental data, for which consent was not obtained? Data subjects are often unaware of answers to these questions. Since PWDs use this technology to access the world, they

---

[1] "How sovereign funds could empower the future of assistive technology and disability AI", (15 August 2023), online: *World Econ Forum* <https://www.weforum.org/agenda/2023/08/sovereign-funds-future-assistive-technology-disability-ai/>.

[2] Directorate-General for Parliamentary Research Services (European Parliament) et al, *Assistive technologies for people with disabilities. Part II, Current and emerging technologies* (LU: Publications Office of the European Union, 2018).

[3] Directorate-General for Parliamentary Research Services (European Parliament) et al, *Assistive technologies for people with disabilities. Part I, Regulatory, health and demographic aspects* (LU: Publications Office of the European Union, 2018).

[4] Carine Marzin, "Plug and Pray?", (15 December 2020), online: *Eur Disabil Forum* <https://www.edf-feph.org/publications/plug-and-pray-2018/>.

often end up having to trade-off their personal and sensitive data in order to achieve independence and convenience.

This state of affairs highlights the relevance of an important body of law—privacy and data protection laws. There are other laws that hold equal value and are relevant in this context, such as human rights laws and constitutional law, but this thesis focuses exclusively on privacy and data protection law. The question of how lawmakers and technology industry stakeholders should engage with laws on data privacy and AI systems, especially when it intersects with ATs and disability, requires urgent attention.

The current literature on ATs/AI-based ATs and PWDs focuses more on the technology itself, with any legal analysis being more focused on the EU[5] and the US[6] as opposed to Canadian law. Moreover, based on my research, there is little scholarship that considers privacy and data protection concerns in relation to PWDs while using AI-based ATs, let alone the trade-off that PWDs may have to accept in their everyday lives between data privacy and independence or convenience.

This thesis responds to these lacunas in the literature. The first chapter serves as a detailed introduction to the thesis and lays the groundwork for the project. It first defines the most used and important terms for the scope of the thesis. It then provides a detailed description of AI-based ATs by offering examples of their use by PWDs, before briefly discussing the major challenges and risks that arise when using AI-based ATs.

The next three chapters will pursue three objectives in turn:

- The first objective of this thesis is to understand the potential privacy concerns that PWDs face while using AI-based ATs. This is covered in the third chapter.
- The second objective is to understand what makes PWDs especially vulnerable to potential privacy risks, especially while using AI-based ATs. The fourth chapter, while examining this exacerbated vulnerability of PWDs, considers two sets of reasons. The first set of

[5] Directorate-General for Parliamentary Research Services (European Parliament) et al, *Assistive technologies for people with disabilities. Part IV, Legal and socio-ethical perspectives* (LU: Publications Office of the European Union, 2018).
[6] Liane Colonna, "Legal and regulatory challenges to utilizing lifelogging technologies for the frail and sick" (2019) 27:1 Int J Law Inf Technol 50–74.

reasons is generic and applicable to any data subject; nevertheless, leads to increased vulnerability for PWDs. The second set of reasons is more specific to PWDs.

- The third research objective, discussed in the fifth chapter, is to analyze the current and pending Canadian legal framework for data protection and examine if there is any provision specifically addressing PWDs or vulnerable data subjects. Legislative gaps that could pose potential high privacy risks for data subjects will also be highlighted, especially as they apply to PWDs.

This thesis will act as a guiding source for organizations engaged in the business of AI-based ATs to understand the potential privacy concerns of their target audience (i.e., PWDs) and ensure the development of safe AI-based ATs. It will further contribute to the legal scholarship dealing with the exacerbated vulnerability of PWDs to potential privacy risks, especially while using AI-based ATs. Lastly, it aims to fill the void in the Canadian legal context by analyzing data protection legislative framework as it applies to data subjects, especially PWDs. Even though this research does not offer detailed recommendations, it suggests adoption of better privacy protection measures. The thesis does not argue about imposing a total ban on the incorporation of AI into ATs, but rather urges better legal regulations to protect PWDs' privacy.

2 Incorporation of AI in ATs for PWDs and their potential risks

Marginalized Groups, such as PWDs, are often the collateral damage of economic, social, and political advancement. The twenty-first century has added a component to the foundational economic, social, and political trio—technology. This technological revolution is also called the fourth revolution.[7] With emerging technologies, including social robots, IoT, and artificial intelligence (AI), we are now, more than ever, generating and using data at an unstoppable rate.[8] One such technology is ATs, which positively contributes to PWDs' lives. ATs aim to make everyday activities more accessible for PWDs.[9] It further contributes to independence, health, productivity, education, employment opportunities, and active participation in society for PWDs.[10] In order to function, ATs generate and process high volumes of data, or as the industry calls it, "the new oil",[11] at a rampant pace. Further, these technologies operate in connection to online servers which permit remote monitoring of user data and its aggregation, storage, and utilization.[12] These behind-the-scenes activities, in addition to PWDs' increasing reliance on ATs, raise serious potential privacy and cybersecurity concerns.

Before proceeding to further discussion of AI-based ATs revolutionizing the modern living standards for PWDs, it is crucial to understand the terminology to be used throughout this thesis, primarily the terms like "disability", "ATs", "AI" and "privacy". The absence of universal definitions for these major terms makes it more important to define them for this research.

---

[7] "The Fourth Industrial Revolution: what it means and how to respond", (14 January 2016), online: *World Econ Forum* <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.

[8] "How Fast Is Technology Growing Statistics [Updated 2023]", online: <https://leftronic.com/blog/how-fast-is-technology-growing-statistics/>.

[9] *Report of the Special Rapporteur on the rights of persons with disabilities,* UNGA, 49th Sess, UN Doc A/HRC/49/52 at 8.

[10] World Health Organization, "Assistive technology" (2 January 2024), online: <https://www.who.int/news-room/fact-sheets/detail/assistive-technology>.

[11] Nisha Talagala, "Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires" (2 March, 2022) online: <https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/>.

[12] Aqueasha Martin Hammond et. al., "Understanding design considerations for adaptive user interfaces for accessible pointing with older and younger adults" (W4A '15: Proceedings of the 12th International Web for All Conference, May 2015) [unpublished: <https://dl.acm.org/doi/abs/10.1145/2745555.2746645>.

2.1 Definitions

2.1.1 Disability

For this research, I will use the term "disability" throughout. The primary problem is defining the selected term "disability". Various organizations and legislatures have defined it differently, and its use in academic scholarship has changed overtime.[13] The literature finds that some experts believe there is no single definition of disability and that having a standard definition is neither possible nor desirable.[14] There are three primary reasons for this. First, the term's multidimensionality makes it a complex concept. For instance, when discussed in terms of physical or medical aspects, it is seen as an impairment. In contrast, when discussed as a social construct, people view it as a disadvantage because of historical systemic discrimination.[15] The second reason is the difference in the definitions used across various jurisdictions. Some define it based on the duration of the disability, others define it based on whether the certification of disability by a medical practitioner is required.[16] The third reason is that every policy or law has different eligibility criteria and objectives. For instance, the definition used in the context of human rights is broader as opposed to the definition used for entitlement to benefits.[17]

The World Health Organization (WHO) while discussing the term "disability" in its International Classification of Functioning, Disability and Health (ICF) considers its social aspects along with medical or biological aspect.[18] Whereas, the Americans with Disabilities Act (ADA), the USA's federal law prohibiting discrimination against PWDs, adopts a legal definition of disability than a medical one. ADA defines disability differently as opposed to how Social Security Disability related benefits in the US define disability.[19] ADA defines disability as:

> The term "disability" means, with respect to an individual (A) a physical or mental impairment that substantially limits one or more major life activities

---

[13] Erin E Andrews, *Disability As Diversity: Developing Cultural Competence* (Oxford University Press, 2019).
[14] Canada. Human Resources Development Canada. Office for Disability Issues, *Defining disability : a complex issue* (Ottawa - Ontario: Human Resources Development Canada. 2003), online: <https://publications.gc.ca/collections/Collection/RH37-4-3-2003E.pdf>
[15] *Ibid at* 39.
[16] *Supra* note 14 at 40.
[17] *Ibid.*
[18] "Disability and Disabilism - Manual for Human Rights Education with Young people - www.coe.int", online: *Man Hum Rights Educ Young People* <https://www.coe.int/en/web/compass/disability-and-disablism>.
[19] "What is the definition of disability under the ADA? | ADA National Network", online: <https://adata.org/faq/what-definition-disability-under-ada>.

> of such individual; (B) a record of such an impairment; or (C) being regarded as having such an impairment

An essential definition for this research is the one under the Accessible Canada Act (ACA). ACA's definition is broader and more detailed as compared to ADA's definition. It defines ''disability'' as:

> any impairment, including a physical, mental, intellectual, cognitive, learning, communication or sensory impairment—or a functional limitation—whether permanent, temporary or episodic in nature or evident or not, that, in interaction with a barrier, hinders a person's full and equal participation in society.[20]

This definition is essential for three reasons. First, it is in consonance with the United Nations *Convention on the Rights of Persons with Disabilities* (CRPD), the convention which protects PWDs. CRPD states that disability is not mere impairment; instead, it is a combination of impairment and the interaction of PWDs with "attitudinal and environmental barriers" which hinder PWDs from equally (compared to non-disabled people) interacting with the environment and society.[21] Second, based on this definition, Canadian courts have been considering contemporary factors, barriers, and developments like biomedical, technological, and social factors while formulating an equality-based framework for disability.[22] Lastly, ACA's definition covers different forms of disabilities, such as physical, cognitive, and sensory, as opposed to only physical and mental forms under ADA. Therefore, this study will follow the definition of disability provided by ACA because of its compliance with CRPD, consideration of barriers, and coverage of various forms of disabilities. To conclude, one shall construe disability as an outcome of a combination of barriers and an individual's impairment.

---

[20] Accessible Canada Act, S.C. 2019, c. 10, s.5.

[21] In 2010, Canada ratified the United Nations' *Convention on the Rights of Persons with Disabilities*, (2006), 13 December 2006, U.N.T.S. vol. 2515, [*CRPD*], (entered into force 3 May 2008, accession by Canada 11 March 2010). Available online at: www.un.org/disabilities/documents/convention/convention_accessible_pdf. From the Preamble (e) to the *CRPD:* Parties to the Convention are required to promote and protect the full enjoyment of human rights by people with disabilities and ensure that they enjoy full equality under the law. In Ontario, the provincial government passed the *Accessibility for Ontarians with Disabilities Act, 2005*, S.O. 2005, c. 11 [*AODA*] to improve accessibility standards for Ontarians with physical and mental disabilities in all public establishments by 2025].

[22] Quebec (Commission des droits de la personne et des droits de la jeunesse) v. Montréal (City); Quebec (Commission des droits de la personne et des droits de la jeunesse) v. Boisbriand (City), 2000 SCC 27 (CanLII), [2000] 1 SCR 665.

2.1.2 Assistive Technologies (ATs)

WHO explains "assistive technology(s)" as a term that includes products and services that aid and enable people to live "healthy, productive, independent, and dignified lives and to participate in education, the labour market, and civic life".[23] The phrase "any product or service delivering assistance" in the definition expands the scope of ATs. According to this, ATs can range from basic spectacles that correct vision to today's facial recognition apps used by PVI. For instance, this definition even includes powered eyeglasses that aid in viewing the world or, broadly, living an independent life. ATs are categorized based on different factors, such as level of technology—high tech or low tech, and purpose of AT—to enhance ability or improve accessibility.

The European Telecommunications Standards Institute (ETSI)'s *Accessibility requirements suitable for public procurement of ICT products and services in Europe*[24] provides a more contemporary definition by describing ATs as any:

> Hardware or software added to or connected to a system that increases accessibility for an individual. Examples include Braille displays, screen readers, screen magnification software, and eye tracking device.[25]

The significant difference in these definitions is the user base. The users could be either only PWDs or both PWDs and people without disabilities.[26] However, the common element in all definitions is the focus on their role in enhancing accessibility and offering a better standard of living. Unlike the WHO definition, the ETSI definition explicitly includes contemporary technology, including software, hardware, and product systems. For this research, I adopt a combination of these definitions and define ATs as any hardware, software, and product system whose purpose is to increase, maintain, or promote accessibility, independence, autonomy, and functioning capacity of PWDs and to reduce or eliminate the challenges, barriers, and limitations

---

[23] *Supra* note 10.
[24] ETSI, "Accessibility requirements suitable for public procurement of ICT products and services in Europe", online (pdf): <https://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.00.02_30/en_301549v010002v.pdf>.
[25] Marzin, Moledo & Naughton, *Supra* note 4.
[26] Interestingly, according to the definition provided by the province of British Columbia, ATs can be used by either disabled or non-disabled people. It defines ATs as—"*An umbrella term covering the systems and services related to assistive products. Both people with and without disabilities use AT. For example, speech recognition software (like Siri or Alexa) is a form of AT*."

faced by PWDs due to disability or incapacity.[27] Since this thesis primarily focuses on ATs using AI, such as facial recognition, image recognition, speech recognition, text-to-speech converters, and AI-programmed social robots, this definition is suitable because of two reasons. First, its focus on contemporary devices/products, and second, the current purposes that ATs intend to achieve including accessibility, autonomy and independence. The later sub-sections of this chapter discuss these technologies and their impact, benefits, and associated risks in detail.

2.1.3 Artificial Intelligence (AI)

Currently, there is no single universally agreed upon definition of AI. However, a discussion of AI would be incomplete without the definition of AI offered by Professor John McCarthy, also called the father of AI. He defines AI as "the science and engineering of making intelligent machines, especially intelligent computer programs."[28] This is a broad and generic definition and not necessarily the most suitable with the emerging complexities of AI, such as generative AI. The European Union's definition of AI under its AI Act is more detailed, suitable to emerging complications in AI, and complies with the OECD's[29] definition of an AI system:

> Artificial Intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.[30]

The original definition in the EU bill provided a list of techniques and approaches for the development of the software, mapping what AI does along with how it does it.[31] However, the new

---

[27] Freitas, Maurício Pasetto de et al, "Artificial Intelligence of Things Applied to Assistive Technology: A Systematic Literature Review" (2022) 22:21 Sensors (Basel) 8531.

[28] "What is AI? / Basic Questions", online: <http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html>.

[29] OECD, "Updates to the OECD's definition of an AI system explained", online: <https://oecd.ai/en/wonk/ai-system-definition-update>. OECD definition- "An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

[30] EU, *Regulation* 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 1 at 46; "Article 3: Definitions | EU Artificial Intelligence Act", online: <https://artificialintelligenceact.eu/article/3/>.

[31] Original EU AI Act definition: "*(1) 'artificial intelligence system' (AI system) means software developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*"

amended definition removed the list and instead now provides a broader scope by including the term "with varying levels of autonomy". This newly amended definition focuses more on what AI does rather than how it does it. I believe this last definition of AI is more suitable since AI's functioning is often a black box, and any attempt to define that aspect would eventually become obsolete given AI's rampant development. Thus, focusing on what AI does and including both explicit (for example, human prompts as in the case of ChatGPT) and implicit (for example, autonomous driving systems) functions is a better approach.

This thesis will follow the EU's definition because of its broader outlook on technology and its functional approach. It does not restrict the definition by providing a list, instead keeps it inclusive. This would help include any upcoming, unpredictable, or unknown technological developments in AI in the future. Thus, the EU's functional definition is more suitable for this research as it focuses on the functions and operations without the need to delve into the intricate implementation details.

2.1.4 Privacy

Various scholars have concluded that there is no one-size-fits-all definition of privacy because of the scope of the term privacy.[32] It is a broad concept that covers various forms of privacy, such as physical, spatial, informational, and decisional privacy. Highlighting the different types of privacy, La Forest J. in *R v. Dyment*[33] made a notable attempt at defining privacy and introduced three zones of privacy—personal privacy (dealing with the human body), territorial privacy (dealing with territory such as home), and information privacy (dealing with data or information of person). The focus of this research is on the third zone of privacy—informational privacy, which provides protection against, *inter alia,* data breaches,[34] control over information,[35] and the right to be alone.[36]

---

[32] Wilkinson, Daricia et al. "Moving Beyond a "one-size fits all": Exploring Individual Differences in Privacy" (delivered at Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, 2018) online: <https://dl.acm.org/doi/10.1145/3170427.3170617>.
[33] *R v Dyment,* [1988] 2 S.C.R. 417.
[34] Daniel J. Solve & Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 TEX. L. REV. 737 (2018).
[35] Alan F Westin, "Privacy And Freedom" (1968) 25: 1 Washington & Lee L Rev at 166.
[36] "Warren and Brandeis, 'The Right to Privacy'", online: <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

Some scholars argue that privacy focuses on control[37] whereas others argue that control is not the primary factor for understanding privacy.[38] Alan Westin, known as the father of modern data privacy law, has described the term privacy as "the control over how information about a person is handled and communicated to others."[39] Westin's definition focuses on the control dynamic. Whereas Neil Richards provides another important working definition in his book *Why Privacy Matters,* which does not focus on control. He defines privacy as "the degree to which human information is neither known nor used."[40]

As concluded by scholars, formulating a comprehensive definition of privacy would be a futile attempt, given its vast scope.[41] Therefore, as a pragmatic solution, it is suitable to adopt a working definition for this research. Since this research also focuses on information privacy, similar to Richards's book, the working definition proposed by Richards is the most suitable.

2.2 The Relationship of PWDs with Tech

World Health Organization (WHO) estimates that 15% of the world's population requires access to ATs,[42] and currently, one billion PWDs do not have access to ATs.[43] The gap between the need and actual access to ATs continues to be a struggle.[44] Some reasons for this gap are high-cost ATs that are often unaffordable for users, lack of properly trained AT professionals or experts, and lack of knowledge among people.[45] This issue has gained attention over the years, and as a result, global organizations have been working to reduce the disparity. Certain noteworthy initiatives and GATE (Global Cooperation on Assistive Technology) established by WHO in 2014

---

[37] Jonathan Salem Baskin, "The Privacy Debate Isn't About Secrets, It's About Control", online: *Forbes* <https://www.forbes.com/sites/jonathansalembaskin/2014/07/22/the-privacy-debate-isnt-about-secrets-its-about-control/>.
[38] Neil Richards, *Why Privacy Matters,* (the United States of America: Oxford University Press, 2022).
[39] *Supra* note 36.
[40] *Supra note 38 at 22.*
[41] "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997) 42 McGill LJ 355 , (1997) 42 RD McGill 355.
[42] World Health Organization. (2015). WHO global disability action plan 2014-2021: Better health for all people with disability.
[43] "Sovereign funds: future of assistive technology and disability AI | World Economic Forum", online: <https://www.weforum.org/agenda/2023/08/sovereign-funds-future-assistive-technology-disability-ai/>.
[44] *Supra* note 10. World Health Organisation. (2021).
[45] Luc de Witte et al, "Assistive technology provision: towards an international framework for assuring availability and accessibility of affordable high-quality assistive technology" (2018) 13:5 Disability Rehabilitation Assistive Technology 467–472.

signal the likelihood of AT market or industry expanding and gaining prominence in contemporary discussions.[46] Other notable initiatives are the UN 2030 Agenda for Sustainable Development[47] and the resolution adopted by the World Health Assembly in 2018 to provide access to ATs to promote the universal health coverage objective.[48]

Despite the unequal access to ATs, PWDs have been a crucial group at the forefront of using emerging technologies, and in particular, ATs.[49] These technologies have transformed the lives of many by offering them a better opportunity to interact with their environment. ATs help to carry out everyday chores and specialized tasks in different aspects of life including education, health, work, leisure, and mobility.[50]

The user base of ATs is burgeoning with people who were not initial target users becoming part of a majority user base. Even people without disabilities use some ATs in their everyday life, which makes those ATs mainstream. For instance, applications like Google Docs or web browsers like Microsoft Edge integrated with the audio command features and the speech-to-text feature. Not just ATs, people without disabilities also use other innovations which were originally developed for PWDs.[51] Some landmark examples of such innovations include integration of audio-to-text converters into our phones' search engines like Google Chrome; use of audiobooks by people without visual impairment or perceptual disabilities; and use of video captioning—originally created for people with hearing impairment. This change in user base may be a result of universal design principles demanding equity and inclusivity.[52] Not surprisingly, PWDs also use the technology targeted at the general audience to enhance accessibility. For instance, PWDs use the infamous virtual assistants, Alexa by Amazon and Siri by Apple for visual impairment or mobility disability to perform functions on their devices. ATs have applications in different

---

[46] Sarah Abdi, et. al., "Emerging technologies and their potential for generating new assistive technologies, Assistive Technology" (2021) 33 The Official J of RESNA at 517.
[47] "Transforming our world: the 2030 Agenda for Sustainable Development | Department of Economic and Social Affairs", online: <https://sdgs.un.org/2030agenda>.
[48] "World Health Assembly endorses resolution on social participation", online: <https://www.who.int/news/item/29-05-2024-world-health-assembly-endorses-resolution-on-social-participation>.
[49] "Assistive tech enables people with a disability to live independently", online: <https://blog.richardvanhooijdonk.com/en/assistive-tech-enables-people-with-a-disability-to-live-independently/>.
[50] *Rights of persons with disabilities-Report of the Special Rapporteur on the rights of persons with disabilities*, HRC, 49th sess, UN Doc A/HRC/49/52 (2021).
[51] *Ibid.*
[52] The seven principles of Universal Design are equitable use; flexibility in use; simple, intuitive use; perceptible information; tolerance for error; low physical effort; and size and space for approach for use.

domains, including mobility, communication, vision, cognition, hearing, self-care, commercialization, and environment.[53] Despite the use of ATs by people without disabilities, the current research and development (R&D) related to ATs focuses more on the needs of PWDs.[54] The below sub-sections discuss ATs focused on PWDs.

Before proceeding to different ATs available in the market, it is interesting to note that a study by the EU found that ATs catering to PVI outnumber the ATs for people with other forms of disabilities.[55] This discrepancy is because of the informational revolution which has focused more on visual modes of communication.[56] However, given the growing pace of technology, the industry expects the revolution to focus on sensory or sound modes as well, thereby growing the landscape of ATs.[57] Another report by WIPO—*WIPO Technology Trends 2021 Assistive Technology Report* (WIPO Report) analyzed the number of patents registered and revealed that major corporations are leading the R&D of ATs, especially in vision, hearing, and communication.[58] Thus, based on the data, a majority of examples in this thesis will surround visual ATs used by PVI.

According to the WIPO Report, the results of a patent search conducted from 2015 to 2022 revealed that developers filed for a stark number of 15,000 patents related to ATs enabled by emerging technologies.[59] This new era of technologies targeted at PWDs includes the incorporation of reality technologies such as virtual reality (VR) and augmented reality (AR), robotics, human-computer interface,[60] AI and the internet of things (IoT).[61] ATs have been revolutionary for PWDs from hearing aids to ASL convertors. With the incorporation of emerging technologies, experts expect ATs to play an even bigger role in PWDs' lives.[62]

---

[53] World Intellectual Property Organization, *WIPO Technology Trends 2021- Assistive Technology*, online: <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055_2021.pdf>.
[54] *Ibid.*
[55] R. Matter, et. al., "Assistive technology in resource-limited environments: a scoping review" 12:2 Disability and Rehabilitation: Assistive Technology, online: <https://www.tandfonline.com/doi/full/10.1080/17483107.2016.1188170>.
[56] *Ibid.*
[57] *Supra* Note 2.
[58] World Intellectual Property Organization, *supra* note 53.
[59] *Ibid* at 32.
[60] *Supra* note 46 at 519.
[61] *Ibid.*
[62] World Intellectual Property Organization, *supra* note 53.

Figure 1: Enabling Technologies for Upcoming ATs; source: WIPO Report[63]

[Figure 1 description:

Enabling technologies: Addictive manufacturing, IoT and connectivity, brain-computer machine interface, advanced sensors, AI, virtual reality/augmented reality, new materials, and robots.

Six categories of ATs: self-care, vision, communication, environment, hearing, and mobility.]

Figures 2 and 3 below describe ATs into six categories: vision, self-care, mobility, communication, environment, and hearing.

---

[63] *Ibid* at 31.

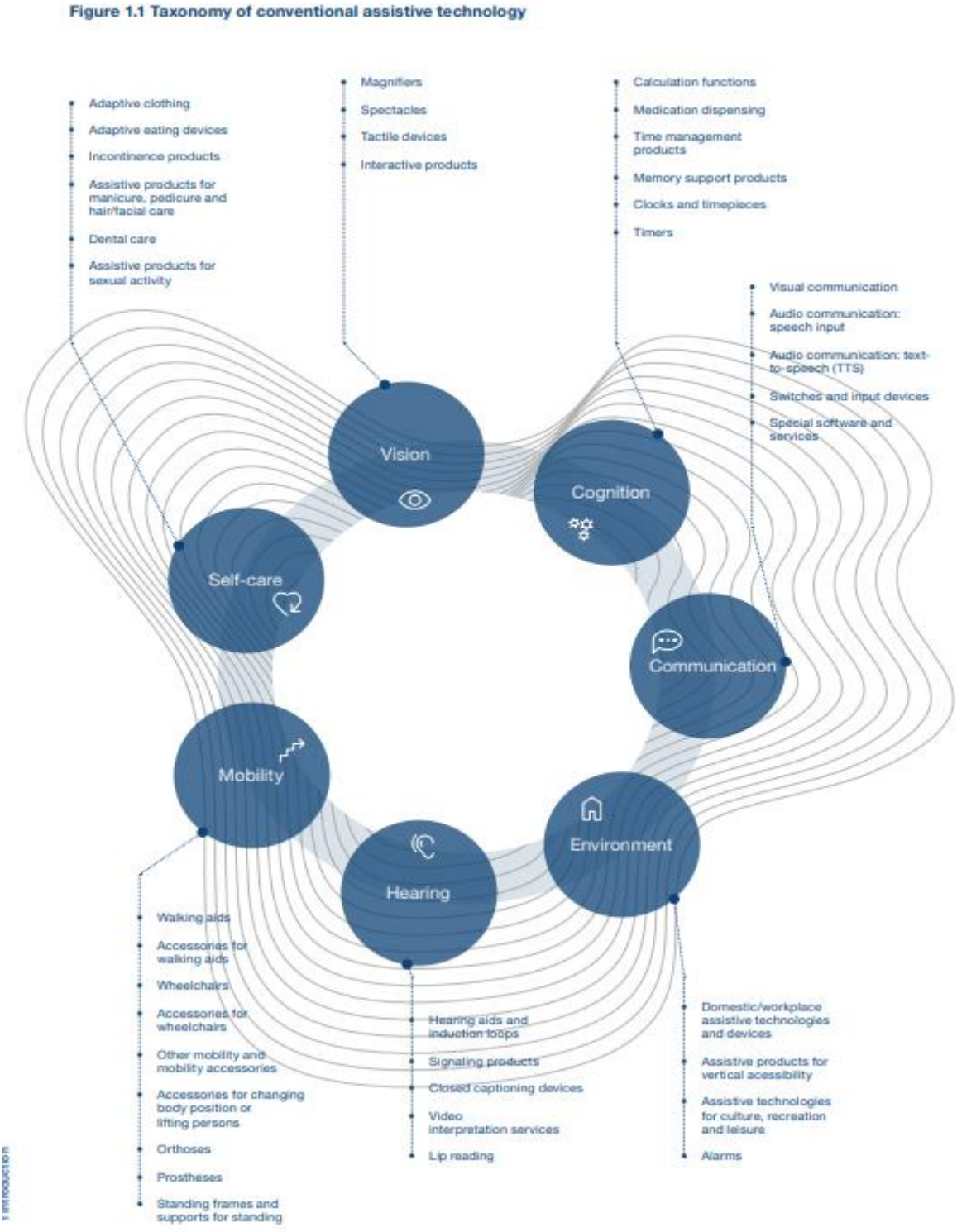

Figure 2: Diagram of conventional ATs; Source: WIPO Report[64]

[64] *Ibid* at 28.

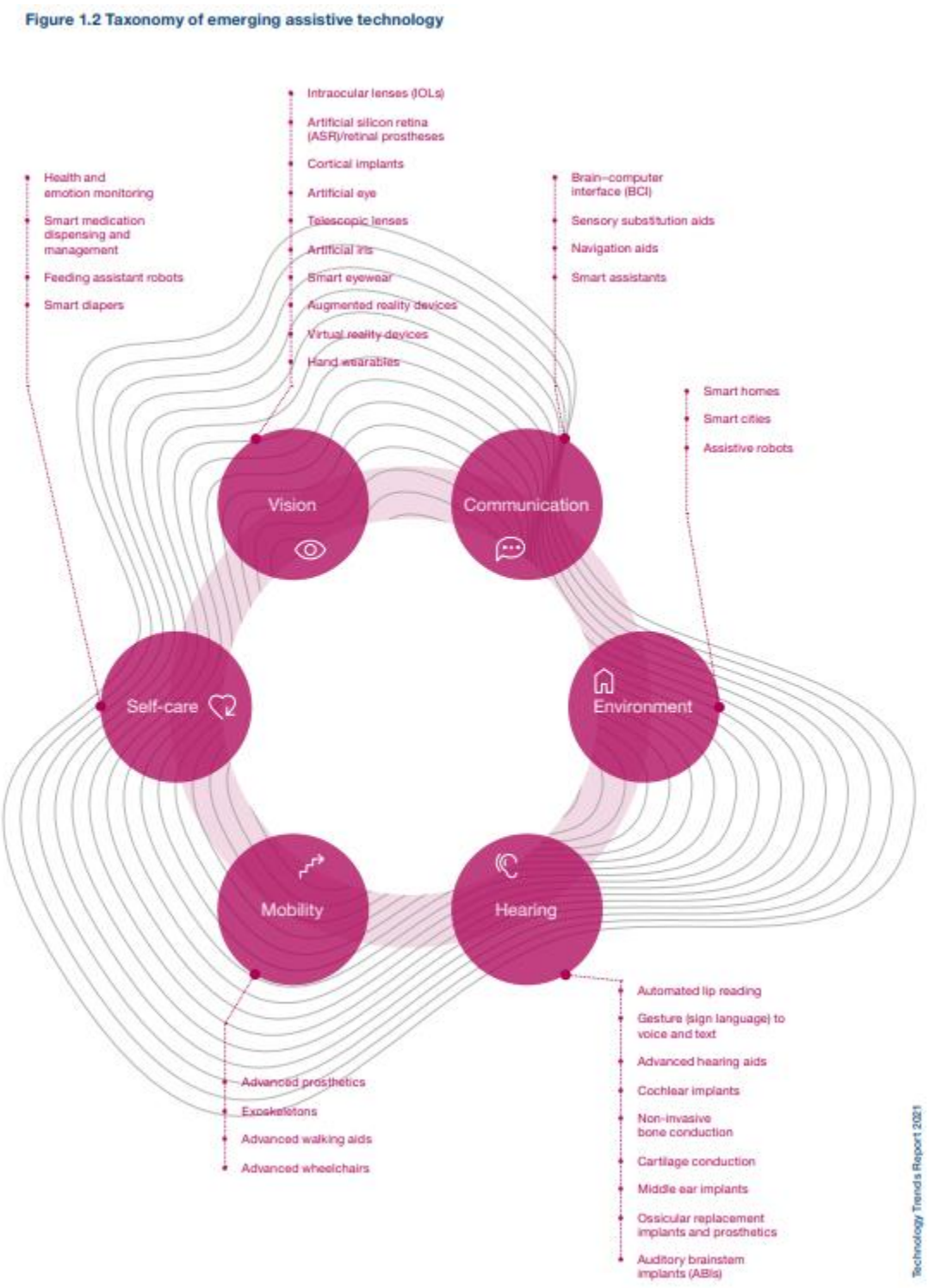

Figure 3: Diagram of emerging ATs; Source: WIPO Report[65]

[65] *Ibid* at 29.

2.2.1 Incorporation of AI in ATs: a game changer

In this era of emerging technologies, AI is the buzzword. Incorporation of AI in varied technologies and frequent development of new AI models, from Machine Learning (ML) models to Large Language Model (LLM) backed generative AI (the recent development of ChatGPT), is undoubtedly transforming the world. AI is all around us, more than we anticipated or currently appreciate. For instance, AI is assisting in the recruitment process by assessing applications, conducting video interviews, and assessing loan or credit applications. The infamous AI-empowered chatbots are now employed for a broad range of purposes, including marketing, sales, and consulting.

Similar to other spaces, AI is transforming the AT space by aiming to create a more accessible and inclusive world for PWDs. AI-based ATs are assisting PWDs in various ways, such as eye-tracking, mobility, voice-recognition, and image recognition.[66] Along with assisting, AI-based ATs often pose potential privacy risks to PWDs and their data. Users have a mixed reaction to the pro and cons of these AI-based ATs. Some users believe AI-based ATs to be more helpful than detrimental, despite being aware of privacy and data protection concerns.[67] To better understand incorporation of AI in ATs, the following sub-sections will discuss AI-based ATs as per the six categories of ATs described in figures 2 and 3.

2.2.1.1 Hearing

AI-enabled ATs for people with hearing impairment are among the top categories of ATs by the number of patents filed.[68] Such ATs include automated lip-reading technology which use facial recognition to analyze lip movements and provide the result.[69] Another crucial device is the cognitive hearing aid developed by the Columbia School of Engineering and Applied Science. This hearing aid assists in hearing sounds and observing brainwaves to deduce the listening requirements or wants of the user.[70] ATs that convert sign language or gesture to text and speech

---

[66] *Ibid* at 8.
[67] Lydia Manikonda, "What's up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants" (delivered at AIES '18: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, 2018) online: <https://dl.acm.org/doi/10.1145/3278721.3278773>.
[68] World Intellectual Property Organization, *supra* note 53 at 91.
[69] *Supra* note 2.
[70] "Cognitive Hearing Aid Filters Out the Noise", (4 August 2017), online: *Columbia Eng* <https://www.engineering.columbia.edu/news/nima-mesgarani-cognitive-hearing-aid>.

by using sensors to detect hand movements, gestures, and position are another emerging hearing AI-enabled ATs. A famous example of this is Google Glasses, which offers a sign language interpretation feature.[71] However, the Google glasses faced criticism for posing high potential privacy concerns.

Some advanced hearing aids use a combination of AI and sensors to record and maximize the targeted sound or voice while observing the brainwaves. An interesting trend is the use of AI-enabled hearing aids[72] which enable the collection and storage of data related to a user's environment to optimize settings and enhance the user experience for later revisits.[73] For instance, Google apps: Live Caption, Live Transcribe, and Sound Amplifier use this feature to assist people with hearing or cognitive impairment. While these ATs offer benefits to people with hearing impairment or any other impairment, they raise potential privacy concerns, [74] discussed in the next chapter.

An interesting AI-based hearing AT is an app called Ava with over 100,000 people with hearing impairment as its users.[75] It is primarily an audio-to-text converter app where users join a group and converse with fellow users by speaking into the mic. The app then converts audio into text in real time for people who prefer to read along.[76] Voiceitt is yet another innovation that targets people with speech impediments. The app hears the audio of people with temporary or long-term speech conditions like Down Syndrome or Parkinson's. It then converts the mispronounced words into correct audio or textual output by identifying the individual speech patterns.[77] The advanced AI speech recognition software improves the clarity of hearing aids in the presence of noise and increase prediction quality by analyzing different languages, pronunciations and accents.[78]

---

[71] "Google's New Glasses Can Translate Speech in Real Time | IoT World Today", online: <https://www.iotworldtoday.com/iiot/google-s-new-glasses-can-translate-speech-in-real-time->.
[72] "Learn how SoundSense Learn makes listening easier. | Widex" (30 May, 2018), online: <https://www.widex.com/en-ca/blog/global/soundsense-learn/>.
[73] World Intellectual Property Organization, *supra* note 53 at 90. [Bradley McPherson, University of Hong Kong]
[74] Ibid at 95.
[75] *Ibid.*
[76] Jackie Snow, "People with disabilities are using AI to improve their lives" (30 January 2019), online: <https://www.pbs.org/wgbh/nova/article/people-with-disabilities-use-ai-to-improve-their-lives/>.
[77] Ibid.
[78] *Ibid.*

2.2.1.2 Vision

According to the WIPO report, this category has one of the highest numbers of AT inventions and patent filings.[79] Some common vision-related AI-based ATs are screen readers, location and GPS apps, and image or facial recognition-based ATs used for money identification, object identification, and colour identification. *Be My Eyes* is a noteworthy visual AT that originally works by connecting PVI with sighted volunteers to assist viewing the world and providing information.[80] However, it has now paired with Microsoft to provide AI-powered visual assistance which eliminates the requirement of a sighted volunteer.[81] Other examples include Facebook's introduction of the "Automatic Alternative Text" in 2016 which provides an image description even if the image has no alternative text. This Facebook tool uses image recognition model to identify expressions, characteristics, weather, or landscape in the image and provide a detailed description.[82] In 2017, Facebook took a further step and introduced facial recognition technology to identify the people in the image, even if they were not tagged.[83] A similar invention by Microsoft is Microsoft's Seeing AI app which assists PVI to view the world using features like image and facial recognition, text recognition, scene description, barcode scanning, and handwriting recognition. The user captures an image using the camera of a smartphone or any other device compatible with the app and the app works by describing the images captured.

ATs in the vision category also cover AI-enabled ATs that simplify the documents for people with intellectual disabilities. These AI-enabled ATs convert dense text or text with jargon into simpler language, pictorial representation (stats pie-charts, graphs or images), audio, or sign language. A notable AT is the website *Polisis* which uses machine learning algorithms to understand the website's privacy policy and provide a simplified version in terms of flow cart or

---

[79] World Intellectual Property Organization, *supra* note 53 at 165.
[80] "Be My Eyes - See the world together", online: <https://www.bemyeyes.com/>.
[81] *Ibid*.
[82] Jessica Guynn, "Facebook taps artificial intelligence for users with disabilities" (23 March 2016), online: *USA TODAY* <https://www.usatoday.com/story/tech/news/2016/03/23/facebook-accessibility-people-with-disabilities/82026554/>.
[83] Joaquin Quiñonero Candela, "Managing Your Identity on Facebook With Face Recognition Technology | Meta" (19 December 2017), online: <https://about.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/>; Facebook discontinued its facial recognition feature in 2021: "An Update On Our Use of Face Recognition | Meta", online: <https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>.

summary. [84] This helps individuals understand the complex data collection and processing better. *Polisi* is a free software that users can use by adding it as an extension to their web browser.[85] Lastly, AR and VR devices combined with AI, smart eyewear, and artificial vision and hand wearables are also some upcoming ATs.[86] One such AT is *OrCam MyEye* device which works as AI-driven vision by reading out texts, recognizing faces, objects, colors, and currency.[87] A user can use this by magnetically attaching it on a spectacle frame and the device converts image or text into speech by following the user's gaze or their pointed hand gestures.[88] Notably, some AI-based AT apps work even without internet connection by deploying the stored data to identify objects.[89]

2.2.1.3 Communication

PWDs have been using Accessibility and Augmentative Communication (AAC) technologies like text-to-speech, sign language recognition, visual communication, and speech input for a while; however, AI models have advanced their functioning. An example of such AT is the eye mouse-based technology, which comprehends the blinking of the eye as a mouse click and performs functions.[90] This monitoring of eye movement is possible because of the algorithmic model. People with mobility issues use such an AT for communicating. Another crucial development is the use of Generative AI in ATs. The potential of incorporating Generative AI is astonishing. It could augment ATs and robotics, create personalized healthcare and learning solutions,[91] improve accessibility by being associated with speech-to-text or image description

---

[84] Andy Greenberg, "An AI That Reads Privacy Policies So That You Don't Have To" *Wired* (9 February 2018), online: <https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/>.
[85] Hamza Harkous et al, *Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning* (arXiv, 2018) arXiv:1802.02561 [cs].
[86] World Intellectual Property Organization, *supra* note 53 at 144.
[87] *Ibid* at 153.
[88] *Ibid*.
[89] AIPOLY "Aipoly Puts Machine Vision In The Hands Of The Visually Impaired | TechCrunch", online: <https://techcrunch.com/2015/08/17/aipoly-puts-machine-vision-in-the-hands-of-the-visually-impaired/>.
[90] World Intellectual Property Organization, *supra* note 53.
[91] World Economic Forum, "Generative AI holds great potential for those with disabilities – but it needs policy to shape it" (6 November 2023), online: *Eur Sting - Crit News Insights Eur Polit Econ Foreign Aff Bus Technol - Eur* <https://europeansting.com/2023/11/06/generative-ai-holds-great-potential-for-those-with-disabilities-but-it-needs-policy-to-shape-it/>.

software, assist creating an accessible user interface or design, such as broader text, font size, or color to benefit PVI or people with cognitive impairment.

2.2.1.4 Environment

AI-based ATs used in workplace or domestic environment can assist people with functional limitations to access their surroundings. This category includes ATs used in the bathroom or bed and their accessories to provide innovative structures that assist mobility. The second category of environment ATs are ATs used for leisure, recreation, and culture. For instance, IBM is developing AI Suitcase, which is a robot designed as a suitcase. [92] The purpose of this AT is to guide PVI while travelling by using, *inter alia*, image recognition, sensing techniques, and vision sensors. In case the suitcase robot detects any obstacle, it alarms the PVI with a sound or tactile sensation. Certain environment ATs like lateral and vertical movement technologies in smart homes function on ML and robotics. The rise of smart robots has also seen the introduction of AI Robots which incorporate AI system into the physical form of a robot.[93] These robots assist people with mobility, or functional limitations live independently by performing certain tasks for them.[94] They can indulge in conversations with the user and record or process data; and act as assistants by fulfilling the requested tasks. For instance, people with mobility issues or PVI can use such ATs in finding an object or sharing a device's location. [95]

2.2.1.5 Self-care

This category includes the in-demand health-tech wearables, non-wearables, and emotion monitoring devices. These devices track and record data, identify patterns, and offer personalized recommendations.[96] In the non-wearable category, smart platforms are emerging,[97] which connect to a cloud server and collect monitoring information, health, and emotional data.[98] Certain smart

---

[92] World Intellectual Property Organization, *supra* note 53 at 77.
[93] *Ibid*.
[94] *Ibid* at 69.
[95] AIPRM, "Artificial Intelligence and Assistive Technologies · AIPRM", (22 August 2023), online: <https://www.aiprm.com/education/artificial-intelligence-and-assistive-technologies/>.
[96] World Intellectual Property Organization, *supra* note 53 at 122.
[97] *Ibid* at 131.
[98] Global Disability Innovation Hub, "Physiological computing, artificial intelligence and empowering our capability", online: *Glob Disabil Innov Hub* <https://www.disabilityinnovation.com/projects/physiological-computing-artificial-intelligence-and-empowering-our-capability>.

medication dispensing and management devices use AI features like facial recognition to record data and remind intake of medicines.[99] This is a fairly new category that has attracted tech giants like Google and Apple. These ATs assist people with cognitive impairment and their caregivers by maintaining records or setting reminders. Another interesting technology is social robots, robotic pets or companion pets.[100] Developers often equip these robots with cameras to record data and utilize ML models to detect user emotions.[101] Based on observed patterns and trained datasets, the robot or pets offer comfort to the user using facial recognition technologies. These ATs can assist people with mental disabilities.

2.2.1.6 Mobility

The use of AI, advanced sensors, and other emerging technologies show a change in the mobility category. These include advanced prosthetics incorporated with cameras and ML algorithmic functioning, wheelchairs that use neural signals, and AI models that function according to user prosthetic control behaviour and object detection.[102] Another example is the advanced balancing aids functioning using AI and IoT.[103] If trained rightly, these AI navigation systems could assist PWDs in an individualized manner based on their personalized requirements and preference. Moreover, some navigation aids, such as smart canes, now use ML to observe user movement patterns and provide optimal navigational routes.[104] The smart assistants that use AI, especially ML, collect and process user data, primarily the user's interests, routines, preferences, and behavioural patterns, to perform the desired tasks or provide customized recommendations.[105] Such smart assistants assist in everyday tasks, including shopping, ordering, recommending lifestyle changes, and controlling home appliances.[106] This increases access to the environment and assists in communication. However, one shall not ignore the potential data privacy concerns that arise. An important point to remember is that one should not consider AI as a replacement for

---

[99] World Intellectual Property Organization, *supra* note 53 at 132.
[100] *Ibid* at 69.
[101] Matteo Spezialetti, Giuseppe Placidi & Silvia Rossi, "Emotion Recognition for Human-Robot Interaction: Recent Advances and Future Perspectives" (2020) 7 Front Robot AI 532279.
[102] World Intellectual Property Organization, *supra* note 53 at 109.
[103] *Ibid* at 111.
[104] *Ibid* at 50.
[105] *Ibid* at 53.
[106] *Ibid.*

infrastructural advancement. Mobility ATs would be successful in fulfilling their purpose only if the infrastructure supports them.

These advanced AI-enabled ATs, when incorporated into mobile devices, help PWDs living in less resourceful areas or with financial constraints have access to modern technology. If users collaboratively update the AI-enabled AT systems, it will assist ATs in providing better user-targeted experience. A major benefit of the incorporation of AI into ATs is its ability to provide improved and personalized solutions. Its growth offers the opportunity to co-design and develop ATs as per individual requirements and preferences. Elimination of human intermediaries by AI to perform tasks minimizes the risk of privacy breach by such intermediaries. However, AI involves its own set of potential privacy risks discussed in the next chapter. On the one hand, AI-enabled ATs could benefit from crowdsourcing data from AT users to train models; on the other, this data collection and its use to train AI models pose a potential risk of a data breach or misuse of data. These emerging technologies, especially AI, have increased access and made PWD more independent. However, does this independence come at the cost of compromising information privacy, given the involvement of data or information? The third chapter of this thesis will discuss this question in detail.

2.3 Challenges to using AI-based ATs and the associated risks

ATs have long been striving to make the world more accessible for PWDs by offering convenience in performing everyday activities. With the AI-driven innovation, AI-based ATs are increasing in number.[107] In the context of PWDs and AI, a detailed discussion continues to circle around fairness, discrimination, and bias issues created by AI, the issues originating from generative AI, the use of AI in decision-making like the hiring process, and others. The following sub-sections will cover three major challenges and risks associated with AI-based ATs.

[107] UCL, "Policy brief: Powering Inclusion: Artificial Intelligence and Assistive Technology", (23 November 2022), online: *UCL Dep Sci Technol Eng Public Policy* <https://www.ucl.ac.uk/steapp/policy-brief-powering-inclusion-artificial-intelligence-and-assistive-technology>.

2.3.1 Accessibility

Accessibility and usability challenges while using AI-based ATs are very common. The requirement of physically controlling equipment or navigating an interface could be challenging for people with different disabilities.[108] Mobility, including gestures, clenching, rotating, and lifting can be difficult resulting in problems while using AI-based ATs.[109] For instance, controlling a VR headset or clicking the tiny buttons on the headset could be challenging for an individual with cognitive or mobility impairment. Despite the advancement of ATs by incorporation of AI, websites and apps are often hard to navigate because they lack accessible features.[110] Some common accessibility issues with AI-based ATs are limitations linked to the accuracy and connectivity of ATs and lack of standardization.[111] Studies show that lack of training and education in universal design and accessibility is a major reason that often results in designing a difficult-to-use or inaccessible product.[112] A solution is to "enable hyper-personalization/customization, so tech adapts to human diversity."[113]

2.3.2 Discrimination or bias

Discrimination or bias in AI is a pressing concern when AI is deployed for decision-making purposes. Biasness of algorithms or discrimination in their results is a well-known downside of AI models. For instance, use cases show that AI models often fail to identify the facial features of a person with Down syndrome,[114] or provide biased or discriminatory results based on disability, race, gender, sex, and other demographics.[115] However, this discussion falls under the category of AI-risks, which is a detailed research area beyond the scope of the current research.

---

[108] Sheryl Burgstahler, Ph.D., "Working Together: People with Disabilities and Computer Technology | DO-IT", online: <https://www.washington.edu/doit/working-together-people-disabilities-and-computer-technology>.
[109] *Supra* note 4 at 22.
[110] Kate Kalcevich, "Mobile Accessibility Barriers For Assistive Technology Users" (19 February 2024), online: *Smashing Mag* <https://www.smashingmagazine.com/2024/02/mobile-accessibility-barriers-assistive-technology-users/>.
[111] UCL, *supra* note 107.
[112] *Supra* note 4.
[113] *Ibid* at 24.
[114] Stephanie Meredith et al, "The impact of implicit and explicit bias about disabilities on parent experiences and information provided during prenatal screening and testing" (2024) 17:1 Disabil Health J 101514.
[115] IBM Data and AI Team, "Shedding light on AI bias with real world examples", (16 October 2023), online: *IBM Blog* <https://www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples/www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples>.

2.3.3 Privacy and security

Privacy concerns are the centre of discussion of this research, and the second chapter examines them in detail. Concerns related to privacy and security link with the form and extent of disability.[116] In addition to disability, various factors, including but not limited to people, laws, regulations, technologies, and policies, affect PWDs' willingness to disclose personal information.[117] Users are often unaware of what data processors collect, how they collect it, and to what extent they use it. Despite a legal obligation on entities to provide a detailed privacy policy, studies have shown that users, especially PWDs, are unaware of privacy and data rights or the entities' actual data processing details.[118] Highlighted reasons for the same are, *inter alia,* lack of understanding and complex language making it hard for people to understand, especially people with cognitive impairment.[119] Technology experts state that the technological environment can be more dangerous for PWDs making them easy targets for fraud[120] or using technology can reveal information about their disability or conditions, leaving digital footprints that could lead to exclusion.[121] Such cybercrimes or cybersecurity breaches often lead to compromising of privacy. The next chapter delves deeper into the privacy risks caused by the usage of AI-based ATs.

To conclude, another highlighted reason for increased risks is the lack of investment in AI-based ATs by the private sector. [122] This lack of investment slows the invention process and makes it hard to cut down the cost of AI-based ATs. Cost is always a major barrier for any product in the market. A solution for the same is to increase public or government funding for R&D related to

---

[116] Abdul Rohman, et. al., "A continuum of context in informational privacy transmissions: insights from people with disabilities in Vietnam" (2023) Universal Access in the Information Society 1 at 4.
[117] Degutis, Mindaugas et al. "Willingness to Disclose Personal Information: How to Measure it?" (2020) 31 The Engineering Economics 487.
[118] Yuanyuan Feng, et al. "Understanding How to Inform Blind and Low-Vision Users about Data Privacy through Privacy Question Answering Assistants" (2023) *ArXiv*.
[119] Baiqi Chen, et al. "Investigating Users' Understanding of Privacy Policies of Virtual Personal Assistant Applications" (*Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, 2023) online: <https://doi.org/10.1145/3579856.3590335>.
[120] *Supra* note 4 at 27 ("Axel Leblois of G3ICT, the digital environment is "super risky for persons with disabilities").
[121] Shadi Abou Zahra, Accessibility Strategy and Technology Specialist at the World Wide Web Consortium – Interview: "*privacy needs much more attention and persons with disabilities need to be part of the conversation*."
[122] "Assistive Technology: Canada's Little-Known Opportunity", (29 January 2024), online: *TheFutureEconomy.ca* <https://thefutureeconomy.ca/op-eds/assistive-technology-eyra-abraham-lisnen/>.

emerging technologies for PWDs.[123] This would assist in either bringing down the cost or increasing government financial aid for PWDs to afford emerging ATs.[124] Another factor is the lack of training and education provided to people.[125] Technological advancements become ineffective if the targeted user (here PWDs) faces extreme difficulty in operating the technology. Out of all the risks highlighted in this section, the focus of this research is on information privacy risks associated with AI-based ATs, and therefore, the next section will discuss that in detail.

[123] *Ibid.*
[124] *Supra* note 1.
[125] World Intellectual Property Organization, *supra* note 53 at 197.

3 Potential Informational Privacy Risks in AI-based ATs for PWDs

As highlighted in the previous chapter, the inclusion of AI in ATs is helping PWDs immensely. However, this blessing comes with a curse of potential privacy and data protection risks. Research suggests that most of the privacy risks or concerns raised about using AI-based ATs are also typical for AI technologies in general. Nonetheless, this chapter aims to highlight those concerns, along with the application of Fair Information Practice Principles (FIPPs) to AI-based ATs or AI, and effects on PWDs in case of non-compliance. It further provides examples of those concerns in the context of AI-based ATs to facilitate a deeper comprehension of their significance for PWDs.

3.1 Privacy Concerns vis-à-vis Fair Information Practice Principles

As mentioned under the subheading of the 'privacy' definition in the previous chapter, for the purpose of this thesis, privacy means information privacy governed by data protection laws. These data protection laws generally apply whenever personal data is involved, and in the case of AI, usually in the following three stages[126]—collection of personal data; usage of personal data to train, test or validate an AI model; and inputting or inferring personal data with an AI model.[127]

Every jurisdiction has a different data protection legislative framework influenced by that jurisdiction's economic, social, political and other factors. However, the OECD's *Guidelines governing the protection of privacy and trans-border flows of personal data*, also called the Fair Information Practice Principles (FIPPs)[128], form the basis of data protection legislation in most jurisdictions. There are eight FIPPs—collection limitation; data quality (accuracy); purpose specification; use limitation; security safeguards; openness; individual participation; and accountability.[129] In addition to data protection laws based on these FIPPs, private entities face compliance requirements that arise from other sources, including regulations issued by regulatory authorities, common law[130] regulatory considerations such as competition law, internal rules and

[126] Alberto Quintavalla & Jeroen Temperman, eds, *Artificial Intelligence and Human Rights* (Oxford, New York: Oxford University Press, 2023) at 124.
[127] *Ibid.*
[128] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: Organisation for Economic Co-operation and Development, 2002).
[129] OECD, *The Privacy Framework*, (2013) at 14 & 15.
[130] Established through class action related to alleged misuse or treatment of data.

regulations of service providers (privacy policies, user notices, and terms of use), and specific industry standards like reasonableness.

The discussion of information privacy is closely connected to the processing of data. Most businesses, including those offering advanced technological products and services, involve the generation and processing of data.[131] As per a 2023 data privacy and data protection survey, approximately 70% of organizations anticipate an increase in the amount of data they deal with in the coming three years.[132] However, the scope of the collection, storage, dissemination and other parts of data processing differs for each technology. Disclosure of this scope by data processors and controllers in their privacy policies or notices is a requirement under law in many jurisdictions. Reading the privacy notices, including privacy policies and terms and conditions, of these AI-based ATs comprehensively can be more perplexing than enlightening. These privacy notices often contain ambiguous language and at times fail to serve the intended purpose of explaining the processing and handling of an individual's data.[133] More often than not, these notices leave individuals uncertain about—What is the extent of data sharing? Which third parties have access to data? Whether AI models use the data for training? Whether data deletion requests lead to complete deletion of data once the data collected is a part of the training set?[134]

For instance, the privacy policy of *BeMyEyes*, an AI-based AT for PVI, states that third parties assist the company in providing services.[135] It further states—"If you use Be My AI or another Service powered by third-party artificial intelligence technology, and the images or video you submit contain personal information, that information could be processed by our third-party provider to train and improve the artificial intelligence technology."[136] Firstly, the user consenting

---

[131] "What Is Data Privacy? | IBM", (12 March 2024), online: <https://www.ibm.com/topics/data-privacy>.
[132] "2023 Data Privacy and Data Protection Survey: Complex and Underfunded", online: *IDC Prem Glob Mark Intell Co* <https://www.idc.com/getdoc.jsp?containerId=US50134723>.
[133] Joel R Reidenberg et al, "Ambiguity in Privacy Policies and the Impact of Regulation" (2016) 45:S2 J Legal Studies S163.
[134] Solon Barocas & Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent" (Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information, 2009) [unpublished] online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409>.
[135] Be My Eyes, "Privacy Policy", online: <https://www.bemyeyes.com/privacy> See: *"Like most companies, we use third parties to help us provide our Services. When we do, our first choice is to not provide that third party with access to any personal information. But if that third party has to have access to your personal information to help us provide our Services, then, with the one exception described below, we will share the information with them under an agreement that does not allow them to use it for any other purpose…"*
[136] *Ibid.*

to this privacy policy most likely would be unaware of who these third parties are. Secondly, the practice of using PWDs' personal or sensitive data to train AI models itself poses a high potential privacy risk.

Every emerging technology that relies on data brings unique potential privacy concerns. However, the potential of AI and its application to ATs elevates the potential privacy risks,[137] making it essential to address these elevated risks. The first distinctive ability of AI is its capacity to process large volumes of personal or sensitive data in order to operate, which raises further concerns about the storage, access and usage of that data. Certain questions arise here, for instance—Where is this data coming from? Where is it stored? Who can access it? And under what circumstances? Secondly, AI (including machine learning (ML) and deep learning) systems' unexplainable ability to analyze AT users' personal data, learn and teach themselves, make predictions, develop adaptive models, and function non-transparently amplify data breach and privacy concerns. This inability of humans to understand or explain an AI system's decision-making process is called the black box phenomenon.[138] For instance, if developers of an Audio-Visual Speech Recognition (AVSR) AT are not familiar with the decision-making process of that AT, they cannot be certain of the data collection or use purpose or its full deletion from the system after the intended use. Additionally, the analysis of personal data, including location, habits, and behaviour, poses the risks of surveillance, identity theft, and unauthorized data dissemination.

The following excerpt from the 'Plug and Pray' report issued by the European Disability Forum[139] highlights the issue of 'lack of understanding of privacy concerns' which is relevant to the current research:

> Similar questions have been raised about detection of assistive technologies. For example, some accessibility experts have raised concerns about screen reader or browser detection. Lack of understanding about the implications of processing and sharing data, including highly sensitive personal data (e.g. health, disability, biometrics) is common. In a data-driven economy, there is a risk that some could be using this to their advantage. It is therefore

---

[137] "Resolution on the EU Artificial intelligence Act for the inclusion of persons with disabilities", (1 April 2023), online: *Eur Disabil Forum* <https://www.edf-feph.org/publications/resolution-on-the-eu-artificial-intelligence-act-for-the-inclusion-of-persons-with-disabilities/>.

[138] "AI's mysterious 'black box' problem, explained | University of Michigan-Dearborn", online: <https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained>.

[139] *Supra* note 4.

> important for persons with disabilities to be aware of the risks and to know how to protect themselves.

The following sections will answer some of the questions raised in this section while highlighting the implications of data protection principles, privacy risks, and the difficulty in compliance with these principles while using AI-based ATs.

3.1.1 Data Collection

'Data', once considered a by-product of a product or service, has now become a critical business asset.[140] It forms the foundation of any AI model design.[141] Collecting vast amounts of data to train AI systems is a common practice.[142] AI can analyze raw datasets and uncover patterns, correlations and enhanced insights, thereby creating value and an infinite potential for innovation.[143] However, with complex analytics technology such as AI-based ATs which process personal or sensitive data of a vulnerable group—PWDs, the privacy and data protection risks increase multifold.[144] The more data about an individual developer collects and includes in data sets, the higher the potential risks is to such data subjects.[145] Therefore, to understand these risks further, it is necessary to discuss the sources and types of data involved in AI-based ATs.

3.1.1.1 Sources of Data

In the functioning of an AI model, there are two sets of data involved—training data, used to create an AI model; and user data generated while using an AI model. Training data is an umbrella term used for training data, validation data, and testing data used during the design and development phase;[146] whereas during the deployment phase, data is generated when user interacts

---

[140] "Osler AI Series Module 2 – Data, Intellectual Property and Privacy", online: *Osler Hoskin Harcourt LLP* <http://www.osler.com/en/events/2023/osler-ai-series-module-2-data-intellectual-property-and-privacy-en>.

[141] "Why Does Training Data for AI and ML Matter?", online: <https://www.taus.net/resources/blog/why-does-training-data-for-ai-and-ml-matter>.

[142] "What Is AI Model Training & Why Is It Important? | Oracle Canada", online: <https://www.oracle.com/ca-en/artificial-intelligence/ai-model-training/>.

[143] *Supra* note 119.

[144] World Intellectual Property Organization, *WIPO Technology Trends 2021- Assistive Technology* (Geneva: WIPO, 2021) at 19.

[145] "How should we assess security and data minimisation in AI?", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/>.

[146] Telus, *The_essential_guide_to_training_data.pdf*. < https://assets.ctfassets.net/3viuren4us1n/3BsAvkXPsIYPeuJdQortBW/2c12bc7e95ae9ecea06ea84676f4460a/The_essential_guide_to_training_data.pdf>.

with AI systems.[147] Since data is required at every phase of AI systems' functioning, it is important to understand the sources of data. Generally, for an AI model, one or a combination of the following common sources provide data:

1. Data extracted from data repositories, like Common Crawl, data warehouse, and data lakehouse, form the training or testing data for AI systems.[148] These repositories have proprietary or open-source licenses that permit the use of the data.
2. AI developers enter commercial deals or contracts with data suppliers, vendors, or brokers to license access to the data under specified terms and conditions.[149] These vendors, suppliers or brokers use public records, social media content, and third-party data sharing agreements to provide a substantial amount of data.[150]
3. Primary data sources: data collected firsthand to design and develop an AI model through methods including surveys, research cohorts, observation, experiments, and interviews.[151]
4. Data generated by the device during deployment or AI system's operation phase.

For instance, under Project Understood, Google and the Canadian Down Syndrome Society collect speech sample data from people living with down syndrome and use it as training data for a speech recognition algorithm.[152] The Project Understood team seeks participants' registration through its official website and collects the voices of the qualified participants using its voice recording tool called Chit Chat.[153] Another example is the University of Waterloo's public database, which maintains 5.6 million images of the environment to train environment recognition algorithms.[154] In certain cases, AI also assists in collecting data; for instance, *Andyamo*, a French

---

[147] Daswin Silva & Damminda Alahakoon, *An Artificial Intelligence Life Cycle: From Conception to Production* (2021) 13:3 Patterns.
[148] Malcolm Katrak, "The Role of Language Prediction Models in Contractual Interpretation: The Challenges and Future Prospects of GPT-3" in *Leg Anal* (Chapman and Hall/CRC, 2022).
[149] LG, "What data is used to train an AI, where does it come from, and who owns it?", online: *Potter Clarkson* <https://www.potterclarkson.com/insights/what-data-is-used-to-train-an-ai-where-does-it-come-from-and-who-owns-it/>.
[150] Silva & Alahakoon, *supra* note 147.
[151] "Data sources that can be used in Artificial Intelligence", online: <https://www.kantify.com/insights/data-sources-that-can-be-used-in-artificial-intelligence>.
[152] *Using AI to support people with disability in the labour market: Opportunities and challenges*, by Chloé Touzet, OECD iLibrary (Paris: OECD, 2023) at 19.
[153] "Little Black Book | LBBOnline", online: <https://www.lbbonline.com/awards/immortals/entry/2983/>.
[154] *Ibid.*

start-up, uses AI to collect data related to the accessibility of public spaces and transportation systems to integrate it into GPS guidance solutions.[155] This French product aims to increase the accessibility for PWDs making it a disability-centered solution or AI-based AT.

3.1.1.2 Types of data involved in processing

The purpose of discussing the kind of data collected and processed by AI-based ATs is to highlight the level of intimate data at stake, mainly when AI-based ATs can collect data provided intentionally and unintentionally.[156] AI-based ATs assist PWDs in their everyday lives by collecting and processing personal and sensitive data.[157] The data collected by AI-based ATs could include personal information, user metrics, user feedback, and more such information.[158] For instance, voice assistant apps often collect personal data, including voice recordings, text inputs, and demographic information, to improve the functionalities of the app.[159] It also collects other data such as non-personal data; however, this thesis focuses only on data regulated under data protection laws—personal and sensitive data. Sensitive data includes genetic data, financial data, and biometric data.[160] Data protection laws of different jurisdictions even provide higher protection to sensitive data.[161] For example, the EU's GDPR prohibits processing such sensitive data or "special category of personal data", unless an exemption applies.[162]

Another type of data collected by AI-based ATs is the unintentionally disclosed data. What happens in this scenario remains uncertain. For instance, a PVI using an AI-based screen reader to read a document inadvertently discloses sensitive financial information in the background. Since the PVI cannot verify the contents of the image taken, he/she is unaware that the AT has collected

---

[155] Touzet, *supra* note 152.
[156] "AI and Its Implications for Data Privacy", online: <https://www.routledge.com/blog/article/ai-and-its-implications-for-data-privacy>.
[157] Wendy Gonzalez, "Council Post: Three Ways AI Is Improving Assistive Technology", online: *Forbes* <https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/21/three-ways-ai-is-improving-assistive-technology/>.
[158] Cat Noone, "Flawed data is putting people with disabilities at risk", (19 April 2021), online: *TechCrunch* <https://techcrunch.com/2021/04/19/flawed-data-is-putting-people-with-disabilities-at-risk/>.
[159] "Deep learning based assistive technology on audio visual speech recognition for hearing impaired - ScienceDirect", online: <https://www.sciencedirect.com/science/article/pii/S2666307422000031>.
[160] *Ibid*, art 9.
[161] "Data protection and privacy laws | Identification for Development", online: <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>.
[162] EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ, L 119/1, art 5-10.

sensitive financial (unintentional) information, which then becomes part of real-time data. This example highlights the higher vulnerability of PWDs while using AI-based ATs.[163]

AI-based ATs or AI developers create different datasets, structured or unstructured,[164] for the development and deployment phases. Even within the development phase, training, validation and testing data are separate.[165] This leads to a high volume of data transactions to improve results or optimize the AI-based AT. The main concerns with this data collection are potential misuse or unauthorized access. Therefore, data processors must consider generalization of data by removing representative data wherever possible and ensure that the data measures what it initially intended to measure. Parenthetically, PWDs should be a part of the training data to ensure their requirements and experiences form part of the evolving learning of AI models. For instance, a facial recognition AT has custody and control over big face datasets to detect faces from millions of faces. AI developers can use these as datasets for an AI model's development, and when the users (here, PWDs) use the app, it leads to real-time data collection. Sometimes these AI models use this real-time data in the deployment phase to improve or update the AI model.[166]

---

[163] Another form of data collected is the data of people around PWDs or bystanders (secondary data subjects) when PWDs use AI-based ATs. Such users do not directly use the app but face severe privacy risks. For instance, AI-powered hearing aids process the voice of a third person with whom the PWD user is conversing as a part of real-time data for the AI to function. The AT converts the speech into text using such data. Another example is when image or facial recognition-based AT captures images of bystanders or people interacting with the PWD user. These examples raise two questions—Are such secondary data subjects aware of the collection of their data?, and Who is responsible for notifying secondary data subjects of the processing of their data, is it the PWD user or the data processor? If secondary data subjects' do not feel secure around ATs, this might lead to an increase in contempt or resistance towards ATs; Taslima Akter et al, "Shared Privacy Concerns of the Visually Impaired and Sighted Bystanders with Camera-Based Assistive Technologies" (2022) 15:2 ACM Trans Access Comput 11:1.

[163] Ellysse Dick, "How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces", (2020) online: <https://itif.org/publications/2020/12/14/how-address-privacy-questions-raised-expansion-augmented-reality-public/>.

[163] "Interview with Kave Noori and Marine Uldry from the European Disability Forum: 'Nothing about us without us', including AI - EAISF", (31 October 2023), online: *EAISF* - <https://europeanaifund.org/newspublications/interview-with-kave-noori-and-marine-uldry-from-the-european-disability-forum-nothing-about-us-without-us-including-ai/>.

[164] Deloitte, "The AI opportunity in sourcing and procurement - Opportunities in the market today" online:< https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-omniaai-supplychain-pov-aoda.pdf>.

[165] Gonzalez, *supra* note 29.

[166] "(1) Real-time Model Deployment and Inference | LinkedIn", online: <https://www.linkedin.com/pulse/real-time-model-deployment-inference-brindha-jeyaraman-qzjpc/>.

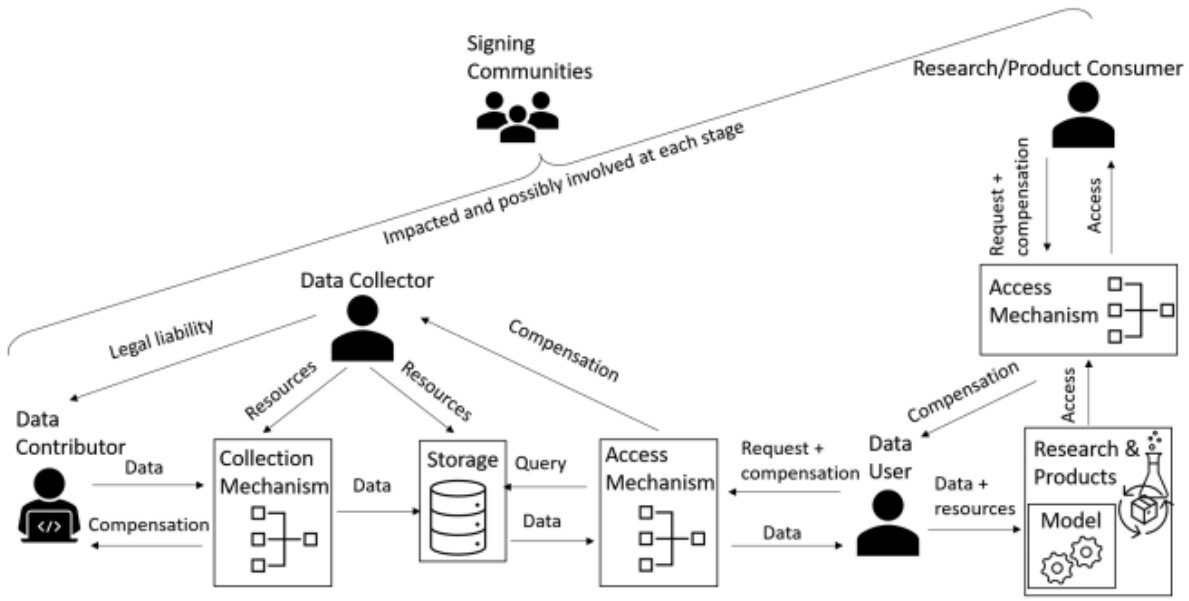

Fig. 1. Diagram of the parties who may participate in sign language dataset creation and usage for AI applications and research and thereby claim some form of ownership. Data format and content may vary throughout the flow. Compensation can take different forms and can be nothing. The data collection may be subcontracted to a third party; in that case, another entity would appear in the flow. Signing communities, and in particular deaf communities, are impacted by the collection and usage process, and may be involved at any stage.

Figure 4: Diagram of parties or potential stakeholders involved in the dataset creation and usage of an AI-based sign language AT[167]

To conclude, developers should consider certain questions in the case of this intimate data collection:

> What information will be collected by emerging technologies, and to whom will it be disclosed? Are users with disabilities adequately informed about the private, sensitive data that they are sharing when using emerging technologies? If AI is used to infer personal details that were not intentionally shared by a user, what are the implications?[168]

[167] Danielle Bragg et al, "The FATE Landscape of Sign Language AI Datasets: An Interdisciplinary Perspective" (2021) 14:2 ACM Trans Access Computing 1–45.
[168] *Supra* note 4 at 27.

3.1.2 Data Storage, Profiling and Sharing

AI-based AT companies or developers collect vast amounts of data from their users, here PWDs, knowingly or unknowingly, and further subject it to storing, sharing, profiling or other processing steps. Organizations often store this collected data on the cloud or remote servers or connected to the internet or other devices.[169] These storage techniques often create potential security and potential data protection issues, thereby raising potential privacy risks.

3.1.2.1 Data Storage and Sharing

In data collection, questions about storing and sharing that data with third parties arise. Some of those questions are—Where is the data stored? Is cloud computing or edge computing being used? If data processors use cloud computing, how many copies of the data exist on the cloud? Who has access to the stored data? Are there any third parties involved in the processing of personal data? Is the personal data collected shared with any third party?

In the technological space, many tech companies, including AI-based AT companies, store their data on the cloud.[170] An important reason is that cloud computing assists tech corporations not operating and owning networks and computers to store data in a suitable environment.[171] Since the data is often kept off-site on external servers and maintained by third parties, it could raise potential privacy and security risks.[172] Security and privacy go hand-in-hand; thus, a security breach often leads to a violation of the legal data protection framework or privacy rights of users.[173] The risk depends on factors such as the service provider used, the level of security offered by that service provider, and if there is any involvement of third parties. In the context of the storage or data retention period, companies often have less incentive to delete or erase the data from the cloud because of the affordable storage cost.[174] They often find alternative ways to use the collected

---

[169] "Cloud computing for disability storage: Empowering Accessibility: How Cloud Computing Supports Disability Storage Solutions", online: *FasterCapital* <https://fastercapital.com/content/Cloud-computing-for-disability-storage--Empowering-Accessibility--How-Cloud-Computing-Supports-Disability-Storage-Solutions.html>.
[170] Pushpa Singh et al, "Artificial Intelligence for Smart Data Storage in Cloud-Based IoT" in Fadi Al-Turjman et al, eds, *Transform Manag AI Big-Data IoT* (Cham: Springer International Publishing, 2022) 1.
[171] *Ibid*; Office of the Privacy Commissioner of Canada, "Cloud computing and privacy", (4 October 2011), online: <https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/cloud-computing/02_05_d_51_cc/> Last Modified: 2011-10-04..
[172] Sina Ahmadi, "Security And Privacy Challenges in Cloud-Based Data Warehousing: A Comprehensive Review" (2023) 11:6 Int Jour of Comp Sci Trends and Tech (IJCST) 17–27.
[173] *Ibid*.
[174] Canada, *supra* note 171.

data.[175] Thus, exceeding the storage period encroaches on the effect of purpose limitations and use limitations data protection principles (discussed later).

AI requires vast storage and has led to an increased demand for cloud storage or computing,[176] thus it becomes crucial to look at specific potential privacy issues that arise when AI systems, including AI-based ATs, use cloud computing:

- The first is the data confidentiality issue. Whenever data processors outsource or store externally personal or sensitive data, they must ensure that such data is out of reach of unauthorized parties.[177] Maintaining data confidentiality allows data controllers, processors and users (here, PWDs) to trust the cloud service provider.[178]
- The second is the data loss or data breach issue, which is a combined security and privacy concern. There have been data breaches of the personal information of PWDs[179] or children with disabilities[180] in the past, creating devastating aftereffects.
- The third is the jurisdictional or geographical data storage issue. In cloud computing, issues like the distribution of data over different geographical locations and remote storage of data raise questions surrounding applicable data protection law in such a multi-jurisdictional arrangement.[181]
- The fourth is the concern of misuse of the data streams[182] created or the personal data stored. The cloud model potentially creates a vast collection of data and provides cloud

---

[175] *Ibid.*
[176] Afzal Badshah, "Issues and challenges in Cloud Storage | Intuition | Medium" (28 September 2022), online: <https://medium.com/intuition/issues-and-challenges-in-cloud-storage-d3c7b7826dd0>.
[177] Johndavid Kerr & Kwok Teng, "Cloud computing: legal and privacy issues" Journal of Legal Issues and Cases in Business at 6.
[178] Shekhar Kausalye & Sanjeev Sharma, "Data Confidentiality in Cloud Storage. A Survey" in (2021), online: < https://www.researchgate.net/publication/356756446_Data_Confidentiality_in_Cloud_Storage_A_Survey>.
[179] "Justice Department investigated for data loss", *CBC News* (25 February 2013), online: <https://www.cbc.ca/news/politics/justice-department-investigated-for-data-loss-1.1319192>.
[180] "Unprecedented' breach involving personal information of 8,900 kids could have been avoided: ombudsman", *CBC News* (29 April 2021), online: <https://www.cbc.ca/news/canada/manitoba/privacy-breach-childrens-disability-services-ombudsman-1.6007824>.
[181] Reeta Sony, Kan Sri & D Bhukya, "Data Protection and Cloud Computing: a Jurisdictional Aspect" (2013) Право Журнал Высшей Школы Экономики 81.
[182] Data streaming can be understood as continuous and high-speed transfer of data for processing into analytics and other outputs. [Source: "What is Streaming Data? - Streaming Data Explained - AWS", online: Amaz Web Serv Inc <https://aws.amazon.com/what-is/streaming-data/>].

service providers or infomediary access to such data.[183] Since AI-based ATs have access to data as intimate as a single click on technological devices or behavioral patterns of the user, storing this data in the cloud poses the potential risk of this intimate data being used by cloud infomediaries beyond the purpose mentioned while taking consent.[184] The service provider could inappropriately manipulate, mine, and access the data stored, and in this case, one must differentiate between acts done as a processor and acts beyond the role of a processor.[185]

- The fifth is the risk of the data not being entirely deleted from the servers or cloud storage on a data subject's request or upon fulfillment of the purpose. Especially with AI systems, incomplete deletion of data is an ongoing concern.[186] Thus, this lack of transparency and failure of complete deletion can raise potential privacy risks.
- Lastly, sharing computational resources among various tenants can create multi-tenancy security issues.[187] These resources include storage space, the same logical or physical platform at the cloud provider's premise or applications services.[188] Attackers can attack multiple tenants simultaneously, and the data of PWDs may become collateral damage of an attack targeted at a co-tenant.

Breach or misuse of data in the case of PWDs becomes an alarming concern because of the historical and systematic oppression that PWDs have to face. Chapter three discusses the reasons for exacerbated vulnerability of PWDs to potential privacy risks.

To illustrate the risks associated with cloud computing, Widex's *SoundSense Learn*, an AI-powered hearing aid, uses the input data provided by its users (here, people with hearing impairment) worldwide to provide a personalized hearing experience.[189] It then shares the

---

[183] Reaching for the Cloud(s): "Privacy Issues related to Cloud Computing" (March 2010), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/media/1723/cc_201003_e.pdf>.
[184] "Competition and Privacy in Web 2.0 and the Cloud by Randal C. Picker :: SSRN", online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985>.
[185] Supra "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing".
[186] Antonio A. Ginart, et al. "Making AI Forget You: Data Deletion in Machine Learning." (2019) *ArXiv* abs/1907.05012, online: < https://www.semanticscholar.org/reader/6a2efd7e59ec314e29850e744be05eb65ccdfbc4>.
[187] "7 Privacy Challenges in Cloud Computing - GeeksforGeeks", online: <https://www.geeksforgeeks.org/7-privacy-challenges-in-cloud-computing/>.
[188] *Ibid.*
[189] World Intellectual Property Organization, *supra* note 53; *ibid.*

anonymized user input data collected from users worldwide with a cloud-based AI system. This cloud storage assists in creating personalized settings for every user based on content, intent and context.[190] However, even after anonymization of data in the cloud, there is always the risk of re-identification or de-anonymization.[191] In the case of AI-based ATs, which collect personal or sensitive data, the chances of re-identification or cross-referencing are high[192] because AI has the ability to identify unanticipated patterns and draw connections. As a countermeasure, some AI-based AT companies use edge computing (processing of data near the collection location).[193] Examples of such technologies are Okeenea's AI-based guiding solution and Echo. They process the collected data locally on devices, and the aim is to not share personal data with cloud-based servers.[194]

Sharing personal or sensitive data with third parties is a major concern for AI-based ATs. Data processors or controllers take the defense that data sharing is a result of data subject's consent, but as I will discuss in the next chapter, critics often question if this is informed consent. Further, in literal terms, the concept of "informed consent" itself is hard to achieve. Studies have shown that users are often unaware of or fail to understand the privacy policies or terms and conditions, filled with legalese.[195] Additionally, the concept of indirect forced consent is becoming prominent with technologies like AI-based ATs, which provide personalized suggestions. For instance, to fully access an environment recognition app, the user (in this case, PVI) has to provide consent to access its location, habits, routines and other personal data. In relation to providing consent for the processing of data, specific questions arise—Does the user consent to the unfettered sharing of this personal data?[196] Does the user providing consent to tracking of personal data reasonably expect the service provider to share it? Does that expectation amount to implied consent?[197]

---

[190] *Ibid*.
[191] "Re-Identification of 'Anonymized' Data", (12 April 2017), online: *Georget Law Technol Rev* <https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/>.
[192] Meredith Ringel Morris, "AI and accessibility" (2020) 63:6 Commun ACM 35–37.
[193] Touzet, *supra* note 152; *ibid*. at 49.
[194] *Ibid*.
[195] Jana Korunovska, Bernadette Kamleitner & Sarah Spiekermann, "The Challenges and Impact of Privacy Policy Comprehension" (delivered at the Twenty-Eigth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco, 2020) online: < https://arxiv.org/abs/2005.08967 >.
[196] Theodore F. Claypoole, eds, *The law of artificial intelligence and smart machines: understanding A.I. and the legal impact* (Chicago, Illinois: American Bar Association, Business Law Section, 2019) at 428.
[197] *Ibid*.

Thus, before proceeding with such technological developments, we as a society must consider if we even want to proceed with this level of intrusion into PWDs' lives by processing data using AI.

3.1.2.2 Creation of user profiles by AI

The vast amount of data collected by AI systems can reveal enough about an individual to create a dedicated user profile.[198] In the case of PWDs, especially with rare diseases or smaller populations of PWDs, the risk of being identified in case of aggregation of data is high, even if the data is not directly identifiable.[199]

AI-based ATs, as a part of their purpose and function, use data to provide personalized experience or assistance.[200] They use AI systems using ML, pattern recognition and analysis to understand the activities, routines, interests, preferences, reactions, and behavioral patterns, basically profiling the data of PWDs to provide customized results to every user.[201] For instance, a user can adjust AI-powered smart glasses based his/her degree of sight loss or granted access to certain personalized features.[202] The usage of AI models in ATs can result in identifiable personal data for individuals since it has the power to draw inferences and recognize patterns. As another example, smart AI-based ATs assist with medical conditions, shopping, tracking health information, food delivery, dispensing medicine, or record-keeping.[203] This information, in isolation, might be of limited use; however, once aggregated and analyzed, it could create a detailed profile of PWDs with intimate information about their lifestyle, medical condition, personal characteristics, and more.[204] There is a potential risk of exploitation of these detailed profiles for, *inter alia*, unauthorized surveillance, manipulation or decreasing insurance coverage based on medical conditions, tailored advertisements, discrimination, limiting opportunities and growth, and creating bias. Thus, the potential for misuse of user profiling data and for exploitation

---

[198] Sune Holm, "Should People Have a Right Not to Be Subjected to AI Profiling based on Publicly Available Data? A Comment on Ploug" (2023) 36:2 Philosophy Technology 38.
[199] Morris, *supra* note 195.
[200] World Intellectual Property Organization, *supra* note 53 at 114.
[201] *Ibid* at 54.
[202] "Smart Glasses For The Visually Impaired: Envisioning Accessibility", (24 April 2024), online: <https://top5accessibility.com/blog/smart-glasses-for-the-visually-impaired-technological-advancements-in-accessibility/>.
[203] *Ibid*.
[204]World Intellectual Property Organization, *supra* note 53 at 55.

of such profiles without data subjects' informed consent, especially for PWDs, who are often vulnerable to potential exploitation,[205] is enormous.

3.1.3 Lawfulness and Fairness

Lawful, fair and transparent, one of the principles under the FIPPs, is crucial for PWDs using AI to avoid bias and discrimination.[206] This principle requires compliance with two features—reasonable expectation and subject to independent oversight.[207] Different data protection laws, including Canada's private sector federal data protection law—*Personal Information Protection and Electronic Documents Act* (PIPEDA), require "reasonable" processing of data.[208] As per PIPEDA, to check reasonableness one must ask if a person of ordinary prudence would consider the collection or line of query reasonable is essential.[209] AI-based ATs, devices used in everyday lives and recording personal or sensitive data, often subject their users (here, PWDs) to surveillance.[210] For instance, Google Assistant was found to be listening to its users' activity (surveillance) even when there was no expectation of data collection.[211] In this case, users had no "reasonable expectation" of being heard by the device. This is merely one example of the breach that was exposed. Similar to Google Assistant, some AI-based ATs heavily rely on the use of voice or image recognition, which increases the potential risk of being heard or recorded without expectation for a purpose beyond what PWDs consented to. Therefore, the risk of a potential privacy breach or breach of the reasonable expectation principle is undoubtedly high in such AI-based ATs.

---

[205] Francisco Jose Bariffi, "Artificial Intelligence, Huamn Rights and Disability" (2021) 26:2 Pensar Revista de Ciencias Juridicas 1.
[206] OECD, *supra* note 128.
[207] *Supra* note 126 at 125.
[208] Personal Information Protection and Electronic Documents Act SC 2000, c 5, s. 5(3).
[209] Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)", (24 May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/> Last Modified: 2018-05-24.
[210] Maurício Pasetto de Freitas et al, "Artificial Intelligence of Things Applied to Assistive Technology: A Systematic Literature Review" (2022) 22:21 Sensors 8531.
[211] "Google tells Parliament IT Panel that its employees listen to some Ok Google queries", online: <https://www.indiatoday.in/technology/news/story/google-tells-parliament-it-panel-that-its-employees-listen-to-some-okay-google-queries-1820975-2021-06-30>; "CNBC Google Conversational Actions Update: June 2023 – CNBC Help Center", online: <https://cnbc.zendesk.com/hc/en-us/articles/15754642300315-CNBC-Google-Conversational-Actions-Update-June-2023>.

Complying with the lawful principle in the context of AI can be complex because a lawful ground under the law for processing the data might be relevant for one phase of AI processing and could not be valid for another phase.[212] For instance, the ground of 'performance of the contract' could be appropriate for AI processing targeted at providing financial service advice. However, it will not be a relevant ground for developing an AI model.[213] In the context of AI-based ATs, the grounds for "vital interest of data subject" can be valid in case of a medical emergency, i.e., during the deployment phase. However, this ground could not be considered valid during the development phase.

The fairness principle requires that the data processor processes personal data in a manner that is within the reasonable expectations of data subjects.[214] The intent is to ensure that processing does not adversely or unjustifiably impact data subjects' interests.[215] One shall conduct the balancing and proportionality test to comply with this principle.[216] The test checks and ensures sufficient mitigation of the risk and if processing is crucial. As highlighted in the literature, the fairness principle has two components in the AI context—statistical accuracy and non-discrimination.[217] The sub-section below highlights the challenges faced in obtaining statistical accuracy. In the context of the second component (i.e., non-discrimination), the developers' or the training data's biases and discriminatory beliefs could translate into the AI models.[218] For example, AI-based smart assistants often fail to understand the voice of people with speech impairment.[219] The main reason for this failure is the use of average speech while ATs' training, creating a bias towards average speech.[220]

---

[212] Quintavalla & Temperman, *supra* note 126 at 125.
[213] UK Information Commissioner's Office (ICO), 'Guidance on AI and Data Protection' (ICO, 20 July 2020).
[214] Gianclaudio Malgieri, "The Concept of Fairness in the GDPR" (Paper delivered at the Conference on Fairness, Accountability, and Transparency, 2020) [unpublished] online: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517264>.
[215] *Ibid*.
[216] Quintavalla & Temperman, *supra* note 126 at 126.
[217] "How do we ensure lawfulness in AI?", (7 February 2024), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/>.
[218] Cathryn Copper, "Research guides: Artificial Intelligence for Image Research: Datasets, Bias, Discrimination", online: <https://guides.library.utoronto.ca/c.php?g=735513&p=5297043>; "AI language models show bias against people with disabilities, study finds | Penn State University", online: <https://www.psu.edu/news/information-sciences-and-technology/story/ai-language-models-show-bias-against-people-disabilities/>.
[219] Quintavalla & Temperman, *supra* note 126 at 253.
[220] *Ibid*.

3.1.4 Lack of transparency

The application of the transparency principle becomes crucial in the case of the collection of different kinds of data, from personal to sensitive data, by AI-based ATs. This principle provides data subjects with the right to access or the "right to be informed" about the processing of their personal data.[221] Data controllers or processors are required to inform data subjects, *inter alia*, in an accessible and understandable manner of the kind of personal data collected, the purpose of processing the personal data, the retention period for that data, associated risks, safeguards adopted related to the processing of data collected, or any other information sought by data subjects.[222] The purpose is to increase accountability on the part of data controllers and processors.[223] The current data protection laws around the globe, including the two relevant laws for this research, the EU's GDPR[224] and Canada's PIPEDA[225] provide this right to data subjects.

In addition to data protection principles, transparency is a crucial principle to ensure the responsible use of AI. Therefore, "Transparency and Explainability" is one of the AI Principles released by the OECD.[226] As per the explanation by the OECD, transparency has different meanings. Firstly, AI actors (data processors or controllers) need to be transparent about the use of AI systems. Secondly, AI actors need to inform people about the general functioning of AI systems, in this context, the cycle of data processing. Thirdly, AI actors need to enable individuals affected by AI systems to understand and challenge the outcomes.[227] The increased focus on

---

[221] "How do we ensure transparency in AI?", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-transparency-in-ai/>.

[222] Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 3 – Consent", (8 January 2018), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/> Last Modified: 2020-08-13.

[223] Quintavalla & Temperman, *supra* note 126, ch 8 at 127.

[224] Supra note 32, Art 13-15.

[225] PIPEDA, Supra note 208, ss 4.8-4.9

[226] "Transparency and explainability (OECD AI Principle) - OECD.AI", online: <https://oecd.ai/en/dashboards/ai-principles/P7>,"

[227] *Ibid*. Principle 1.3. "AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information appropriate to the context, and consistent with the state of art:

- to foster a general understanding of AI systems,
- to make stakeholders aware of their interactions with AI systems, including in the workplace,
- to enable those affected by an AI system to understand the outcome, and,
- to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."

incorporating transparency rights in data protection and AI regulations highlights the importance of improving data subjects' understanding of their rights to control their data usage.[228]

Transparency in the context of AI-based ATs would mean providing information to data subjects (here PWDs) about the decision-making functionalities of the AI model used in ATs and processing of their personal or sensitive data. For instance, a PWD using an automated lip-reading technology should be, among other things, informed of the facial recognition technology used, the collection of data and its processing. The application of this principle in such AI systems is complex for two reasons. First, the right holders closely guard the functioning of an algorithm as it is "proprietary information" leading to incomplete disclosure of information about the algorithm.[229] The second and most crucial issue is the black box phenomenon—the inability of even the AI system developers to understand its decision-making process.[230] The black box phenomenon is a result of deep neural networks involved in complex AI systems. Neural networks form a hidden layer of artificial neurons between the input and output layers of an AI model that mimics the functioning of a human neuro system. While highlighting the difficulty of being transparent in the case of AI, Professor Paul Ohm rightly stated that "when a program 'thrives on surprising correlations and produces inferences and predictions that defy human understanding.....[h]ow can you provide notice about the unpredictable and unexplainable?"[231] Non-transparency in AI-based ATs where the data collected is either personal or sensitive raises the potential risk of misuse of the data manifold. This can be dangerous especially because the data can reveal information about PWDs, a vulnerable group which is prone to discrimination and bias in AI systems. Moreover, auditing these systems and ensuring compliance with data protection laws becomes extremely difficult due to the lack of transparency. This non-transparency also raises correlated issues like fairness and accountability when the AI system's functioning is opaque.

---

[228] Supra note 221.
[229] "Working Paper on Privacy and Artificial Intelligence" (2018) International Working Group on Data Protection in Telecommunications, Working Paper, online: *<2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf>*.
[230] *Ibid* [also read: "Creators know how their systems work theoretically (they implement methods such as gradient descent that should optimize the way the system work), but in practice the huge number of parameters and their automated tuning based on the statistical properties of the data make it hard to be able to precisely explain why such a decision was made, why such a parameter is so high while another is so low, etc."].
[231] "Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice", The Centre for Information Policy Leadership at Hunton Andrews Kurth LLP (Feb. 13, 2018) online:<cipl_ai_project_description.pdf>.

Additionally, it is difficult to comply with other principles like data minimization or the right to be informed, along with transparency, as they might be incompatible with each other.[232] For example, if the developer modifies the training data and removes any contact information to minimize personal data from the data set, it would be difficult to communicate information or deliver notice to those data subjects.[233] Furthermore, the concept of informed consent becomes less meaningful if there is a lack of clarity about how the AI system operates. All these associated risks combined raise concerns about the personal and sensitive data of PWDs and the current legal accountability framework,[234] which is not keeping pace with the speedy advancement of AI systems.

3.1.5 Purpose limitation and specification

In the case of personal or sensitive data of PWDs, a group that is prone to misuse of data, bias and discrimination[235], the lack of purpose specification, unpredictability and unforeseeability can prove to be detrimental to them. The principle of purpose limitation requires the data controller and processor to process the collected data only for the purpose mentioned in the collection notice during the data collection phase.[236] Additionally, the law can permit the usage of data for any secondary "reasonably expected" purpose.[237] This principle can be a challenge in AI models because of the vast amount of data required both during the development and deployment phases and AI's ability to derive meaning beyond the data collection purpose.[238] With AI-based ATs or any AI system in general, there is a requirement for different sets of data, and the purpose served by these data at different stages also varies. Developers use the data in the development phase to design, train and improve the AI system, whereas they use the data during the deployment phase for the functioning of the AI system.[239] For instance, while using an object detection app, PVIs

---

[232] Quintavalla & Temperman, *supra* note 126 at 127.
[233] Supra note 229.
[234] Reuben Binns, "Algorithmic Accountability and Public Reason" (2018) 31 Philosophy & Technology 543-56.
[235] "Why privacy is particularly crucial for people with disabilities", online: *Eur Digit Rights EDRi* <https://edri.org/our-work/why-privacy-is-particularly-crucial-for-people-with-disabilities/>.
[236] Kamrul Faisal, "Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective" (2023) 28:1 Commun Law Policy 67–97.
[237] "Principle (b): Purpose limitation", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/>.
[238] Rainer Mühlhoff & Hannah Ruschemeier, *Updating Purpose Limitation for AI: A normative approach from law and philosophy* (Rochester, NY, 2024).
[239] Quintavalla & Temperman, *supra* note 126 at 128.

might consent to the use of their data for improving the image recognition model. However, this does not permit using such data to train AI models with PVIs' data. This example raises the question of what an appropriate secondary purpose is.

Another issue with AI systems is to meet the requirement of purpose specification while collecting the data. As noted in a report "it is not possible to predict what the algorithm will learn….. Its purpose may also be changed as the machine learns and develops."[240] Most of the time, even the developers or programmers cannot fully predict the purpose or use of data.[241] The purpose limitation and use specification principles require the purpose clause in data collection notices to be precise and not vague. Therefore, for AI systems to function, data controllers must re-obtain consent if the use does not fall under a legitimate secondary purpose.[242] Re-obtaining consent from PWDs can be often challenging, especially in the case of people with intellectual and developmental disabilities (PWIDD). However, controllers and processors can potentially use for research or statistical purposes, which are exceptions for purpose specification in various jurisdictions.[243] Also, restrictions on purpose specification and limitation raise concerns about hindering innovation.[244] Hindering innovation is problematic for a technology like AI-based ATs, which are changing lives.

3.1.6 Data Minimization and Storage Limitation

According to the data minimization principle, data controllers and processors shall process personal data shall for the purpose and to the extent specified in the data collection (usually privacy policy) notice.[245] Additionally, the objective should be to minimize the amount of data collected

---

[240] Artificial Intelligence and Privacy, Datatilsynet (Norwegian Data Protection Authority) at page 4 (January 2018), <*ai-and-privacy.pdf*>. Christopher Kuner et al, "Expanding the artificial intelligence-data protection debate" (2018) 8:4 Int Data Priv Law 289–292.

[241] Supra note 231.

[242] Quintavalla & Temperman, *supra* note 126.

[243] "The Consent Exception for Research Purposes", online: *Éloïse Gratton* <https://www.eloisegratton.com/blog/2016/06/03/the-consent-exception-for-research-purposes/>; PIPEDA, *Supra* note 208, s. 7(2)(c).

[244] Maximilian Von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation* (Nomos Verlagsgesellschaft mbH & Co. KG, 2018).

[245] "Purpose limitation, data minimisation and storage limitation", (19 May 2023), online: <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/purpose-limitation-data-minimisation-and-storage-limitation/>.

wherever possible.[246] Taking precautions and limiting the data from the design phase can help in minimization of data.[247] However, with AI, data minimization could be a challenge because AI models require vast amounts of data. AI models, especially the commonly used ML models and LLM require loads of data from development to deployment.[248] It is often advisable to have more training data because it assists in efficient training and improves the accuracy of the model.[249]

Fulfilling the data minimization principle becomes challenging with a technology that thrives on data maximization. Especially with AI-based ATs, which extensively involve processing personal and sensitive data, the inability to minimize such data can be problematic. Algorithm developers often adopt techniques like anonymization, pseudonymization or data encryption to minimize personal data and preserve the identity of data subjects.[250] However, with a vast amount of data and AI's ability to infer patterns and build correlations, AI-based ATs could identify patterns and correlations in personal data and indirectly be successful at identifying an individual's personal data.[251] So, even if AI-based ATs claim to be working with anonymized or de-identified data of PWDs, there have been instances in the past where AI models have been successful in identifying "anonymized" users by using a small amounts of data.[252] In the case of PWDs, especially people with rare diseases, this can increase the risk that this data is misused and leads to bias and discrimination. One such case was of an ML system identifying the user 81% of the time by using merely three records in the data processor's data set.[253] In another example, an AI (ML) system identified anonymized users with an accuracy rate of above 94% using only 100 seconds of motion data (i.e. FRT/VR data).[254] These examples are testaments to AI's ability to extract personal information or identify an individual even from de-identified or anonymized or

---

[246] "OECD Legal Instruments", online: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.
[247] *Supra* note 145.
[248] P Mattson et al, "MLPerf: An Industry Standard Benchmark Suite for Machine Learning Performance" (2020) 40:2 IEEE Micro 8–16.
[249] *Supra* note 26 at 4.
[250] Stanford Law Review & tribe, "Privacy in the Age of Big Data", (2 February 2012), online: *Stanford Law Rev* <https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/>.
[251] Morris, *supra* note 192.
[252] Nicholas Carlini et. al.,"The secret sharer | Proceedings of the 28th USENIX Conference on Security Symposium", online: <https://dl.acm.org/doi/10.5555/3361338.3361358>.
[253] "You're very easy to track down, even when your data has been anonymized", online: *MIT Technol Rev* <https://www.technologyreview.com/2019/07/23/134090/youre-very-easy-to-track-down-even-when-your-data-has-been-anonymized/>.
[254] Quintavalla & Temperman, *supra* note 90, ch8 at 130.

small amounts of data. Therefore, in the case of contemporary AI models like ML and LLMs, traditional forms of technical privacy protection or data sanitation, including de-identification, anonymization, or differential privacy, often fail to provide privacy protection.[255]

As discussed in earlier subsections, other concerns with failure to comply with data minimization in AI-based ATs are user profiling, data leaks from cloud servers, and misuse of that leaked data or user profiles generated. Lastly, as discussed in the "data collection" subsection above, it is crucial to note that with the involvement of AI in ATs, along with direct data collection, users (here, PWDs) often unconsciously or unintentionally provide personal data to these technologies. It also collects data of secondary data subjects. Thus, failure to comply with the data minimization principle puts vast amounts of data at risk. A solution to this is data minimization during deployment stage.[256] Organizations can minimize data by "converting raw personal data into abstract numbers", "hosting the model on the device used for collection to avoid communicating some of the subject's data to an external host", or "only using the features of data relevant to the purpose of the model".[257]

The second principle, directly linked with data minimization, is to focus on storage limitation. It requires storing the data only for the necessary processing period and ensuring its erasure upon fulfillment of its purpose.[258] In AI systems, this means deleting the data upon completion of the development phase or any intermediate files once they become irrelevant.[259] In the *Del Giudice v. Thompson* case,[260] the defendant (One Capital) retained, stored, and migrated the data for longer than necessary. This prolonged retention increased the risk and led to a data breach and misuse of data. Similarly, with AI-based AT, storing or retaining data of PWDs beyond the necessary period (based on the collection purpose) by businesses or third parties involved heightens the risk of data breach and misuse of that data. Moreover, there is a risk of disclosing of

---

[255] Insights Team, "Forbes Insights: Rethinking Privacy For The AI Era", online: *Forbes* <https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/>.
[256] Quintavalla & Temperman, *supra* note 126.
[257] *Ibid* at 130.
[258] "Principle (e): Storage limitation", (4 August 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/>.
[259] *Supra* note 145.
[260] *Del Giudice v. Thompson* 2021 ONSC 5379.

personal information contained in one data set if coupled with other data sets.[261] Therefore, it is necessary to limit the collection and storage of personal data collected of PWDs by AI-based ATs. Furthermore, AI developers cannot defend themselves from minimizing data usage by taking the defence that the data might be helpful for future prediction purposes.

Thus, data controllers and developers must maintain a balance between achieving the data minimization and storage limitation target and maintaining the effectiveness of the AI model.

3.1.7 Accuracy or Data quality in AI models

The principle of accuracy holds different meanings in the data protection and AI sphere.[262] In data protection, it provides data subjects with the right to correction or rectification, or request deletion of their personal data collected.[263] The purpose of this principle is to keep the data updated, free from errors and relevant for the collection purpose.[264] Non-compliance with the accuracy principle would lead to a violation of data protection law. However, in the context of AI, this principle means statistical accuracy. It refers to the accuracy with which the AI model can correctly label test data based on its training using the training data.[265] Lack of statistical accuracy creates AI risks like bias and discrimination.

In AI-based ATs or any AI system, exercising the right to correction or rectification to ensure accuracy in personal data could impact the functioning of the AI model.[266] Compliance with deletion requests could negatively impact the outcomes or accuracy.[267] For instance, if data subjects request erasure of their data during the training or development phase of the AI model, it can hinder the model's statistical accuracy, worsen disparate outcomes, or impact the principle of fairness.[268] The principle of accuracy could apply to the input, output or even intermediate data.

---

[261] Kuner et al, *supra* note 240.
[262] "What do we need to know about accuracy and statistical accuracy?", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-do-we-need-to-know-about-accuracy-and-statistical-accuracy/>.
[263] "Principle (d): Accuracy", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/>.
[264] "OECD Privacy Principles", online: <http://oecdprivacy.org/>.
[265] *Supra* note 262.
[266] "Proxy Discrimination in Artificial Intelligence: What We Know and What We Should Be Concerned About | Chaire de recherche du Canada sur la culture collaborative en droit et politiques de la santé", online: <https://www.chairesante.ca/en/articles/2024/proxy-discrimination-in-artificial-intelligence-what-we-know-and-what-we-should-be-concerned-about/>.
[267] *Ibid.*
[268] Quintavalla & Temperman, *supra* note 126 at 131.

With neural network functioning, it would be a challenge to meet erasure requests since programmers are sometimes unaware of the AI model's functioning between input and output layers.[269] To illustrate, if data subjects (here PVI) while using an image recognition software (AI-based AT) exercise the right to erasure, it could have effects, *inter alia*, on performance, fairness and bias components of the model. The right to rectification might not affect an individual during the training phase but it could affect the output or deployment stage of the AI model.[270] Lastly, it is crucial to note that the exercise of the accuracy principle affects other data protection principles, including fairness. On a side note, data minimization can be counterproductive for statistical accuracy. Therefore, it is crucial to maintain a balance between the two.

3.1.8 Security, integrity, and confidentiality in AI

For PWDs using AI-based ATs, security breaches can be alarming as they could also affect privacy rights. Thus, an AI-based AT susceptible to hacking or cyberattacks can, in turn, lead to privacy breaches or misuse of PWDs' personal data. As per the FIPPs issued by the OECD, it is a necessary requirement to maintain security, integrity, and confidentiality while processing data.[271] The requirement includes non-disclosure of data to third parties and placing safety measures to avoid data security breaches.[272] Failure to protect the data processor or controller's data security, integrity and confidentiality, triggers the requirement of notification of breach to data subjects. This notification of breach is a requirement under different data protection laws, including the EU's GDPR[273] and Canada's PIPEDA[274].

A significant concern with AI-based ATs or any AI model is the involvement of external forces. Development and deployment of most AI models using externally sourced codes raises potential security concerns. Using an external source code requires auditing the security of both—

---

[269] "Understanding deep learning through neuron deletion", (21 March 2018), online: *Google Deep* <https://deepmind.google/discover/blog/understanding-deep-learning-through-neuron-deletion/>.
[270] "Enabling access, erasure, and rectification rights in AI systems | Information Commissioner's Office", online: <https://www.wired-gov.net/wg/news.nsf/articles/Enabling+access+erasure+and+rectification+rights+in+AI+systems+16102019132000?open>.
[271] OECD, *supra* note 128.
[272] "Principle (f): Integrity and confidentiality (security)", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/integrity-and-confidentiality-security/>.
[273] GDPR, Supra note *161*, art. 33-34
[274] PIPEDA, Supra note 85, s 10.1

the AI developed in-house and the external source code used.[275] For security concerns when using cloud services, two points require attention—first, the potential security risk when transmitting the data between the device and the cloud servers, and second, when the data is already in the cloud.[276] Further, data processors should protect the data from intrusion and its security, in the backup and recovery stages.[277] Security risks are a vast area of study and are outside the scope of this thesis; however, it is worth noting that at times a security breach also results in a privacy breach. Therefore, developers must focus on both equally.

3.1.9 Accountability

For the accountability principle in the case of AI-based ATs, the data controllers or processors need to look at data protection risks and AI risks. First is the data protection accountability principle described in the next paragraph, which focuses on privacy and data protection concerns. Second is the organizational accountability principle for AI, which deals with AI risks, including bias, inaccuracy, and discrimination. As highlighted throughout this chapter and will be further elaborated in the next chapters, when dealing with personal and sensitive data of PWDs, data controllers must be extra cautious because of the increased vulnerability of PWDs to privacy concerns.

The accountability principle is the umbrella or 'meta-principle', which puts the onus on the data processor and controller to comply with all other principles.[278] Data protection laws around the world, including GDPR[279] and PIPEDA, provide provisions for checks and balances. Two parts of this principle are—being responsible for compliance and demonstrating that compliance.[280] These compliance requirements include third-party auditing, Data Protection Impact Assessments

---

[275] Quintavalla & Temperman, *supra* note 90 at 132.
[276] Supra note 65 at 5.
[277] *Ibid* at 6.
[278] "Accountability (OECD AI Principle) - OECD.AI", online: <https://oecd.ai/en/dashboards/ai-principles/P9>. OECD; '"Accountability principle", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accountability-principle/>.
[279] GDPR, Supra note *161*, art. 5(2) & 24.
[280] Formiti-Robert Healey, "GDPR and the Accountability Principle", (12 December 2020), online: *Lexology* <https://www.lexology.com/library/detail.aspx?g=34144a92-3aa2-4c75-b1c3-346be0719117>.

(DPIA), and appointment of privacy officers.[281] Due to the increased unpredictability of AI, DPIAs have become crucial in identifying risks during the development phase of an AI model. Post DPIAs, compliance can be demonstrated during the auditing stage.[282]

3.2 Conclusion

This chapter discussed the implications of data protection principles to AI-based ATs or AI and different kinds of potential privacy (informational privacy) risks and associated risks (for example, security risks) that arise from using AI-based ATs and AI in general. The literature revealed that the privacy risks or concerns faced in the context of AI-based ATs are primarily similar to those faced by any other smart AI technology. However, the personal and sensitive data of a vulnerable group (here PWDs) at stake while using AI-based ATs and the capacity of AI to draw inferences and recognize patterns beyond human intelligence makes this a crucial topic of discussion. With AI, complying with data protection principles might conflict with other interests.[283] For instance, compliance with data minimization might affect the statistical accuracy and effectiveness of the AI model, and purpose and storage limitations might hinder innovation. Therefore, to ensure the safe and responsible deployment of AI-based ATs and the protection of privacy, developers must comply with data protection principles, including data minimization, purpose specification, and accuracy. The next chapter examines reasons for exacerbated vulnerability of PWDs to privacy risks while using AI-based ATs.

---

[281] Office of the Privacy Commissioner of Canada, "Getting Accountability Right with a Privacy Management Program", (17 April 2012), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/> Last Modified: 2012-04-17.
[282] Quintavalla & Temperman, *supra* note 126 at 134.
[283] *Ibid.*

4 PWDs' exacerbated vulnerability to privacy risks

AI-based ATs aim to help PWDs live a more independent and accessible life. However, in the data-driven functioning of AI-based ATs, we often notice that PWDs face potential privacy risks. While PWDs are not the only group vulnerable to potential privacy risks, they face a higher level of vulnerability.[284] The heightened vulnerability of PWDs to information privacy has received scant attention, primarily because most studies at the intersection of technology and disability focus on accessibility.[285] In the current data-driven world, it is imperative to explore PWDs' vulnerability against potential privacy risks related to the rise of AI-based ATs. This chapter answers the question—what makes PWDs especially vulnerable to potential privacy risks while using AI-based ATs. This analysis can also apply to AI systems in general.

As noted in Malgieri's book, *Vulnerability and Data Protection,* the vulnerability literature runs across different disciplines, including social studies, human rights, legal feminism, and others.[286] Scholars from one discipline often adopt the concept of vulnerability from other disciplines. For instance, bioethics adopts the concept of vulnerability from political theory.[287] Therefore, this thesis does not offer a new understanding of vulnerability but briefly reviews some of the important conceptual frameworks proposed by different scholars and follows an understanding that seems to be more relevant in the current data-driven era. Further, this chapter explores the reasons for vulnerability in two phases: during data collection (processing-based) and post-data collection (effects-based).

4.1 The Concept of Vulnerability

Researchers have utilized the term "vulnerability" in various contexts. Some use it synonymously with terms like helplessness, weakness, pain, violence, and dependency.[288]

---

[284] AI Now Institute, "Disability, Bias, and AI - Report", (20 November 2019), online: *AI Inst* <https://ainowinstitute.org/publication/disabilitybiasai-2019>. ["Of course, efforts to collect more, and more accurate, data from disabled people are in tension with efforts to preserve privacy. This is true of all social data collection, but the risks are especially pronounced in the case of disability, given that simply disclosing a disability can pose a significant risk."]

[285] Manifestos for the future of critical disability studies, 1st ed. by Katie Ellis, et. al., (New York: Routledge, 2017) at 13. [Technology and social futures by Goggin, G.]

[286] Gianclaudio Malgieri, *Vulnerability Data Protection Law* (Oxford University Press, 2023), ch 3 at 47 ["Who is the vulnerable individual?"].

[287] *Ibid*.

[288] *Ibid* at 49.

Whereas, others use it whenever support with health, economy, and social challenges is required.[289] Vulnerability also often correlates with risks and victimization, meaning the risk of falling victim to a crime.[290] The literature categorizes definitions of vulnerability into three kinds: "lack of power and possibility of being exploited"[291]; "lack of capacity to protect one's interest"[292]; and a "high likelihood of harm and risks".[293] All three definitions of vulnerability hold equal importance and focusing merely on one by eliminating others would lead to an incomplete understanding of the concept. However, given the theme of this research is potential privacy risks, the "high likelihood of harm and risks" definition seems to be the most relevant and will remain constant throughout the thesis. Apart from the theoretical discussion, there are also various real-life examples to highlight the vulnerability of PWDs in digital space. For instance, cases when PWDs find it harder to locate privacy policies, cannot understand the privacy policies even if they access those, do not understand data processing, cannot consent freely,[294] or cannot exercise their data protection rights.

Jonathan Herring highlights two schools of thought on vulnerability - the first believes in universal vulnerability, and the second considers specific groups or people as vulnerable (individual vulnerability).[295] The latter approach, i.e., the traditional approach, associates vulnerability with people or groups with a distinctive vulnerable character, such as PWDs, ethnic or racial minorities, asylum seekers, and older people. Research and policy-making often use this approach.[296] Against that, Martha Fineman proposes the first approach, universal vulnerability theory. According to the universal theory, everyone experiences vulnerability as a fundamental

---

[289] David Mechanic and Jennifer Tanner, "Vulnerable people, groups, and populations: societal view" (2007) 26:5 Health Affairs 1220.
[290] N. Chakraborti and J Garland, "Reconceptualizing hate crime victimization through the lens of vulnerability and "difference" (2012) 16:4 Theoretical Criminology 499.
[291] Zion D, Gillam L, and Loff B., "The Declaration of Helsinki, CIOMS and the ethics of research on vulnerable populations" (2000) 6 Nature Medicine 613 at 615.
[292] Ruth Macklin, "A global ethics approach to vulnerability" (2012) 5 IJFAB: International Journal of Feminist Approaches to Bioethics 64.
[293] Samia A. Hurst, "Vulnerability in research and health care; describing the elephant in the room?" (2008) 22:4 Bioethics 191.
[294] Article 29-Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" online (pdf): <https://ec.europa.eu/newsroom/article29/items/611236/en> at 10.
[295] Jonathan Herring, *Vulnerable Adults Law* (Oxford University Press, 2016), ch 1 ["Introducing Vulnerability"].
[296] RM Hewer, "A Gossamer Consensus: Discourses of Vulnerability in the Westminster Prostitution Policy Subsystem" (2019) 28 Social & Legal Studies 227.

aspect of human existence.[297] What differentiates humans is their resilience—the ability to overcome or bounce back from a situation faced by an individual. Social factors and the duty of the responsive state influence these situations. For instance, the COVID pandemic affected the entire world and made every human vulnerable; however, an individual's resilience—affected by social factors—determined the extent of vulnerability. Such factors include the availability of healthcare infrastructure and financial capacity to afford treatment or healthcare equipment. Some people criticize this theory for neglecting the injustice that particular groups experience.[298]

Luna, an Argentinian researcher and a WHO expert, proposed a middle ground that takes both individual and universal vulnerability into consideration.[299] Her theory identifies vulnerability as compromising layers[300] and states that despite every individual being vulnerable, there are layers of vulnerability.[301] She notes that a proportionality principle exists between the "quantity and quality of layers of vulnerability" and "intensity of legal protection of vulnerable individual."[302] According to this theory, vulnerability of PWDs is a result of their fundamental existence as a human (universal theory) and also additional factors. These additional factors include, *inter alia,* natural (disability), personal (a personal form of disability and dependency), social (for example, less accessibility), and economic (unaffordable ATs making it harder to have access to the world equally or low investment in R&D of AI-based ATs) factors.

By way of an example illustrating applicability of Luna's theory to PWDs, every individual using an image recognition app (AI-based AT) is vulnerable to potential privacy risks arising from data collection. However, certain additional layers make PVI especially vulnerable to such potential risks. These additional layers or factors include the visual impairment making PVI inherently more dependent on an image-detection app than a person without visual impairment. This dependency exacerbates vulnerability of PVI to potential privacy risks while using the AI-

---

[297] "What Vulnerability Theory Is and Is Not – Vulnerability and the Human Condition", online: <https://scholarblogs.emory.edu/vulnerability/2021/02/01/is-and-is-not/>.
[298] Alyson Cole, "All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique" (2016) 17 *Critical Horizons* 260; Seetal Sunga, "Dealing with Oppression: Indigenous Relations with the State in Canada" (2017) 11 *Ethics and Social Welfare* 135.
[299] "Florencia Luna | The HIV Prevention Trials Network", online: <https://www.hptn.org/Florencia_Luna>.
[300] Florencia Luna, "Identifying and evaluating layers of vulnerability - a way forward" (2019) 19:2 *Developing world bioethics* 86.
[301] *Ibid.*
[302] *Supra* note 286 at 51.

based AT. Another factor or layer that exacerbates vulnerability is accessibility obstacles[303] that often limit PVI's access to relevant information. For example, the captcha function and image verification[304] make it harder to understand privacy policies and present significant barriers for PVI to be aware of privacy practices. Consequently, this leads to risky behaviour, compromised security, and increased potential privacy risks.[305]

Another additional factor that often exacerbates the vulnerability of PWDs is dependency on society to provide alternate accommodation whenever required. Thus, all these additional factors form multiple layers of vulnerability for PWDs. In light of the above example, Luna's vulnerability theory is the most suitable in the context of PWDs using AI-based ATs. This is because even if every data subject is vulnerable to privacy risks with the use of technology, PWDs' vulnerability is heightened because of additional layers. These layers consist of personal attributes, including disability of the individual and social factors, including accessibility barriers.

The European Court of Human Rights (ECtHR) in the case of *Dudgeons v. UK*,[306] recognized this combination of a universal and individual approach to vulnerability.[307] It stated "to provide sufficient safeguards against exploitation and corruption of others, particularly those who are especially vulnerable because they are young, weak in body or mind, inexperienced, or in a state of special physical, official or economic dependence."[308] The terms "especially vulnerable", "weak in body or mind", and "state of special physical…dependence" signify the belief that even if vulnerability is universal, some groups are more vulnerable than others. This interpretation aligns with Luna's vulnerability theory and strengthens the argument that PWDs are especially vulnerable.

---

[303] Tousif Ahmed et al, "Understanding the Physical Safety, Security, and Privacy Concerns of People with Visual Impairments" (2017) 21:3 IEEE Internet Comput 56–63.
[304] Harry Hochheiser, Jinjuan Feng & Jonathan Lazar, "Challenges in Universally Usable Privacy and Security" online: <https://cups.cs.cmu.edu/soups/2008/SOAPS/hochheiser.pdf>.
[305] Daniela Napoli et al, "I'm Literally Just Hoping This Will {Work:'}' Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities" (delivered at Proceedings of the Seventeenth Symposium on Usable Privacy and Security, 2021) online: <https://www.usenix.org/system/files/soups2021-napoli.pdf>.
[306] *Dudgeons v. The United Kingdom* (1981) ECHR A59 7525/76, [1981] ECHR 5.
[307] L Peroni and A Timmer, "Vulnerable Groups: The Promise of an Emerging Concept in European Human Rights Convention Law" (2013) 11 International J of Constitutional L 1056.
[308] *Supra* note 306 at 37 [para. 12].

Similar to Malgieri's analysis of vulnerability in data protection,[309] this thesis will divide the discussion of why PWDs are especially vulnerable to privacy risks while using AI-based ATs into two parts. The first part is the "processing-based" phase—vulnerability during data processing. This phase discusses reasons equally applicable to general users and highlights why the PWDs' vulnerability is exacerbated. The second part is the "Effects-based" phase—vulnerability through the post-collection processing phase. This phase discusses how privacy breach leads to violation of other rights and freedoms.

4.1.1 Power imbalance

Since Luna's layered vulnerability theory relies on power imbalance, it is crucial to discuss the concept before proceeding to the two categories of vulnerability phases. In the digital world, "power is the capacity of A to motivate B to think or do something that B would otherwise not have thought or done."[310] For instance, if users do not share data, then technology platforms often deny access to technology features or the software altogether. This lack of control over marketplace interaction results from information asymmetry, leading to increased vulnerability of one stakeholder, in this case, the vulnerable group or user.[311] Information asymmetry includes opacity and lack of transparency.[312]

In the case of AI-based ATs, data controllers have control over the personal and sensitive data of PWDs and additionally possess greater power to predict or generate new data[313] from the existing data. These factors skew the asymmetry to the data controller's advantage. Along with information asymmetry, one can observe a power imbalance between data subjects and data controllers in terms of knowledge, time, resources, and manpower available.[314] Furthermore, a country's national development also affects the extent of vulnerability. For instance, in a Global

---

[309] *Supra* note 286, ch 4 at 82.
[310] R Forst, "Noumenal Power" (2015) 23 J of Political Philosophy 111.
[311] *Supra* note 286 at 51.
[312] E. Claes, A. Duff, & S. Gutwirth (eds.), *Privacy and the criminal law (*Antwerp/Oxford: Privacy and the criminal law, 2006) at 61 [P De Hert and S Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power'].
[313] Citron and F Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington L Rev 1.
[314] *Supra* note 126, ch 11 at 162 [Bart Van der Sloot, "The Production of and Control over Data in the AI-Era"].

South country like Vietnam, information privacy is still a luxury as the focus is primarily on accessibility.[315]

Looking at this power imbalance from Luna's layer vulnerability theory perspective, even though every user is vulnerable when dealing with the data processor, certain groups could be more vulnerable because of additional factors. For instance, some studies observed that PWDs, especially PVI and people with cognitive impairment, were unaware or lacked understanding of the data collection practice due to problems locating, reading or understanding privacy policies.[316] This example shows that the power imbalance dynamic affects different groups of people differently. Certain groups of PWDs might be more vulnerable than others; however, the capacity to protect information privacy is limited in all groups of PWDs.[317]

The concept of power imbalance in the data protection space relates to consumer protection. It could be a one-to-one relationship or a broader structural context. As discussed by Malgieri in his book "*Vulnerability and Data Protection Law,"*[318] in data protection studies, one should consider the factors and effects of consumer vulnerability as layers of vulnerability for data subjects:[319]

- Personal characteristics of consumer (here, data subject)
- Power characteristics of suppliers (here, data controller)
- Vulnerability drivers

The applicability of these three factors in the context of PWDs can be explained through an example. A PVI uses an image recognition app, such as Microsoft's Seeing AI, to identify objects in everyday life. In order to use the app, the PVI has to consent to data collection or simply accept the privacy policy to use the app—power characteristics of the data controller. Here, visual impairment of the individual (the disability) is the individual or personal characteristic. The user's dependency on the app to see the world around them or to be more independent creates a power

---

[315] *Supra* note 116.
[316] Virginie Cobigo, et al. "Protecting the privacy of technology users who have cognitive disabilities: Identifying areas for improvement and targets for change" (2020) 7 *Journal of rehabilitation and assistive technologies engineering*.
[317] Hajer Chalghoumi et al, "Information Privacy for Technology Users With Intellectual and Developmental Disabilities: Why Does It Matter?" (2019) 29:3 Ethics Behav 201–217.
[318] *Supra* note 286.
[319] *Ibid* at 70.

imbalance in favour of the data controller. While using the app, the PVI may unknowingly provide financial data, medical data, or any other personal data, which is then processed or stored on a data server, exposing them to potential privacy breaches or security issues. Lastly, certain vulnerability drivers could exacerbate the vulnerability. These include inaccessible environment—necessitating the use of the app, and the use of an AI model for tracking of preferences, everyday activities, or PVI's user profile. This could reveal a plethora of information about the users and make them easy targets for advertisements and fraud—especially because of the increased dependency of PVI on this app.

One might argue that the power characteristics of the data controller would remain the same for all its users, making every user vulnerable. However, based on the layer vulnerability approach in a data-driven world, I contend that the additional factors exacerbate an individual's vulnerability. For instance, in the above example, PVI's disability leading to the dependency on the app to perform everyday activities and contributing factors such as inaccessible environment exacerbate PVI's vulnerability to potential risks. This thereby compounds their vulnerability, making PWDs an evident vulnerable group in the context of AI-based ATs.

To conclude, as Malgieri rightly highlights that following a universal approach in the data-driven world would outcast and ignore the differences that make certain groups more susceptible to data privacy rights breaches in an already unequal and imbalanced world. Conversely, adopting only the individual approach would create further bifurcation within the legal framework, making it harder for entities to comply with or navigate the data protection framework. Therefore, Luna's theory is the right balance between the two extreme theories and is appropriately relevant in today's data-driven world. This layered approach justifies the placement of PWDs in the vulnerable group category, considering the additional layers which add to their vulnerability.

As described in Malgieri's book[320], vulnerability in the context of data protection can be in two phases: vulnerability during the data processing (processing-based) and vulnerability to the consequences or adverse effects of data processing (effects-based).[321] Some reasons discussed in these phases make PWDs more vulnerable than they would have been without the incorporation

[320] *Supra* note 286, ch 4 at 82.
[321] *Ibid*, ch 3 [Data Subjects' Vulnerability].

of AI in ATs, while others make PWDs more vulnerable than people without disabilities. These will be examined below in turn.

4.2 During the data processing phase [Processing-based Vulnerability] — generic but exacerbated for PWDs

The reasons discussed under this section also apply to general data subjects; however, these reasons exacerbate the vulnerability of PWDs.

4.2.1 Trade-off

PWDs make a fundamental trade-off during the data collection phase of AI-based ATs. On the one hand, while using AI-based ATs, PWDs provide personal and sensitive data to data controllers and processors to improve access and perform everyday activities. On the other hand, processing such personal and sensitive data collected during PWDs' daily activities raises potential privacy and data breach risks and thus requires protection. Guidelines, legal frameworks, or technical solutions such as privacy-by-design provide this protection.[322] However, despite the protection offered under these solutions, PWDs often end up making compromises about control over their data. This causes an intentional or unintentional trade-off between the privacy of PWDs in exchange for access, independence, and convenience to perform everyday activities by using AI-based ATs. As I will discuss below, this trade-off exacerbates PWDs' vulnerability to potential privacy risks while using AI-based ATs.

Various reports and empirical research have shown that privacy is one of the major concerns in the adoption or usage[323] of technology, including the internet, computers, and monitoring, surveillance, and tracking systems, by PWDs.[324] Despite the privacy concerns raised, PWDs use ATs and disclose tons of personal data every day. This creates a paradox in the expressed concerns and depicted behaviour of PWDs—a phenomenon commonly known as the privacy paradox. This paradox demonstrates the trade-off PWDs make between privacy and gaining access, independence, or convenience in performing everyday activities. The discussion

---

[322] Kris Vera Hartmann, Nadia Primc & Giovanni Rubeis, "Lost in translation? Conceptions of privacy and independence in the technical development of AI-based AAL" (2023) 26:1 Med Health Care Philos 99–110.
[323] Scott Beach et al, "Disability, Age, and Informational Privacy Attitudes in Quality of Life Technology Applications: Results from a National Web Survey" (2009) 2:1 ACM Trans Access Computing (TACCESS) 5:1-5:21.
[324] *Ibid.*

of privacy paradox encompasses various forms of privacy,[325] including territorial privacy, physical privacy, and information privacy.[326] However, given the scope, this thesis will focus on the privacy paradox in relation to information privacy.

Users without disabilities also demonstrate privacy paradox while using a majority of technology. For instance, a survey conducted a year before the adoption of GDPR revealed that two-thirds of Europeans were concerned about the lack of informational control, and a majority were concerned about the personalization of advertisements.[327] Despite these concerns, tech companies like Google and YouTube have seen an increase in the number of users over the years.[328] A similar paradox exists in the context of education, as children prefer the ease of use while trading off their privacy.[329] Even if general users show these paradoxical patterns, empirical studies have shown a higher tendency of PWDs to share their personal or sensitive data despite knowing the cost of losing their privacy.

National-level research studied the privacy concerns of 1518 adult participants concerning quality-of-life technology (a type of AT).[330] The results revealed that those with disabilities were significantly more willing to allow sharing and recording of personal information while using quality-of-life technology, including ATs and AI-based AT, than participants without disabilities. Irrespective of whether the PWDs were younger or older in age, their acceptance rate to use and share personal information with these technologies was significantly higher than people without disabilities. This was an important finding based on a large-scale national-level sample size. Another interesting finding in the same study was that prior use of ATs by PWDs did not affect their attitude towards information privacy. Furthermore, researchers divided the participants into three categories based on their level of disability—first, no disability participants; second, PWDs that needed help with Instrumental Activities of Daily Living (IADL); and third, PWDs that needed

---

[325] Spyros Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon" (2017) 64 Computer & Security 122–134.
[326] Privacy or ability of data subjects to control their data or information and its processing.
[327] Eurobarometer S. Special Eurobarometer 431: Data protection (Directorate-General for Communication, 2015) online: <https://data.europa.eu/data/datasets/s2075_83_1_431_eng?locale=en>.
[328] Francesco Massara, Francesco Raggiotto & W Gregory Voss, "Unpacking the privacy paradox of consumers: A psychological perspective" (2021) 38:10 Psychol Mark 1814–1827.
[329] Lorayne Robertson and Bill Muirhead, "Digital Privacy in the Mainstream of Education" (2019) 18:7 The Open Cybernetics & Systematics J 118.
[330] *Supra* note 323.

help with IADL and Activities of Daily Living (ADL). PWDs who required assistance with both IADL and ADL showed the highest acceptance to sharing and recording their personal data than those PWDs who required assistance only with IADL, who in turn showed higher acceptance compared to those with no disability.[331] This finding suggests that people suffering from health problems are more likely to become accepting of ATs.[332] This links back to the vulnerability theory of how additional layers (here, disability extent) can increase an individual's vulnerability state. It further notes that the extent of disability increases reliance on ATs, leading to a trade-off, which, in turn, exposes PWDs to potential privacy risks.

PWDs' consent to using AI-based ATs or ATs is less of a choice and more of a requirement to keep themselves protected, have access to the world, or gain independence to perform everyday tasks. For instance, a study showed that caregivers, despite raising privacy concerns, supported the use of video-based ATs or surveillance for people with dementia to keep them protected and avoid risks to their health.[333] Many PWDs believe they are more susceptible to trade-offs in emergencies because they lose control over their personal medical data.[334] Despite such awareness, a detailed literature review of video-based Active and Assisted Living Technologies (AAL or AT) revealed that the greater the medical necessity or need for help, the higher the willingness of a PWD to give up their privacy.[335] Further, PWDs have shown a willingness to use the detection of medical emergencies feature even if it meant accepting surveillance and loss of privacy.[336] Therefore, unlike other technologies, the use of AI-based ATs by PWDs becomes necessary to perform everyday activities on their own and live a safe life instead of using them as a choice. This is because by denying the use of ATs, PWDs often will either have to seek human assistance or

---

[331] Tamara Mujirishvili et al, "Acceptance and Privacy Perceptions Toward Video-based Active and Assisted Living Technologies: Scoping Review" (2023) 25:1 J Med Internet Res at 14.
[332] Jane Chung, et. al., "Ethical considerations regarding the use of smart home technologies for older adults: an integrative review" (2016) 34:1 Annual review of nursing research 155.
[333] Maurice Mulvenna et al, "Views of Caregivers on the Ethics of Assistive Technology Used for Home Surveillance of People Living with Dementia" (2017) 10:2 Neuroethics 255–266.
[334] Alisa Zezulak, Faiza Tazi & Sanchari Das, *SoK: Evaluating Privacy and Security Concerns of Using Web Services for the Disabled Population* (arXiv, 2023) arXiv:2302.13261 [cs] at 4; F. Hamidi, et. al., "Who should have access to my pointing data? privacy trade-offs of adaptive assistive technologies" (delivered at Proceedings of the 20th international ACM sigaccess conference on computers and accessibility, 2018); D. Grunwel and T. Sahama, "Delegation of access in an information accountability framework for ehealth," (delivered at Proceedings of the Australasian Computer Science Week Multiconference, 2016).
[335] *Supra* note 331.
[336] *Ibid.*

inadequately perform certain tasks. Seeking human assistance has its own privacy concerns and, most importantly, includes physical, informational, and spatial privacy concerns.[337]

Another concerning observation in at least 27 empirical studies is that users often choose not to use the technology altogether if they feel their data is exposed to higher privacy concerns.[338] Thus, declining to trade-off deprives PWDs of technological advancements that can benefit them. On the contrary, PWDs sometimes believe the privacy trade-off is acceptable in return for AT's benefits.[339]

The studies discussed in this section can be summarized into three points. First, PWDs have shown higher willingness to share their personal data compared to people without disabilities. Second, their willingness to share their personal data and adopt ATs increases with the extent of their medical condition or disability. Third, the purpose of use an AT or AI-based AT is to live an independent life and have equal access to the world and opportunities. Therefore, providing consent for data collection to use the AT is not necessarily a deliberate choice instead often a necessity. These results establish the trade-off of privacy to use AI-based ATs that PWDs make. For PWDs, there can be three scenarios. First, PWDs all-together avoid using AI-based ATs due to potential privacy concerns, thereby compromising their access and independence to perform everyday tasks. Second, PWDs continue to use AI-based ATs out of need but have expectations of privacy protection. Third, PWDs make peace with the trade-off and consider this to be an acceptable trade-off. However, the important question that arises here is whether this trade-off is reasonable.

4.2.2 How "informed" is the informed consent

Consent is a common basis of data processing in various jurisdictions, including Canada, unless an exception to data collection applies. As a part of legal compliance in major jurisdictions, the data processor and controller have to provide, *inter alia*, a detailed account of the data processing in the privacy policy or notice to seek consent. Most jurisdictions' privacy and data

---

[337] Taslima Akter, Bryan Dosono & Tousif Ahmed, "'I am uncomfortable sharing what I can't see': Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications" (delivered at USENIX Security Symposium, 2020).
[338] Zezulak, Tazi & Das, *supra* note 334.
[339] Alessandro Diogo Vieira, Higor Leite & Ana Vitória Lachowski Volochtchuk, "The impact of voice assistant home devices on people with disabilities: A longitudinal study" (2022) 184 Technol Forecast Soc Change 121961.

protection laws emphasize obtaining informed or meaningful consent. However, with the overflow of information and frequent introduction of new technology, how informed is this informed consent, especially in the context of PWDs and ATs?

Consent as a legal basis for data processing, especially under the notice-consent model followed in major jurisdictions, including Canada, presents challenges for users. Various studies highlight the issues with privacy policies or notices. A writer for the Washington Post found that reading the privacy policies of all the apps on his phone would mean reading 1 million words.[340] Another study found that reading and providing consent to the privacy policies of all the websites Americans visit in a year would take 244 hours per year.[341] At times, many users are unaware of what they are consenting to. A 2019 study revealed that only 9% of the users read the privacy policy.[342] These highlight the problematic conclusion of a consent being an informed consent if obtained after providing privacy notice to a user.

Apart from the general issues highlighted in literature, there are certain consent-related concerns specific to AI-based ATs or AI in general. First, AI's functioning is often unpredictable and opaque. This often leads to unforeseeable predictions, interrelations among different personal data, and the creation of novel uses, all of which lead to issues with transparency.[343] Second, the issue with obtaining re-consent in the case of AI to comply with the purpose specification principle and use data only for the purpose for which the consent was obtained, as discussed in the previous chapter. The re-consent requirement is primarily because of AI's capability to use personal or sensitive data for a purpose other than the initial purpose to which the user consented. In the case of people with cognitive disabilities, obtaining re-consent becomes crucial since the cognitive capabilities of such people could decrease over time.[344] Thirdly, how to notify and the entity or

---

[340] "I tried to read all my app privacy policies. It was 1 million words.", (31 May 2022), online: *Wash Post* <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>.
[341] Brooke Auxier Turner Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica, "4. Americans' attitudes and experiences with privacy policies and laws", (15 November 2019), online: *Pew Res Cent* <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>.
[342] Ibid.
[343] Lori Cameron, "Artificial Intelligence and Consent: Navigating The Ethics of Automation and Consumer Choice", (16 September 2018), online: *IEEE Comput Soc* <https://www.computer.org/publications/tech-news/research/ai-and-the-ethics-of-automating-consent/>.
[344] Chalghoumi et al, "Information Privacy for Technology Users With Intellectual and Developmental Disabilities", *supra* note 317.

individual responsible for notification is another challenge with AI-based ATs. For instance, AI-powered AR glasses record audio and video data. If used in public spaces, PWDs can verbally notify the bystanders or the person they are interacting with. In this case, even though the company provides these features, it shifts the burden to the PWD user to notify bystanders or people PWDs interact with. Moreover, certain AI-based AR glasses collect audiovisual data to process and provide output. This could mean using the audiovisual data provided by PWDs to provide additional information about the surroundings or bystanders using image or facial recognition technology. The transparency requirements with AI technology are far more complicated than the traditional audiovisual recordings.[345] These technical complications make it harder for PWD or proxy decision-makers to understand what they are consenting to.[346]

In addition to AI specific concerns in obtaining meaningful consent, PWDs extensively rely on technology (here, AI-based ATs) to equally participate in society makes it more challenging.[347] It is worth considering whether PWDs provide meaningful consent to access a technology that assists them in communicating, working, and navigating physical and digital environments. Given the usual method of seeking consent on "take-it-or-leave-it" terms, not consenting often restricts PWDs from using AI-based ATs and deprives them of ATs' benefits. This links back to the trade-off made by PWDs in absence of an actual choice. Another challenge that hinders obtaining meaningful consent for PWDs is the lack of accessible information or lack of understanding on the part of PWDs, combined with complicated privacy policies. Literature shows that PWDs face various accessibility issues when accessing technologies or data processing information, including authentication interface issues.[348] Studies have also observed a discrepancy between what PWDs perceive personal data collection and process to be and the reality of a technology's privacy characteristics or data processing process.[349] This could be because of the

---

[345] Dick, *supra* note 163.
[346] Tenzin Wangmo et al, "Ethical concerns with the use of intelligent assistive technology: findings from a qualitative study with professional stakeholders" (2019) 20:1 BMC Med Ethics 98.
[347] Ilias Bantekas, Michael Ashley Stein, and Dimitris Anastasiou (eds), *The UN Convention on the Rights of Persons with Disabilities: A Commentary* (online edn, Oxford Academic, 2018) at 604 [Molly Land et al, "Art.22 Respect for Privacy", online: *Oxf Public Int Law* <https://opil-ouplaw-com.ezproxy.library.yorku.ca/display/10.1093/law/9780198810667.001.0001/law-9780198810667-chapter-23>].
[348] Zezulak, Tazi & Das, *supra* note 334.
[349] N. Gorm & I. Shklovski, "Sharing Steps in the Workplace: Changing Privacy Concerns Over Time" (delivered at CHI Conference on Human Factors in Computing Systems, 2016) 4315 online:

vague terminology used in the privacy policies which make it harder to understand the data processing. The use of legalese adds onto this issue, which limits users, especially PWIDD, from fully understanding data processing information.[350]

Even within PWDs, different levels of vulnerability exacerbate this issue. A 2023 study found that PVI were the most vulnerable in the digital space because of limited access to resources, which hindered their capacity to search for privacy related information.[351] PVI have also expressed a lack of understanding and concerns about storage provisions, especially cloud storage.[352] A study participant with visual impairment revealed that she clicks photos of her credit cards and other financial data to be more independent while making transactions. However, even after deleting photos of her credit cards or other financial information, she was often unsure and worried if the photos are still being backed up in the cloud.[353] Additionally, various studies have observed that the limited capacity of PWIDD to understand and process information could make them more vulnerable to privacy threats.[354] A 2019 study highlighted that PWIDD appeared to be more vulnerable than other users.[355]

Another obstacle for obtaining meaningful consent is that many PWDs are unaware of the privacy and security concerns of the technology or web services they use.[356] Researchers tried to understand the PVI's perception of the privacy policies of ATs before and after educating them about the content of privacy policies. The results revealed that along with disability, other

---

<https://doi.org/10.1145/2858036.2858352>; R Kang, et. al., "My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security" (delivered at Eleventh Symposium On Usable Privacy and Security SOUPS, 2015) online: <https://www.usenix.org/conference/soups2015/proceedings/presentation/kang>; W. Zhou and S. Piramuthu, "Security/privacy of wearable fitness tracking IoT devices" (delivered at 9th Iberian Conference on Information Systems and Technologies (CISTI), 2014) online: <https://doi.org/10.1109/CISTI.2014.6877073>.

[350] Chalghoumi et al, "Information Privacy for Technology Users With Intellectual and Developmental Disabilities", *supra* note 317.

[351] *Supra* note 116.

[352] Jordan Hayes et al, "Cooperative Privacy and Security: Learning from People with Visual Impairments and Their Allies" online: <https://www.usenix.org/conference/soups2019/presentation/hayes>.

[353] Ibid.

[354] R. Didden et al., "Cyberbullying among students with intellectual and developmental disability in special education settings" (2009) 12:3 Developmental Neurorehabilitation 146; K. M. Holmes & N. O'Loughlin, "The experiences of people with learning disabilities on social networking sites" (2014) 42:1 British J of Learning Disabilities 1; Löfgren-Mårtenson, "Love in cyberspace: Swedish young people with intellectual disabilities and the internet 1" (2008) 10:2 Scandinavian Journal of Disability Research 125.

[355] Chalghoumi et al, "Information Privacy for Technology Users With Intellectual and Developmental Disabilities", *supra* note 317.

[356] *Ibid.*

sociodemographic backgrounds, including vision, age, health conditions, living conditions, race/ethnicity, and education, affected PVI's tendency to adopt ATs after educating them about the privacy policies of those ATs.[357] As a solution, it further suggested using educational tools to assist PVI in better understanding privacy concerns and policies. Reading this observation in the context of the vulnerability theory, we can conclude that the sociodemographic backgrounds act as additional layers of vulnerability to the primary 'disability' layer.

Apart from PWDs facing challenges in making informed decisions while consenting, the privacy policies of these AI-based ATs are problematic. A 2015 study revealed that privacy policies do not disclose all data practices or deliberately remain silent on certain data processing features.[358] Another study published in 2022 analyzed the privacy policies of 13 visual AT (VAT) companies.[359] The results of this study showed:

- 7 out of 13 VAT companies did not clarify if the technology collected images and videos.
- None of the companies provided users with any information regarding the retention of personal visual data and the option to opt out of data (images or videos) collection.
- Only 1 company mentioned that users had the right to delete their data.
- Only 2 out of 13 companies disclosed whether they use the collected data (images and videos) for training AI models,
- Merely two companies disclosed selling or sharing the collected data with third parties.[360]
- One VAT vaguely mentioned that the company anonymizes the data "as much as possible" and "cannot, however, strip or edit the content of the video stream." These incomplete privacy policies leave users unaware of the crucial aspects of the data processing phase.
- VAT policies did not disclose the parties internally and third parties who had access to user data.[361]

---

[357] Hyung Nam Kim, "Digital Privacy of Assistive Technology Users with Visual Disabilities" (delivered at Proceedings of the 2022 HFES 66th International Annual Meeting, 2022).
[358] "How 'Notice and Consent' Fails to Protect Our Privacy", online: *New Am* <http://newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/>.
[359] Abigale Stangl et al, "Privacy Concerns for Visual Assistance Technologies" (2022) 15:2 ACM Trans Access Comput 1–43.
[360] Ibid
[361] Ibid at 20.

- The same study found that users' most common privacy risk was "unknown data handling" which primarily arose because of the use of AI in VATs.

Table 8. Results of the Privacy Policy Analysis, Showing Whether Companies Provide ***notice*** About Collecting Users' Data (Prompts 1-3), the Length of Data Retention (Prompt 4), the Use of Data to Train AI (Prompt 5), and the Dissemination of Data to Third Parties (Prompt 6), as well as the ***choice*** these Companies Provide Users for Deleting Their Data (Prompt 7) and opting-out of having their Data Collected (Prompt 8)

	Collect			**Retain**		**Train AI**		**Third Party**		**Delete**		**Opt-Out**	
	1	*2*	*3*	*4a*	*4b*	*5a*	*5b*	*6a*	*6b*	*7a*	*7b*	*8a*	*8b*
	Any	*Video*	*Image*	*Any*	*Visual*	*Any*	*Visual*	*Any*	*Visual*	*Any*	*Visual*	*Any*	*Visual*
Company													
Aira	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
Be My Eyes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No	No
BeSpecular	Yes	No	Yes	Yes	No	No	No	Yes	No	Yes	No	No	No
LookTel	Yes	No	No	No	No	No	No	No	No	Yes	No	Yes	No
OrCam	Yes	No	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No
Sensotech	Yes	No	No	Yes	No	No	No	No	No	Yes	No	No	No
TapTapSee	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No
Google	Yes	Yes	Yes	Yes	No	Yes	No	No	No	Yes	No	No	No
Microsoft	Yes	Yes	Yes	No	No	Yes	No	Yes	No	No	No	Yes	No
Adobe	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Amazon	Yes	**Yes**	**Yes**	No	No	No	No	Yes	No	No	No	Yes	No
Apple	Yes	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	No
Facebook	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	No	No
Totals													
Yes	13/13	8/13	9/13	8/13	0/13	9/13	2/13	10/13	2/13	10/13	1/13	6/13	0/13
No	0/13	5/13	4/13	5/13	13/13	4/13	11/13	3/13	11/13	3/13	12/13	7/13	13/13
Inter-rater Reliability Measures													
Cohen's kappa	1.0	.92	.84	.84	.77	1.00	.77	.92	.77	.61	.77	.84	.84

For prompts 4-8, each question comes with two sub-prompts, the first one related to data in general and the second one specifically looking at handling of visual data. **Yes** = instances when the policy included the information; **No** = instances when the policy did not include the information.

Figure 5: Table showing results of the 13 VAT companies' privacy policies analyzed in the 2022 published study[362]

Findings of these studies reveal that such privacy policies defeat the concept of informed or meaningful consent. They mis-align the expectation of users to be informed about the data processing and the information they receive from the data controller. A question thus arises—how can a PWD make an informed decision if the privacy policies lack information?

[362] Stangl et al, *supra* note 359.

To conclude, social network and context affect disclosure of information by PWDs, and it is not merely their deliberate decision.[363] This decision-making results from a power imbalance in society and its effects on users, primarily marginalized users such as PWDs.[364] The Council of Europe (CoE) Convention on Trafficking in human beings[365], in its explanatory report,[366] discussed the concept of abuse of a position of vulnerability in the context of human trafficking. The report highlighted "abuse of any situation in which the person involved has no real and acceptable alternative to submitting to the abuse." Even though this interpretation cannot unequivocally be extended to other fields, it is relevant for vulnerability in information privacy.[367] As suggested in the previous subsection, PWDs do not necessarily have a real choice regarding the use of AI-based ATs, especially with the notice-consent model. If PWDs do not accept the terms and conditions or agree to the privacy policies, they often cannot use the AT altogether. In such a case, PWDs lack bargaining power. Not consenting to the privacy policy notice results in losing access to the technology. What aggravates this vulnerability is that with AI-based ATs and PWDs, one not only loses access to technology but also the chance to live a more independent life.

Thus, the reality of user behaviour is contrary to the notice-consent model's assumption that a user is reasonable and rational.[368] This assumption expects users to read and understand the privacy policy or notices reasonably and rationally before deciding.[369] Data controllers under this model often perform the bare minimum by notifying data subjects. Resultantly, this imposes a higher responsibility on the data subjects to understand and consent to the data collection.[370] Despite the common issues with notice-consent model, additional layers such as accessibility issues, sociodemographic influence on an individual's understanding of the privacy notice, and

---

[363] Alice E Marwick & Danah Boyd, "Networked privacy: How teenagers negotiate context in social media" (2014) 16:7 New Media Soc 1051–1067.
[364] *Supra* note 116.
[365] Council of Europe Convention on Action against Trafficking in Human Beings, 2005, Council of Europe Treaty Series - No. 197, online: <https://www.coe.int/it/web/conventions/fulllist/-/conventions/rms/090000168008371d>.
[366] Council of Europe, *Explanatory* Report to the Council of Europe Convention on Action against Trafficking in Human Beings (Warsaw: Council of Europe Treaty Series, 2005) at 15, online: <https://rm.coe.int/16800d3812>.
[367] Malgieri, *supra* note 286 at 61.
[368] Kirsten Martin, "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online" (2013) J of Pub Pol'y and Marketing.
[369] Caroline Ross, "Canadian Bar Association - The privacy paradox" (19 April 2022), online (blog): <https://www.cba.org/Sections/Privacy-and-Access/Articles/2022/The-privacy-paradox>.
[370] Kirsten Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy" (2016) 137:3 J Bus Ethics 551–569.

incomplete information in privacy policies or notices clearly heighten PWDs' vulnerability to potential privacy risks.

4.2.3 The "sensitivity" of PWDs' data collected by AI-based ATs

An important factor that makes discussion of the privacy of PWDs in relation to AI-based ATs highly crucial and unique is the kind of data at stake. The majority of the data collected or processed by this technology is personal or sensitive. Sensitive data, referred to by different names such as "special categories of personal data",[371] is often subject to additional or stricter regulations. This data category includes data regarding a PWD's everyday activities, medical records, disability data, biometric data, financial data and more.[372] The following two studies illustrate the categories of personal data collected by AI-based ATs or ATs. First, an analysis of 20,000 image-and-question pairs from the VizWiz[373] dataset found personal data ranging from addresses, medicine labels, and credit card information to the presence of face or body parts of users or bystanders.[374] Second, a 2019 study visually analyzed 40,000 images PVI clicked using the app VizWiz. This analysis discovered 19 types of personal visual content containing private objects and texts.[375]

Apart from direct data collection, sometimes indirect patterns can reveal information, for instance, by typing speed or voice clarity. This is called non-identifiable data. This data, if linked to the user's demographic information can reveal hidden details and invade privacy. Given the vast amount of data collected by AI-based ATs, for PWDs, this might lead to unwanted disclosure of their disability status or other important information through non-identifiable data. For instance, an AI-based AT does not capture images and videos, but it captures PWDs' skeletons, silhouettes, and movements using AI models. This sensor detection if combined with other AI technology like emotion recognition[376] can lead to an invasion of privacy equivalent to that by visual detection of faces.[377] For example, many AI-based ATs do not collect or process strictly medical data.

---

[371] *Supra* note 161, art 9.
[372] *Ibid*.
[373] "VizWiz", online: <https://www.vizwiz.com/>.
[374] Taslima Akter et al, "Privacy Implications of Artificial and Human Intelligence Assistive Tools for Visually Impaired People" (2019) online: < https://aktertaslima.github.io/files/CHI_Workshop_19.pdf>.
[375] Danna Gurari, et.al., "VizWiz-Priv: A dataset for recognizing the presence and purpose of private visual information in images taken by blind people" (delivered at Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019).
[376] Rus Silvia, et. al. "The emotive couch - learning emotions by capacitively sensed" (2018) Procedia Computer Science 130.
[377] Hartmann, Primc & Rubeis, "Lost in translation?", *supra* note 322.

However, the data collected can infer behaviour, routines, and health status.[378] Examples of such data include self-tracking data collected from non-medical wearables, camera-recorded data, voice-recorded data, swiping behaviour, and data from screen-reading ATs.[379] Furthermore, with access to personal and sensitive data, AI-based ATs can invade PWDs' emotional privacy too. Literature revealed that PWDs expressed concerns about emotional and physical privacy breaches, along with information privacy, because of AT's data collection.[380] Therefore, AI's capacity to infer or identify details from proxy disclosure makes the privacy interest of PWDs a crucial topic of discussion.

As mentioned previously, AI's capacity to identify patterns and draw inferences from data makes this data more vulnerable to exploitation. AI is different because algorithmic decision-making or functioning is based on input data processing, which leads to results, forecasts, decisions or suggestions. Unlike traditional technologies' "input-processing-output" model, AI has the additional layer of learning, understanding, acting and perceiving from the input data. For instance, a visual AI-based AT could reveal the user's disability, the extent of vision loss, and more personal or everyday information based on usage of the AT.[381] As emphasized in the US report on Facial Recognition Technology (FRT), FRT (used in certain AI-VATs) impinges on privacy because it can identify and track users' behaviours, patterns, habits, and affiliations.[382] This additional layer of advanced functioning makes adhering to human rights and ethical values crucial.[383] In the case of PWDs, such ATs collect medical, biometric, behavioural, and other kinds of sensitive data.

---

[378] Mason Marks "Emergent Medical Data: Health Information Inferred by Artificial Intelligence | Semantic Scholar" (14 March 2020), online: <https://www.semanticscholar.org/paper/Emergent-Medical-Data%3A-Health-Information-Inferred-Marks/6ec346394b4f3f54d4de9a4e8b35b4f96ef8f21c>.

[379] Wangmo et al, "Ethical concerns with the use of intelligent assistive technology", *supra* note 346.

[380] Mujirishvili et al, "Acceptance and Privacy Perceptions Toward Video-based Active and Assisted Living Technologies", *supra* note 331.

[381] Nora McDonald, Aaron Massey & Foad Hamidi, "Elicitation and Empathy with AI-enhanced Adaptive Assistive Technologies (AATs): Towards Sustainable Inclusive Design Method Education" (2023) 11:2 J Probl Based Learn High Educ 78–99.

[382] "Advances in Facial Recognition Technology Have Outpaced Laws, Regulations - New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns | National Academies", online: <https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns? >.

[383] Artificial intelligence and privacy, and children's privacy - Report of the Special Rapporteur on the right to privacy HRC, 46th sess, 2021 A/HRC/46/37.

Studies have shown that the functioning of AI-based systems could lead to compounded intersectional discrimination (discussed later in this chapter) against PWDs.[384]

Disclosure of disability-related information drastically affects PWDs. According to laws in most jurisdictions, PWDs have the ability to control whether they disclose a disability to an employer or any third party. However, with AI-based ATs, its mere usage can disclose a disability or AI can potentially interpret disability information from collected data. The class action case of *Bloom v. ACT, Inc.*[385] illustrates how disclosure of disability can be harmful to PWDs. In this case, some students filed a lawsuit against ACT (American College Test) for disclosing disability status and personally identifiable data of students, including their disability data, to universities. This disclosure allegedly led to the exclusion of students with disabilities from admission process. Even though ACT did not accept the claims, it settled the matter by paying $16 million to affected students and promising to remove students' accommodation requirements on score reports sent to universities.[386] This is a prime example of how disclosing personal and sensitive information can harm PWDs because of unfair practices. Certain AI-based ATs offer cloud-based assistive services, including image or facial recognition for PVI and text-to-speech or text simplification for people with cognitive and learning disabilities. In such cases, the data discloses the user's disability at least to the developer, network operator, operating system vendor, and data processor. If used unfairly, this could cause harm to PWDs.

Data privacy concerns linked with disclosure of sensitive data are worrisome for every user; however, it affects socially vulnerable and marginalized groups like PWDs more.[387] A significant reason for that is the stigma associated with disability, coupled with segregation and discrimination that PWDs often face. As discussed in the previous chapter, AI amplifies the potential privacy concerns ATs pose. Technologies like AI-based ATs or AR do not just passively record the environment; instead, they collect and process audiovisual data to provide outputs or personalized results for users. Since some AI-based ATs can be used on mobile or wearable

---

[384] Francisco Jose Bariffi, "Artificial Intelligence, Human Rights and Disability" (2021) 26:2 Pensar - Rev Ciênc Juríd 14–1.
[385] "Bloom v. ACT, Inc., Case No.: CV 18-6749-GW-KSx | Casetext Search + Citator", online: <https://casetext.com/case/bloom-v-act-inc>.
[386] Ariana Aboulafia, "Internet Privacy Is A Disability Rights Issue | TechPolicy.Press", (19 January 2024), online: *Tech Policy Press* <https://techpolicy.press/internet-privacy-is-a-disability-rights-issue>.
[387] *Supra* note 235.

devices, it becomes difficult to understand when they are in use.[388] Further, if third parties, such as employers, insurance companies, and university admission organizations, have access to the data collected, there is a risk of discrimination. Such discrimination could include issues with performance reviews with employers, altered health insurance by insurance providers, or university admission issues with admission committees, limiting opportunities or inflicting other forms of harm, which might not have existed without the disclosure of disability. Further, disclosure of personal data related to disabilities can lead to bullying, harassment, mental or physical abuse[389], and social exclusion. An example of this is when data leakage led to tele-frauds against PWDs in China.[390]

This brings me to the second set of reasons—effects-based vulnerability—which are PWDs-specific and discuss how privacy rights violation can impact or lead to violation of other rights, freedoms, or principles.

4.3 Post-collection processing phase [Effects-based]

There is a conflict between the need to incorporate AI and big data into technologies and the protection of the privacy needs of individuals. However, apart from direct privacy concerns arising during the data collection or processing phase, violation of privacy right is intertwined with other freedoms, principles, or rights under the CRPD and domestic laws.[391] According to a "human rights-based approach" to AI, these other freedoms, principles, or rights, include equality and non-discrimination, participation and accountability principles. These principles also form the basis of the Sustainable Development Goals (SDGs) and guiding principles of Business and Human Rights.[392]

Despite express rights under the law, PWDs are often unable to exercise them. A scholar rightly states, "the reality of persons with disabilities' rights experience in most contexts is more

---

[388] Dick, *supra* note 163.
[389] "Office for Victims of Crime - Multidisciplinary Response to Crime Victims With Disabilities", online: <https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/victimswithdisabilities/stateguide/risk-factors.html>.
[390] Fei Yang, Kaili Zheng & Yu Yao, "Protecting people with disabilities' data privacy in government information disclosure: facilitation by procurator-led public-interest litigation" (2024) 39:3 Disability Soc 811–816.
[391] Daniel J Solove, "Conceptualizing Privacy" (2002) 90 Cal L Rev 1087.
[392] *Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights Report of the Secretary-General* UNHRC, 43rd sess, A/HRC/43/29 (2020), para. 41.

complex than simply outright denial. Even when their entitlement to rights has been formally recognized and uncontentious, their disability has often effectively excluded them from rights enjoyment."[393]

As pointed out earlier, according to Luna's vulnerability layer theory, there are two factors to assess vulnerability: harmfulness (severity of the risk) and likelihood.[394] In Malgieri's book, for effect-based vulnerability, the likelihood factor is the primary factor. Likelihood is the possibility of risk occurrence ranging from low to medium to high levels.[395] The higher likelihood of risks differentiates vulnerable data subjects from average data subjects.[396] A question here arises about the minimum likelihood level of incurring risks to other rights, freedoms, or general principles. Since the answer is subjective on a case-to-case basis, Malgieri suggests that the likelihood of risk must be medium to high, or in other words, higher than for the average data subjects.[397] Thus, the following subsections discuss the effect-based vulnerability of PWDs, in certain cases especially while using AI-based ATs. It looks at general principles, freedoms or rights that are impacted, violated, or likely to be violated, along with PWDs' privacy violations.

4.3.1 The UN Convention on the Rights of Persons with Disabilities (CRPD)

CRPD is often the tool that assists PWDs in realizing their rights and overcoming barriers.[398] It contains a few provisions worth noting in the context of AI-enabled ATs. These provisions impose certain obligations on the state (public) and private parties, such as data controllers and processors of these AI-based ATs, including protection of users' privacy. Looking at the CRPD's drafting Committee's discussions reveals that during drafting, they also considered privacy of PWDs in contexts other than information privacy.[399] Although the focus of this thesis is on information privacy, this right still protects other aspects, such as thoughts and opinions,

---

[393] Frédéric Mégret, "The Disabilities Convention: Toward a Holistic Concept of Rights" (2008) 12: 2 Int'l J of Human Rights 261.
[394] *Supra* note 286, ch 4 at 14.
[395] European Union Agency for Cybersecurity (EU body or agency), *Guidelines for SMEs on the security of personal data processing* (Publications Office of the European Union, 2016), §6.4.3.
[396] *Supra* note 286, ch 4 at 14.
[397] *Ibid.*
[398] "Laws | Free Full-Text | Protection for Privacy under the United Nations Convention on the Rights of Persons with Disabilities", online: <https://www.mdpi.com/2075-471X/6/3/10#B24-laws-06-00010%20%E2%80%A6>.
[399] *Supra* note 347.

religious beliefs, sexual data, and family.[400] Even the ECtHR has recognized PWDs as a vulnerable and marginalized group in society and found it consistent with CRPD.[401]

Unlike other international conventions, CRPD notably lists general principles in a stand-alone provision to guide state parties in drafting and implementing local laws to comply with the convention. As explained in the subsequent sub-sections, these general principles are closely connected to the privacy of PWDs, especially while using AI-based ATs.

4.3.1.1 Explicit privacy provisions under CRPD

CRPD, the convention targeted at promoting and protecting PWDs' rights, has two provisions dealing explicitly with the privacy and data protection of PWDs. These two provisions are Articles 22 and 31. The CRPD's provision for privacy protection builds on the *International Covenant on Civil and Political Rights* (ICCPR) (Article 17) by recognizing PWDs' specific barriers and risks. The Human Rights Committee (HRC) held that under Article 17 of ICCPR, the state needs to regulate the collection and holding of personal data by public and private authorities alike.[402] Additionally, under the provision, the data shall not be accessible to unauthorized parties, and PWDs shall have the right to rectification.[403] In addition to the elements covered under ICCPR, CRPD provides explicit protection for certain aspects of privacy. Most importantly, as per Article 31, states must "[c]omply with legally established safeguards, including legislation on data protection, to ensure confidentiality and respect for the privacy of persons with disabilities" while collecting statistical data.[404] People considered PWDs a neglected minority, prior to CRPD.[405] However, with CRPD and Article 31, there has been a substantial advancement in statistics and

---

[400] Frédéric Gilles Sourgens, "The Privacy Principle" (2017) 42 Yale J Int'l L 345 at 352.
[401] Delia Ferri and Andrea Broderick, "The European Court of Human Rights and the Human Rights Model of Disability: Convergence, Fragmentation and Future Perspectives." (2019) *European Yearbook on Human Rights* 261.
[402] HRC, General Comment No 16: Article 17 (Right to privacy) UN Doc HRI/GEN/1/Rev 1 (1994) para 5 [General Comment No 16 para 10].
[403] Ibid.
[404] *Convention on the Rights of Persons with Disabilities*, 12 December 2006, 61st sess, A/RES/61/106, art 31(1)(a).
[405] Department of Economic and Social Affairs, Disability, *Report of the Secretary-General on the Implementation of the World Programme of Action concerning Disabled Persons: The Millennium Development Goals and Synergies with other United Nations Disability Instruments*, UN DESA, 63rd sess, UN Doc A/62/157 (27 July 2007), para 17.

research data ensuring the maintenance and fulfilment of PWDs' rights.[406] This is a one-of-a-kind provision which was inserted in a human rights treaty for the first time.[407]

Article 22 explicitly protects general privacy and personal, health, and rehabilitation data. Mark C. Weber contends that article 22 is "substantive and calls for different treatment when the protections society generally affords are insufficient to guard privacy and reputational interests of those who have disabilities."[408] Irrespective of an explicit privacy protection provision, CRPD does not define the term 'privacy'. Examining the drafting process of CRPD reveals that Article 22[409] (then Article 14) underwent amendments which broadened its scope. The amendments added the phrase "correspondence or other types of communications" to "consider recent communication technologies."[410] Since the amendment, the term 'privacy' under Art 22 has evolved to cover technological advancements. Therefore, commentaries on Art 22 recognize the effect of these emerging technologies on PWDs.[411] PWDs greatly rely on ICT, including AI-based ATs, for social life, work, and everyday activities.[412] This greater reliance leads to the collection of more personal and sensitive data in digitized form and exposure to differential potential privacy risks.[413] With recent developments like IoT and AI (including AI-based ATs) new potential risks arise. For instance, where the technology lacks screen-based interfaces, providing notice to users becomes challenging, and data collection becomes ubiquitous.[414]

Moreover, another amendment in Article 22 was the addition of the phrase "regardless of place or living arrangements." The intention behind this was to cover various living circumstances of PWDs. The drafters emphasized protecting PWDs in every living arrangement and stated: "to protect the privacy of a person wherever she or he may be—be it in a home, in a camping trailer,

---

[406] Nora E Groce, "Disability, Poverty, Human Rights and the Need for Accurate Data to Promote Action" (2009) 3 Alter, European J of Disability Research 185.
[407] *Supra* note 347.
[408] *Supra* note 398.
[409] "Art. 22: No persons with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication, or to unlawful attacks on his or her honour and reputation. All persons with a disability have the right to the protection of the law against such interference or attacks."
[410] *Supra* note 347 at 608.
[411] *Ibid.*
[412] Jonathan Lazar and Michael Ashley Stein (eds), *Disability, Human Rights, and Information Technology* (U Penn Press, 2017), ch 12 [Jonathan Lazar, Brian Wentz, and Marco Winckler, "Information Privacy and Security as a Human Right for People with Disabilities"].
[413] *Supra* note 347 at 617.
[414] *Ibid.*

or within a family—not just in an institution."[415] This phrase imposes a duty on the state to ensure privacy protection in places or circumstances where the risk of arbitrary infringement is high. For instance, the ECtHR held that an institution which screened communication of people with a psychological disability violated their privacy rights.[416]

Furthermore, paragraph 2 of Article 22 is a testament to extra protection provided by the CRPD Committee for personal, health, and rehabilitation data of PWDs. The purpose is to prevent PWDs from discrimination or harm to individuals' ability to control their personal data or their portrayal in public. This provision influences the data protection regimes worldwide, especially the EU's GDPR.[417] The CRPD Committee has repeatedly expressed concerns about personal data, especially data disclosing health or disability status. Two examples of this are Denmark and Latvia. In Denmark, the Committee asked the state to protect patients by banning the practice of psychiatric hospitals sharing personal and private data of patients with third parties without patients' consent.[418] In Latvia's case, the Committee raised issues with the absence of safeguards to protect patients with certain diseases' privacy rights since this impacted such patients' access to services and employment.[419] Additionally, the Committee raised concerns about the inability of PWDs to contest the collection of their data by third parties without consent.[420]

The right to Privacy is not an absolute right and is subject to exceptions. However, as per Article 22, any interference with the right must not be unlawful or arbitrary. Despite the differences in privacy clauses of the ICCPR and CRPD, the test of lawfulness, proportionality, and legitimate purpose applies to interference with privacy.[421] While assessing proportionality of the interference with Article 22 privacy right, one must consider the disproportionate effect of technologies on PWDs. For instance, surveillance might be lawful and proportionate in general but not in the case of PWDs.[422] Thus, states shall ensure that PWDs do not have to choose forcefully between the

---

[415] "Enable - Fifth Session of the Ad Hoc Committee - Daily summary of discussions - 2 February 2005", online: <https://www.un.org/esa/socdev/enable/rights/ahc5sum2feb.htm>.
[416] *Herczegfalvy v Austria*, (1993) 15 EHRR 437, paras 87–91.
[417] *Supra* note 347.
[418] Committee on the Rights of Persons with Disabilities, *Concluding observations on the initial report of Denmark* (UN, 2014), paras 50–51 at 7, online: <https://documents.un.org/doc/undoc/gen/g14/194/60/pdf/g1419460.pdf>.
[419] *Supra* note 347 at 626.
[420] *Ibid*.
[421] *Ibid* at 620.
[422] *Ibid* at 621.

privacy protection and enjoying other rights guaranteed under international or domestic law.[423] The subsequent subsections discuss other rights affected by privacy violation.

4.3.2 Loss of autonomy

Loss of privacy links with the violation or loss or possibility of loss of other fundamental concepts or rights, such as autonomy. During the drafting of CRPD, the right to privacy was among the early drafted provisions because of its essentiality for protecting personal autonomy, which is considered a core concept of CRPD.[424] CRPD does not expressly define the term autonomy. However, the preamble's text of CRPD allows for a wide understanding of autonomy as the freedom to make one's own decisions and be in charge of one's life.[425] Lord Hoffman, in the case of *Campbell v MGN Ltd.*[426] stated that "what human rights law has done is to identify private information as something worth protecting as an aspect of human autonomy... the new approach ... focuses upon the right to control the dissemination of information about one's private life". Furthermore, in the same case, the Court referred to privacy as "the protection of the individual's informational autonomy." Thus, the case acknowledges the meaning of privacy in the informational age and equates privacy with informational autonomy.

To further understand the privacy and autonomy link in CRPD, the CRPD Committee did not adopt the suggestion to use 'self-determination' instead of autonomy. This was because the Danish Human Rights Institute highlighted that the former is generally a fundamental right used in relation to colonial countries, national minorities, and Indigenous people.[427] The Institute further noted during the second Ad hoc Committee session that autonomy embodies five interrelated rights.[428] One of these five rights was the 'right to privacy'. During discussions, the Committee acknowledged the vulnerabilities of PWDs because of technology by stating—"Issues of privacy

---

[423] Nicholas Caivano, "Inaccessible Inclusion: Privacy, Disclosure and Accommodation of Mental Illness in the Workplace" (2016) 5 Can J Human Rights 97 at 131.
[424] *Supra* note 347 at 607.
[425] Preamble part n: "(n) Recognizing the importance for persons with disabilities of their individual autonomy and independence, including the freedom to make their own choices".
[426] *Campbell v MGN Ltd* [2004] 2 AC 457. [the UK].
[427] "UN Enable - Ad Hoc Committee - Rights of Persons with Disabilities - Danish Institute for Human Rights Contribution (A/AC.265/2003/CRP/9)", online: <https://www.un.org/esa/socdev/enable/rights/a_ac265_2003_crp9.htm>.
[428] *Ibid*, ["right to personal development, to create ideas and goals for life; right to privacy; right to integrity, liberty and freedom from coercion; right to inclusion in community life; and right to participate actively in political processes"].

are also highly relevant for persons with disabilities whose dependence on technical and personal aids may lead to situations of vulnerability." Violation of privacy can undermine PWDs' autonomy by stripping them of control over their personal data. This control directly impacts independent decision-making about their lives, influencing human diversity and respect for individual differences (general principle under article 3 paragraph (d) of CRPD). Even the state parties to CRPD have recognized autonomy in the context of PWDs.

With the AI development, there is an exacerbated risk of loss of control over their personal data and the resultant loss of autonomy. Recent instances have revealed that AI can identify a user's disability status from online traces. For example, research observed that using a PWD's social media profile and activity, AI can infer if they are blind. [429] Another example is when researchers could identify if the user has Parkinson's disease from their mouse movements.[430] This identification can lead to creation of user profiles, which organizations can potentially use for various harmful purposes, including digital nudging, without the knowledge of the PWD.[431] This raises the question whether PWDs have control over their personal data, especially disclosure of their disability or health status.

This unintended disclosure of a disability of PWDs, especially hidden disability, also leads to loss of autonomy. A study revealed that PWDs were more concerned about the disclosure of their hidden disabilities than physical disabilities because of the stigma associated with hidden disabilities.[432] The term "hidden disabilities" includes a wide range of not-obvious disabilities, such as internal conditions like chronic pain, mobility disorder, autism spectrum, attention deficit hyperactivity disorder (ADHD), and dyslexia.[433] Recognizing such concerns, the Ontario Court of Appeal in Canada has also recognized the right to personal autonomy for people with mental health disabilities. It held that self-determination, dignity, and personal autonomy are equally significant

---

[429] M.R. Morris, et al., "With most of it being pictures now, I rarely use it: Understanding Twitter's evolving accessibility to blind users" (delivered at CHI '16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2016) online: < https://dl.acm.org/doi/10.1145/2858036.2858116>.
[430] M.R. Nario-Redmond, D. Gospodinov and A. Cobb, "Crip for a day: The unintended negative consequences of disability simulations" (2017) 62:3 Rehabilitation Psychology 324.
[431] Markus Weinmann, Christoph Schneider & Jan vom Brocke, "Digital Nudging" (2016) 58:6 Business & Information Systems Engineering 433.
[432] *Supra* note 430.
[433] Yang Wang & Charlotte Emily Price, "Accessible Privacy" in Bart P Knijnenburg et al, eds, *Mod Socio-Tech Perspect Priv* (Cham: Springer International Publishing, 2022) 293.

for people with mental health disabilities as for people with any physical disability.[434] Literature classifies disclosures into different categories—authorized disclosure, forced disclosure (students or employees seeking accommodation), selective disclosure (PWD disclosing only to AT and not a human), disclosure by others (a friend or family member disclosing without PWD's permission)[435], and unauthorized disclosure (disclosure by a third party or data controller without PWD's consent or knowledge). Use of AI could often lead to potential unauthorized disclosure.

In relation to PWDs, safeguarding personal and sensitive data, especially disability status and medical or health data, is essential in ensuring their dignity and autonomy.[436] The express actions of public or private actors, along with the design and implementation of the technology PWDs rely on, can compromise their privacy. These by-design privacy violations could also expose users to high risks or harms, such as discrimination.[437] This is evident from the CRPD Committee's emphasis on dignitary interest linked to privacy while condemning the display of children for 'medical or charity purposes.'[438] To conclude, potential privacy risks undermine PWDs' control over their personal data and affect their human or informational autonomy.

4.3.3 Freedom from discrimination and equal opportunity

The right to privacy is closely linked with the right to freedom from discrimination, or the non-discrimination principle, a fundamental right in most jurisdictions. As the HRC pointed out in the international human rights landscape, it is a "basic and general principle relating to the protection of human rights."[439] Even though certain international conventions do not recognize disability as a ground of discrimination, state parties, including Canada and the EU, do. For

---

[434] "16. Consent and capacity | Ontario Human Rights Commission", online: <https://www.ohrc.on.ca/en/policy-preventing-discrimination-based-mental-health-disabilities-and-addictions/16-consent-and-capacity>.
[435] MacDonald-Wilson, et. al., "Disclosure of mental health disabilities in the workplace" (2011) *Work Accommodation and Retention in Mental Health*, 191–217.
[436] Land et al, *supra* note 347.
[437] Jeroen van den Hoven and John Weckert, *Information Technology and Moral Philosophy*, eds. (Cambridge: Cambridge University Press, 2008), ch 16 at 322 [Mary Flanagan, Daniel C Howe, and Helen Nissenbaum, 'Embodying Values in Technology: Theory and Practice'].
[438] Committee on the Rights of Persons with Disabilities, Concluding Observations on the Initial Report of *Armenia,* UN Doc (8 May 2017) CCPR/C/ARM/CO/1, paras 37–38 at 8.
[439] CCPR General Comment No 18: Non-*discrimination,* UN OHCHR (1989) para 1, online: <http://www.refworld.org/docid/453883fa8.html>.

example, the EU Charter of Fundamental Rights, which was implemented post-CRPD, lists disability as a discrimination ground.[440]

The CRPD text incorporates the principle of non-discrimination across multiple provisions, including the preamble, general principle, stand-alone non-discrimination provision under Article 5, right to education (Article 23), health (Article 25), and employment (Article 27). Article 2 of CRPD defines discrimination as "any distinction, exclusion or restriction on the basis of disability which has the purpose or effect of impairing or nullifying the recognition, enjoyment, or exercise, on an equal basis with others, of all human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field. It includes all forms of discrimination, including denial of reasonable accommodation". The term 'reasonable accommodation' is further defined as "necessary and appropriate modification and adjustments not imposing a disproportionate or undue burden, where needed in a particular case, to ensure to persons with disabilities the enjoyment or exercise on an equal basis with others of all human rights and fundamental freedoms."

There are a few things to note in these definitions. Firstly, the definitions imply that non-discrimination, instead of creating new rights, reaffirms the existing human rights. Secondly, it covers both civil and political rights, as well as economic, social, and cultural rights. Thirdly, the definition covers both direct and indirect discrimination. Lastly, CRPD is the first international treaty that explicitly includes denying reasonable accommodation as a discriminatory practice. However, in order to seek accommodation, PWDs often have to disclose personal or sensitive data about their disability. In some cases, employers or organizations may use the reasonable accommodation method to obtain information about PWDs' health status and risks for discriminatory purposes or deny claims for failure to accommodate.[441] For instance, in the *ACT* class action case, students or applicants were subject to discrimination because of seeking accommodation to write the university entrance exam.[442]

---

[440] EU, *Charter of Fundamental Rights of the European Union*, [2000] OJ 2000/C 364/01 at 13, Article 21(1) of the Charter: "[a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

[441] Anita Silvers and Michael Ashley Stein, "An Equality Paradigm for Preventing Genetic Discrimination" (2002) 55 Vulnerability and L Rev 1341, 1366, online: <SSRN: https://ssrn.com/abstract=337720 or http://dx.doi.org/10.2139/ssrn.337720>.

[442] *See* above: 3.2.3 The "sensitivity" of PWDs' data collected by AI-based ATs.

The use of AI-based ATs or ATs leads to processing of personal and sensitive data.[443] Keeping in mind the privacy and data protection concerns, if unauthorized parties breach or expose this data, it affects or violates the right to non-discrimination of PWDs. This is evident from the discrimination practices against PWDs observed in employment, education, insurance and other areas of life. A workshop participant revealed having been barred from purchasing life insurance because of her anxiety disorder.[444] This is one example of when disclosure of disability led to discrimination against people with mental health issues. Thus, disclosing disability can risk PWDs' healthcare and employment, especially in countries which closely tie medical insurance to employment.[445] Furthermore, a study found various grey zones in the handling of user data for assistive and clinical purposes.[446] These encompass safeguarding user-generated datasets and use of data by third parties. This is concerning because insurance companies may, upon access, utilize such data to the detriment of patients, such as increasing cost of premiums or terminating insurance coverage.[447]

As noted in the sensitive data section, PWDs' violation of the right to privacy could impact other rights, such as the right to equality, freedom from bias and discrimination, and the right to education. The prime reason for this interconnection is the right to control data about oneself incorporated under the right to privacy. This means a PWD's ability to control data about their disability status. Since disclosure of disability status has been shown in the past to be a reason for bias, discrimination, and stigma, the right to privacy acts as a safeguard to limit this disclosure. This disclosure, for instance, could lead to the rejection of job applications or termination of employment of PWD with ongoing treatment or associated stigma.[448] Additionally, people with non-visibly discernable disabilities could face stigma and discrimination upon disclosure of their disability.[449]

As discussed under the trade-off subsection, for PWDs, disclosure of disability is mostly not a choice. Given the features like receiving accommodation or social welfare benefits require

---

[443] *See* above 3.2.3. The "sensitivity" of PWDs' data collected.
[444] Institute, *supra* note 284.
[445] *Ibid*.
[446] Wangmo et al, "Ethical concerns with the use of intelligent assistive technology", *supra* note 346.
[447] *Ibid*.
[448] Jessica L Roberts, "Protecting Privacy to Prevent Discrimination" (2015) 56 William & Mary L Rev 2097.
[449] Land et al, *supra* note 347.

them to disclose their disability status. Especially with the use of technology like AI-based ATs, PWDs not just lose control over disability status but also over other sensitive and personal information. Also, AI has the capability to recognize patterns and infer disability status even if the user has not explicitly disclosed it. Therefore, the risk of invasion of privacy is further increased with the involvement of AI. A study with people with autism (PWA) found that AI's integration in ATs for PWA showed issues of bias, ethics and cybersecurity.[450] This bias resulted from the replication of societal bias in the AI algorithm. The researchers observed that if the training data contained biases, then the AI system could unintentionally perpetuate stereotypes, show biased results, and not cater to the diverse needs of PWA. Moreover, with the use of AI to assist PWA, problems related to fairness and accessibility can arise. This is primarily because not every user (here, PWA) could have the same opportunity to benefit from AI interventions. This could exacerbate the existing differences between users.

Fear of privacy violation can create barriers that prevent PWDs from participating in certain aspects of public life. This resistance directly affects their right to access, inclusion and principle of equal opportunity.[451] The principle of equal opportunity closely links with non-discrimination, and they are collectively called twin pillars of CRPD. Other general principles, such as equality between men and women, respect for the evolving capacities of children with disabilities, and respect for the right of children with disabilities to preserve their identities, closely link with the equal opportunity principle.

4.3.4 Accessibility

According to the CRPD Committee, accessibility is a precondition to enjoying other rights under CRPD,[452] including the right to independent living and equal participation in society.[453] The availability of accessible information is crucial to fulfilling a variety of rights, such as the right to education and freedom of expression.[454] Accessibility under CRPD directly links to promoting the

---

[450] "Breaking Barriers—The Intersection of AI and Assistive Technology in Autism Care: A Narrative Review - PMC", online: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10817661/>.
[451] "Rights of people with disabilities - Canada.ca", online: <https://www.canada.ca/en/canadian-heritage/services/rights-people-disabilities.html>.
[452] General Comment No 2: Article 9 (Accessibility*)*, UN Convention on the Rights of Persons with Disabilities, 11th sess, UN Doc CRPD/C/GC/2 (2014), para 36 at 11.
[453] *Ibid.*
[454] *Ibid*, *p*ara 37, 38, and 44 at 11 and 12.

principle of full and effective participation in society (Article 3(c)). The CRPD Committee considers this a disability-specific reaffirmation of the right to access and precondition to the enjoyment of civil, political, social, cultural and economic rights of PWDs.[455] Furthermore, the Committee views the denial of accessibility as discriminatory.[456] In case of AI-based ATs, accessibility means right to access surrounding environment, the AT, and privacy or related information in an accessible manner.

Accessibility is not a mere legal compliance requirement; instead, it is fundamental in protecting the privacy and security of PWDs. If the environment is not accessible, then PWDs resort to either human or technological assistance. Both of these affect PWDs' autonomy and pose separate sets of potential privacy risks. For instance, self-checkout kiosks are mostly not accessible and PVI often rely on the checkout option. If they seek a stranger's (store employee) assistance or use a visual AT, they are at risk of potential privacy concerns linked to personal data collection. The purpose of AI-based ATs or ATs is to increase access to the world for PWDs. However, this can bring its own challenges, such as an increased risk of being noticed by attackers or potential privacy risks.

Ironically, the technology built to increase access to the world or to have more independence is not accessible to the majority of people who need it. Only 5% of the population has access to ATs in low-income countries and 15% in middle-income countries.[457] Additionally, if privacy tools, information or technologies are not accessible to PWDs, it impacts data protection and privacy.[458] Many ATs have complex user interfaces that are not accessible to PWDs, thereby making it difficult to control privacy settings.[459] Moreover, privacy policies, terms of service or other privacy notices are often inaccessible, which in addition to lack of transparent information raises questions about informed consent.[460]

Privacy and accessibility go hand-in-hand. Privacy violations impact access and equal opportunity for PWDs. For instance, a privacy breach of personal data collected by AI-based ATs

---

[455] *Ibid*, para 1 at 1.
[456] *Ibid.*
[457] World Intellectual Property Organization, *supra* note 53 at 21.
[458] Wang & Price, *supra* note 433.
[459] *Ibid.*
[460] *See* above 3.2.2. How "informed" is the informed consent.

whose purpose is to increase accessibility, will affect both rights of PWDs: right to privacy and accessibility. The CRPD Committee emphasizes that compliance with ICT accessibility requirements should not affect the realization of other rights, including the right to privacy. *The Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled* (the Marrakesh Treaty) mandates privacy protection while enabling accessibility. The treaty mandates states to create copyright exceptions for creating accessible format copies of printed works for print-disabled people or organizations.[461] Article 8 of the Treaty obligates states to ensure the promotion of accessibility without violating the privacy of individuals.

4.3.5 Intersectionality and Compounded Vulnerabilities

PWDs often belong to multiple marginalized groups, such as racial minorities, economically disadvantaged, gender minorities, or LGBTQ+. These intersecting identities can compound their vulnerability to potential privacy risks raised by AI-based ATs or AI in general.[462] The compounded effect can lead to worse privacy breach consequences for such users. For instance, AI could subject disabled women of colour to discrimination because of the intersectionality of three vulnerable factors: race, gender, and disability. As discussed in Luna's vulnerability theory, in today's tech world, vulnerability results from a combination of micro and macro factors identified as layers.[463] In this example, three additional factors make disabled women of colour more vulnerable to potential risks. Moreover, a study found that intersectional marginalized identities of PVIs influenced their privacy and security practices.[464] This means that most PVIs had other aspects of marginalized identities in addition to disabilities, including gender or race. The term intersectionality was first used in the context of women of colour to study structures of race, gender, class, and sexuality.[465] Since then, various scholars have used the term

[461] Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired, or Otherwise Print Disabled, WIPO (27 June 2013) VIP/DC/8 REV.
[462] KW Crenshaw, 'From Private Violence to Mass Incarceration: Thinking Intersectionally about Women, Race, and Social Control' (2012) 59 UCLA L Review 1418.
[463] *Supra* note 286, ch 3 at 49.
[464] Wang & Price, *supra* note 433.
[465] Crenshaw, Kimberle, "Mapping the margins: Intersectionality, identity politics, and violence against women of color" (1991) 43:6 *Stanford L Rev* 1241.

in different disciplines, including critical disability. The concept of intersectionality has been a recent discussion in human-computer interface (HCI) to better understand people's interactions.

Another compounding factor is the economic state of PWDs. 80-90% of the PWD population in developing countries are unemployed, and the unemployment percentage is around 50-60% in industrialized countries.[466] 20% of the world's poorest population has some form of disability.[467] These statistics portray the problematic economic state of the PWD population. Economic considerations play a significant role in how privacy violations affect users. Such violations affect an individual's financial capacity to fight legal battles in case of privacy breaches and education level-which might affect understanding of privacy notices. Thus, economic conditions can compound to a PWD's vulnerability. Another example of compounded vulnerability is the case of people with rare diseases. With AI's ability to re-identify users from anonymized data, people with rare diseases are more likely to experience greater potential privacy risks when they provide data to AI systems or engage in research studies assessing AI technology.[468] Thus, intersecting factors of PWDs compound their vulnerability to potential privacy risks.

4.4 Summary

This chapter examined the unique privacy interests of PWDs using AI-based ATs and what renders PWDs especially vulnerable to potential privacy risks. Luna's layered vulnerability theory is the most suitable for the discussion of PWDs in the data protection and privacy sphere. While other users of AI technology share a level of vulnerability, PWDs face an elevated privacy risk due to the amalgamation of additional layers of vulnerability. The reasons discussed under "processing-based" vulnerability are applicable to all data subjects; however, the trade-off, lack of choice, purpose of use of ATs, the issue of informed consent, and the nature of highly sensitive and personal data collected by AI-based ATs exacerbate the vulnerability of PWDs. Further, reasons discussed under the "effects-based vulnerability" are specific to PWDs and make them

---

[466] "Disability and Employment | United Nations Enable", online: <https://www.un.org/development/desa/disabilities/resources/factsheet-on-persons-with-disabilities/disability-and-employment.html>.
[467] "Factsheet on Persons with Disabilities | United Nations Enable", online: <https://www.un.org/development/desa/disabilities/resources/factsheet-on-persons-with-disabilities.html>.
[468] Morris, *supra* note 192.

particularly vulnerable. This phase discussed the likelihood of violation of other fundamental rights or freedoms, or general principles provided under international (CRPD) and domestic laws. The next chapter examines the AI, data protection, and privacy framework in Canada through the lens of protection provided to PWDs.

5 Analysis of legal framework of privacy in Canada through a vulnerability lens

The previous two chapters examined the privacy concerns faced by PWDs while using AI-based ATs and their unique privacy interest or exacerbated vulnerability to privacy risks, respectively. Now, the question is whether the current Canadian data protection legal framework protects PWDs' privacy interests or responds to their higher vulnerability to privacy risks. Thus, I will analyze the current federal private sector data protection law—PIPEDA and the proposed Bill C-27 through the vulnerability lens in this chapter. The aim of this analysis is two-fold. First, to determine if there is any provision specifically addressing PWDs or vulnerable data subjects. Second, to highlight gaps in legislation that could pose high privacy risks for data subjects, and especially for PWDs. This assessment draws on Dr Gianclaudio Malgieri's analysis in his book *Vulnerability and Data Protection Law* to examine the role of vulnerability in the wording of GDPR.[469]

Before proceeding with an analysis of the data protection or privacy laws in Canada, I briefly highlight in this paragraph the background of privacy as a right in the international sphere and its adoption in Canada. Privacy as a right emerged in 1948 through the actions of the UDHR. Post UDHR, the UN promulgated the ICCPR. States that signed the ICCPR soon incorporated the right to privacy in their constitutions or under other legislations. Canada has ratified UDHR and ICCPR and as a result includes the right to privacy under different laws. Another relevant convention is CRPD, which aims to protect the interest of PWDs, including their privacy interest. Along with privacy protection, CRPD has been a foundational ground for examining the opportunities and challenges AI presents for PWDs. Canada has been a party to CRPD since 2010 and has made continuous efforts to advance the interests of PWDs in different spheres of life. Canada also aligns its domestic laws with the SDGs, which supplement and promote the objective of CRPD. SDG 10 especially focuses on equal treatment of PWDs and the creation of a society which is free from discrimination.[470] Such international conventions and goals require member

---

[469] *Supra* note 286, ch 4.

[470] "Sustainable Development Goal 10: Reduced inequalities - Canada.ca", online: <https://www.canada.ca/en/employment-social-development/programs/agenda-2030/reduced-inequalities.html>; Even, the UN High-level Panel on Digital Cooperation stated that technological development should aim at the promotion of SDGs.

states, including Canada, to implement domestic laws that promote objectives and provisions of these conventions and goals.

Canada offers privacy protection through a combination of laws. These include, *inter alia*, the public and private sector privacy and data protection legislations, along with the Canadian Charter of Rights and Freedoms (Charter) and human rights code. Even the Canadian courts have recognized the right to privacy in various cases. For instance, the Supreme Court of Canada (SCC) noted in the case of *R. v. O'Connor* that the right to privacy is "an essential aspect of [an individual's] liberty in a free and democratic society."[471] The SCC in the same case further noted that any unwarranted disclosure of personal data "is an invasion of the dignity and self-worth of the individual" because "once [privacy is] invaded, it can seldom be regained."[472] In another case, the SCC divided the concept of privacy into three categories: bodily, territorial, and informational.[473] Canadian Courts consider privacy as a quasi-constitutional right because the Charter entrench some of its elements.[474] Irrespective of the debate about whether privacy is a fundamental right, a quasi-fundamental or a general right under Canadian law, it is one of the necessary rights for individuals to participate or function in the current technological era.

5.1 Current Framework

The private sector privacy and data protection framework in Canada comprises federal and provincial laws. PIPEDA is the federal private sector privacy law. Three provinces, British Columbia, Alberta, and Quebec, have their personal private sector data laws deemed substantially similar to PIPEDA. Whereas in the rest of the provinces and cases where personal information crosses provincial or national borders, PIPEDA applies. Apart from these laws, various sectorial laws, including health data, employment-related data and financial data laws, collectively form the data protection legal framework of Canada.

Health data, out of other sectorial laws, is often a topic of discussion when PWDs use AI-based ATs. Since this thesis focuses on personal data, health data and its regulation are out of its scope. Without an in-depth analysis, it is important to note that, in Canada, provincial health data

---

[471] *R v O'Connor* [1995] 4 S.C.R. 411, para 119.
[472] *Ibid.*
[473] *Royal Bank of Canada v Trang*, 2016 SCC 50. para 49.
[474] Canadian Charter of Rights and Freedoms, s 2(a), 7- 8, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

protection laws govern health information. Only four provinces' health information laws, namely, Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia, are "substantially similar to PIPEDA."[475] For example, Ontario has *the Personal Health Information Protection Act (PHIPA)*,[476] and that is substantially similar to PIPEDA. According to the Frequently Asked Questions (FAQs) released by the Information Privacy Commissioner of Ontario (IPCO), custodians[477] and their agents[478] do not have to comply with PIPEDA to the extent they collect, use and disclose personal health information within Ontario.[479] This limits the scope of protection under PHIPA to Ontario. Other provinces also have their health data laws; however, the federal legislature has not recognized them as substantially similar to PIPEDA. Therefore, PIPEDA still applies in those provinces subject to certain exceptions.

5.1.1 PIPEDA: the private sector federal privacy law

5.1.1.1 Data subject

In the GDPR context, Malgieri analyzes the definition of data subject under GDPR and finds that there is no bifurcation of data subjects based on different personal conditions.[480] Thus, there are no categories of data subjects and no distinction between the average data subjects and vulnerable data subjects,[481] except that GDPR provides additional data protection for children. Through a statutory interpretation of the wording of GDPR, he concludes that the definition of the average data subject is similar to an average consumer.[482] Similarly, PIPEDA does not provide a separate classification for vulnerable data subjects. Unlike GDPR, PIPEDA does not even explicitly address children's data separately. Despite no differentiation between data of children

---

[475] Office of the Privacy Commissioner of Canada, "Summary of privacy laws in Canada", (15 May 2014), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/> Last Modified: 2018-01-31.
[476] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A
[477] *Ibid*, s 2 ["agent": "in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated"].
[478] *Ibid*, s. 3 [who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph].
[479] "Frequently Asked Questions: Personal Health Information Protection Act | Information and Privacy Commissioner of Ontario", online: <https://www.ipc.on.ca/en/resources-and-decisions/frequently-asked-questions-personal-health-information-protection-act> [page 4].
[480] Supra note 287, ch 5-6.
[481] *Ibid, c*h 2 at 101 and ch 5.
[482] *Ibid.*

and adults in the wording of PIPEDA, the Office of Privacy Commissioner (OPC) has considered children's data as "sensitive information" and guided organizations to seek parental consent to process children's data under 13 years.[483] Thus, PIPEDA considers a data subject as an average data subject irrespective of vulnerability factors such as disability.

5.1.1.2 Data categorization

AI-based ATs process various kinds of data. Thus, it becomes crucial to understand the categories of data governed by PIPEDA and to determine if any of those categories consider the vulnerability of individuals.

Firstly, PIPEDA applies to the collection, use, and disclosure of personal data during commercial activities in Canada.[484] The definition of "personal information" under PIPEDA includes "information about an identifiable individual."[485] Canadian courts have held that information is personal if there is a possibility of identification of an individual based on the information, either alone or in combination with other available information.[486] Thus, identifiable feature is a key factor. Moreover, in the case of *R v. Tesling,*[487] the SCC emphasized the importance of protecting data that forms the "biographical core of personal information" including "intimate details of the lifestyle and personal choices of the individual."[488]

Sensitive data belong to the second type often given additional protection. For GDPR, Malgieri analyzes whether "special categories of data" (also called sensitive data) consider different data subjects, especially vulnerable data subjects.[489] He observes that international sources such as the first international legal formulations of sensitive data protection[490] and the UN

---

[483] Office of the Privacy Commissioner of Canada, "Protecting the privacy rights of young people", (28 November 2023), online: <https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20231128/> Last Modified: 2023-11-28.
[484] PIPEDA, *supra* note 208, art 4.
[485] *Ibid, a*rt 2.
[486] "PIPEDA Findings #2020-004: Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia - Office of the Privacy Commissioner of Canada", online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/>; Gordon v. Canada (Minister of Health), 2008 FC 258; Ontario (Attorney General) v. Pascoe, (2002) 22 C.P.R. (4th) 447 (Ont. C.A.), aff'g Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner), [2001] O.J. No. 4987, 16 C.P.R. (4th) 460 (Ont. Div. Ct.).
[487] *R v. Tesling* 2004 SCC 67 at para 25.
[488] *R v. Plant* [1993] 3 SCR 281 at para 293.
[489] *Supra* note 347, ch 5 at 122.
[490] N Lindop (ed), Report of the Committee on Data Protection (H.M.S.O., London, 1978).

Guidelines for the Regulation of Computerized Personal Data Files in 1990[491] acknowledge special protection for sensitive data to guard against harmful discrimination. The Council of Europe *Modernized Convention 108 on Automatic Processing of Personal Data* recognizes data as sensitive whenever there is a "potential risk of discrimination or injury to an individual's dignity or physical integrity, where the data subject's most intimate sphere, such as his or her sex life or sexual orientation, is being affected."[492] Additionally, GDPR in Recital 52 and 71 acknowledges that the sensitive information "merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms," including discrimination risk. Malgieri notes that these justifications of sensitive data align with the concept of vulnerability in the context of data protection.[493] The concept of vulnerability notes two phases of vulnerability because of data privacy risks: processing-based and effects-based vulnerability.[494] Effect-based vulnerability's explanation establishes risk to fundamental rights and freedoms, including freedom from discrimination. Thus, he notes that the notion of sensitive data protection, at least in part, focuses on protecting vulnerable data subjects,[495] including PWDs. However, the GDPR definition while broad, does not cover all situations of vulnerability.

In the Canadian context, PIPEDA does not cover specific vulnerable group under the sensitive data. Neither PIPEDA nor any provincial data protection laws define the term "sensitive data." However, certain provisions under PIPEDA related to sensitive information collection requires express consent[496] and higher levels of protection.[497] Unlike PIPEDA, Quebec's provincial law considers information as sensitive if it requires a higher level of reasonable expectation of privacy. Quebec also has a stricter consent requirement that mandates consent to be explicit, freely given, informed, and specific to purposes.[498] Other than legislation, the OPC has

---

[491] "Guidelines for the Regulation of Computerized Personal Data Files | Refworld", online: <https://www.refworld.org/policy/legalguidance/unga/1990/en/13761>."likely to give rise to unlawful or arbitrary discrimination".

[492] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1 January 1985, ETS No. 108.

[493] *Supra* note 347 at 124.

[494] *Ibid*, ch 4; *see* above ch. 3.

[495] *Supra* note 347 at 124.

[496] *Royal Bank of Canada v.* Trang, 2016 SCC 50 at para 34.

[497] *Supra* note 208, principle 4.7 and 4.7.2; s. 7.2(1)(a) and 7.2 (2)(a); and s. 10.1(8).

[498] "Canada - Data Protection Overview", (26 January 2024), online: *DataGuidance* <https://www.dataguidance.com/notes/canada-data-protection-overview>.

an Interpretation Bulletin (Bulletin) that outlines categories of sensitive personal information.[499] The Bulletin states that sensitive information poses special risks to an individual associated with the use, collection and disclosure of such information.[500] It assesses the sensitivity in relation to potential harms or risks resulting from information breaches. Examples of certain kinds of data considered sensitive according to the Bulletin include health data, financial data, and personal information affecting an individual's reputation and causing embarrassment and harm. The explanation by OPC does not indicate a focus on fundamental rights or freedoms, such as freedom from discrimination, or factors directly linked with vulnerable individuals. Moreover, this Bulletin merely offers guidance and are not legally binding.[501]

The third category of data is de-identified or anonymized data. PIPEDA does not cover anonymized data; whether it covers de-identified data remains unanswered.[502] Thus, when AI-based ATs claim to be using PWDs' data after de-identifying or anonymizing it, do they still need to comply with data protection requirements related to personal and sensitive data processing? To assess application of PIPEDA, the "reasonable expectations" or "reasonably foreseeable" test is applicable. According to the test, information is not anonymous "if it is reasonable to expect that an individual can be identified from the information in issue including when combined with information from sources otherwise available".[503] Especially with AI, there is a continuous discussion whether personal data can ever be fully de-identified.[504] AI has been able to re-identify data or reveal personal information from anonymized data using its algorithms in certain real-life cases.[505] The risk of revealing personal data increases in case of people with rare diseases. Thus,

---

[499] Office of the Privacy Commissioner of Canada, "Interpretation Bulletin: Sensitive Information", (16 May 2022), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/> Last Modified: 2022-05-16.

[500] *Ibid.*

[501] "PIPEDA interpretation bulletins - Office of the Privacy Commissioner of Canada", online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/>.

[502] House of Commons, Canada, *Standing Review of the Personal Information Protection and Electronic Documents Act (PIEDA): Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics* (May 2007), online: <https://www.ourcommons.ca/Content/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-e.pdf>

[503] "CPPA: problems and criticisms – anonymization and pseudonymization of personal information | McCarthy Tétrault", online: <https://www.mccarthy.ca/en/insights/blogs/techlex/cppa-problems-and-criticisms-anonymization-and-pseudonymization-personal-information>.

[504] Latanya Sweeney, "k-Anonymity: A Model for Protecting Privacy" (2002) 10:5 Intl. J. Uncertainty, Fuzziness and Knowledge-Based System 557.

[505] *Supra* note 347, ch2.

non-application of the Act to anonymized or de-identified data in case of AI can pose risks for data subjects, especially vulnerable individuals.

5.1.1.3 Profiling and automated decision-making

The AI risks, including bias and discrimination, increase multifold with user profiling by AI systems and the practice of automated decision-making. Unlike the GDPR[506], neither PIPEDA nor any Canadian provincial data protection law, has an express provision addressing automated decision-making. However, in the case of *Clearview AI*, the court noted that PIPEDA can address some problematic challenges related to automated technologies that use personal information.[507] It further noted that PIPEDA is principle-based[508] and technologically neutral,[509] thus, even the general provisions apply to automated decision-making. The *Directive on Automated Decision-Making* (Directive) released by the Government of Canada are only applicable to federal institutions using automated decision making in administrative decisions.[510] Thus, private entities using automated decision making are out of its scope.

Whereas, GDPR covers, *inter alia*, automated decision-making practice under Article 22(1), which states "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her…" The Article 29 Data Protection Working Party (WP29)[511] provides further clarification to determine the meaning of "significantly affects" under Article 22. According to this clarification, a decision "significantly affects" when—it affects the circumstances, behaviour or choices of the data subject, has a permanent or prolonged impact on the data subject, or leads to exclusion or discrimination of data subjects.[512] Therefore, the right to

---

[506] "Art. 22 GDPR – Automated individual decision-making, including profiling", online: <https://gdpr-info.eu/art-22-gdpr/>.
[507] *Ibid.*
[508] Principle based means it follows a broad framework of principles as opposed to the rules based, which involves detailed and descriptive rules.
[509] "Using privacy laws to regulate automated decision making | McCarthy Tétrault", online: <https://www.mccarthy.ca/en/insights/blogs/techlex/using-privacy-laws-regulate-automated-decision-making>.
[510] Treasury Board of Canada Secretariat, "Guide on the Scope of the Directive on Automated Decision-Making", (18 July 2024), online: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-scope-directive-automated-decision-making.html>.
[511] An advisory body established by the EU under the GDPR [Data Protection Directive 95/46/EC].
[512] EU, "Guidelines on Automated individual decision- making and Profiling for the purposes of Regulation 2016/679", online: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

not be subject to automated decision making protects privacy rights and also protects against AI risks like discrimination. Furthermore, discussions about Article 22 reveal that it offers specific protection to children and other vulnerable groups.[513]

GDPR protects vulnerable individuals against automated decision making and potential privacy and AI risks. Canada lacks a similar express protection for vulnerable groups. AI-based ATs, often produced by private entities, use technologies like FRT and other automated decision-making algorithms, which involve the use of personal and sensitive data of PWDs. As per the real-life examples, automated decision-making has shown results of bias and discrimination against PWDs.[514] Thus, using such algorithms for PWDs can create potential AI risks. In such a scenario, the absence of express regulation under PIPEDA and non-applicability of the Directive create potential data privacy and AI risks for vulnerable individuals, including PWDs.

5.1.1.4 Consent

Under PIPEDA, consent is the legal basis for processing personal information unless an exception applies. Teresa Scassa, Canada Research Chair in informational law and policy, notes that OPC is reluctant to shift away from the consent-based model under PIPEDA.[515] This is because of the belief that consent empowers individuals to control their personal information.[516] However, data protection in the age of AI with notice-consent model focused legislation, like PIPEDA, becomes challenging. The Centre for Information Privacy Leadership (CIPL) notes that using consent as a legal basis to process personal information, especially sensitive data, seems impractical for AI.[517] For instance, seeking and withdrawing consent could result in incomplete or non-representative training data.[518] The right to withdraw consent has been a big issue for AI

---

[513] *Ibid* at 22.
[514] *Supra* note 126 at 252.
[515] Florian Martin-Bariteau & Teresa Scassa, eds., *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021), ch 5 at 11 [AI and Data Protection Law].
[516] For years there have been opposing views about whether Canada should adopt a risk-based approach similar to the EU. The risk-based model prioritizes the assessment of risks or the likelihood of risk before data processing. It makes obtaining consent as a legal basis more onerous, leading data controllers to often explore other legal bases for processing data. But the notice-consent based model relies on consent as the primary legal basis for processing personal information.
[517] CIPL, "Response by the Centre for Information Policy Leadership to the Information Commissioner's Office's Consultation on the Lawful Basis for Web Scraping to Train Generative AI Models" (1 March 2024), online: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_-_ico_consultation_on_the_lawful_basis_for_scraping_data_for_generative_ai__mar_2024_.pdf>.
[518] *Ibid* at 3.

because AI developers collect data from multiple sources to create datasets, and consent withdrawal requests hamper the functioning of those datasets. If AI developers do not meet these withdrawal requests, there is a risk of potential privacy breach. Furthermore, Malgieri notes that the use of consent as a lawful basis for data processing can be an issue in the case of vulnerable people like PWDs due to accessibility challenges.[519]

As noted above, GDPR provides additional protection for children, especially in the case of obtaining consent; however, PIPEDA lacks an explicit additional protection for children. Working party formed under GDPR (WP29) while discussing consent for children data in its guidelines on consent states: "[c]ompared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed".[520] The term 'especially children' does not equate to 'only children'. Moreover, Recital 43 expressly mentions that consent shall not be a valid legal ground for data processing when there is a clear imbalance between the data subject and controller.[521] WP29 further explains consent as invalid if "there is any element of compulsion, pressure or inability to exercise free will."[522] Additionally, Article 7(4) states "when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[523] As established in the previous chapter, there exists a power imbalance between PWDs as data subjects and data controllers while using AI-based ATs or ATs. Thus, after reading these explanations and interpretations from the vulnerability lens, GDPR's non-reliance on consent when there is a power imbalance seems appropriate. This prevents vulnerable groups from consenting to sharing their data because of a lack of choice.

Conversely, PIPEDA has no additional measures foreseen under consent while seeking a vulnerable individual's (PWD's) consent. I do not intend to pursue the notice-consent model (followed by Canada) vs the risk/harm-based model (followed by the EU) debate. However, in the

---

[519] *Supra* note 347 at 113.
[520] European Data Protection Board, "Guidelines on Consent under Regulation 2016/679", online: < https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> at 25.
[521] O Lynskey, The Foundations of EU Data Protection Law (Oxford University Press, 2015) 213.
[522] *Supra* note 520 at 9.
[523] GDPR, *Supra* note 161, art 7(4).

case of vulnerable individuals experiencing power imbalance, consent as a legal basis to process data does not seem a satisfactory or adequate approach due to the power imbalance.

5.1.1.5 Privacy by Design

The GDPR obligates data processors and controllers to adopt privacy-by-design practices when determining the means and the time of processing.[524] Whereas in Canada, a report released before the House of Commons suggested the introduction of privacy-by-design as a central principle under PIPEDA; however, PIPEDA still does not have privacy by design as a principle.

Vander Hof and Lievens note that the fundamental purpose of privacy by design is to protect data subjects; therefore, adopting a vulnerability-centric approach is necessary whenever the processing includes data of vulnerable data subjects.[525] This approach can strengthen privacy practices and the development of responsible AI-based ATs that deal with the personal and sensitive data of PWDs. On the other hand, privacy by design could overlap with other data protection principles. For instance, if privacy by design requires de-identification of data at source, this can lead to huge data collection and create risks to communities and potential non-compliance with the data minimization principle.[526] I acknowledge that data protection in the AI age might be insufficient by solely relying on the traditional privacy by design approach; however, absence of a binding provision for that weakens privacy protection framework.

5.1.1.6 Access and Transparency

The right to access data promotes the transparency principle. The Canadian courts have favoured data subjects' right to access by maintaining a high threshold for denying access. For instance, the Federal Court in a 2016 case denied a bank's (data controller and processor) argument that access to the personal data sought is confidential commercial information. In another case, the court noted that the bar to deny an access request is very high under s. 9(3)(b) of PIPEDA.[527]

---

[524] *Supra* note 286, ch 6 at 151.
[525] Van der Hof Simone and Eva Lievens, "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR" (2018) 23:1 Communications L, online: <https://ssrn.com/abstract=3107660>,
[526] *Supra* note 516 at 15.
[527] *Supra* note 208, s. 9(3)(b) [allows an organization to deny a person's request for access to their personal information if it is "confidential commercial information"].

However, the court has permitted denial requests in extreme situations, such as where disclosing could reverse engineer the simple algorithm.[528]

Canada's private sector law caters more to an average non-disabled data subject in terms of the right to access, transparency, and openness of information. Similar to the GDPR, PIPEDA under Article 10 requires data controllers to make personal information available in an alternative format for people with sensory disability. Alternative format means any format that allows the data subject to access information. However, section 10 is limited in scope and only covers sensory disabilities. Disabilities can be of various kinds, including cognitive, physical, and mental. Thus, the phrase "people with sensory disabilities" leaves out other forms of disabilities. OPC released a *Policy on Accommodating Clients with Disabilities* in 2015. Irrespective of covering all forms of disabilities, this policy only applies to complaints under PIPEDA. It is unclear if this also covers access requests. Though of limited scope, an express provision for accessibility, specific to PWDs, is a step in the right direction because lack of accessibility often leads to privacy risks.[529]

Additionally, PIPEDA requires organizations to be open or transparent about their data processing practices. This openness or transparency principle applies to the collection, use, and disclosure of information.[530] Quebec's new law has taken a further step by requiring more detailed disclosures, including information about third parties or categories of third parties with whom data controllers will share personal information.[531] Privacy advocates have long asked for transparency requirements in AI systems, especially in algorithmic decision-making.[532] Discriminatory or biased outcomes against PWDs are currently difficult to challenge and examine due to lack of transparency. Transparency in the training data or other functions of an AI system would permit examining and challenging the AI system outcomes.[533] The federal privacy law should broaden its transparency principle similar to Quebec's new law.

---

[528] Office of the Privacy Commissioner of Canada, "News Release: Privacy Commissioner releases finding on a bank's refusal to release credit score - PIPEDA Case Summary #2002-39", (22 February 2002), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/pipeda-2002-039/>.
[529] *Supra* note 286, ch 2.
[530] *Supra* note 208, Principle 8 – Openness.
[531] *Supra* note 498.
[532] Rashida Richardson, Jason Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice" (2019) 94 N.Y.U. L. Rev. at 192.
[533] *Supra* note 516 at 18 [Chapter 14 of this volume, Wolfgang Alschner].

To promote the transparency principle, GDPR has a broader provision than PIPEDA. GDPR requires the information to be provided in a "transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child." Thus, GDPR offers additional protection to children's privacy rights. Interpretation provided by *Data Protection on the Protection of Individuals with regard to the Processing of Personal Data (WP29) Guidelines on Transparency* clarifies that this provision also covers other vulnerable situations, especially vulnerable adults.[534] Canada could incorporate a similar provision strengthening transparency principle and the right to access.

The reason behind promoting the openness and transparency requirement is the expectation that if data subjects stay informed, they can exercise their other rights. These other rights include the right to consent, object, rectify, erase and others. Policy makers can strengthen this promotion by providing criteria for assessing whether privacy notifications are transparent & accessible for different data subjects.[535] Thus, increasing transparency and openness can help PWDs protect and exercise data protection rights.

5.1.1.7 Enforcement and Accountability

The current enforcement and accountability obligations under PIPEDA are weak. Scassa points out that Canada's enforcement and accountability requirement suffers because of its ombuds model,[536] and calls PIPEDA "toothless" legislation.[537] There have been continuous efforts to provide the OPC with the power to impose penalties and pass orders.[538] A serious problem is that there is no private right of action under PIPEDA, and the Act is enforceable in the Federal Court and not in a provincial court, as held by the Ontario Court of Appeal in *Del Giudice v.*

---

[534] European Data Protection Board, "Article 29 Working Party - Guidelines on transparency under Regulation 2016/679" online: <https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en>. [WP29 on Transparency, 9: "if a data controller is aware that their goods/services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects."]

[535] *Supra* note 286 at 182.

[536] Jennifer Stoddart, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA" (21 October 2005), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2005/omb_051021/>.

[537] Teresa Scassa, "The Failure of Privacy Law" (14 March 2013) online (blog): < https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=123:the-failure-of-privacy>.

[538] *Supra* note 516 at 18.

Thompson.[539] The plaintiff in this case alleged data breach and misuse of data under PIPEDA. While denying the statutory claims, the Court observed that under PIEPDA, first, the Privacy Commissioner (PC) investigates and prepares a findings and recommendations report, either by acting on a complaint or initiating a complaint. Once PC generates the finding report, thereafter, the federal court hears a case.

Contra Canadian framework, the GDPR has a stronger enforcement feature which permits the imposition of hefty fines in case of non-compliance with the law.[540] It also has other enforcement and accountability provisions. For instance, the data breach notification provision under GDPR mentions "categories of data subjects." WP29 explains this phrase in its Guidelines about data breach notification as "depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers."[541] WP29 further states that the concept of vulnerable data subjects is based on the 'higher risk of harm' notion.[542]

This indicates that, unlike PIPEDA, GDPR focuses on vulnerable groups, including PWDs, in the case of data breaches. However, despite of its inadequacies, Canada's pending Bill C-27 (discussed later) provides a stronger enforcement mechanism, which could assist vulnerable data subjects in seeking remedial action.

5.1.1.8 Erasure and modification/rectification

The right to erasure and rectification strengthens the autonomy and control of data subjects over their personal information.[543] It also mitigates the power imbalance between data subjects and controllers.[544] For vulnerable groups, including PWDs, this becomes a crucial right, because

---

[539] Del Giudice v. Thompson, 2021 ONSC 5379 (CanLII), at para 159.
[540] *Supra* note 162, art. 83(5).
[541] European Data Protection Board, "Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01" online: <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_en> at 14.
[542] *Ibid.*
[543] Bartolini and L Siry, "The Right to Be Forgotten in the Light of the Consent of the Data Subject" (2016) 32 Computer Law & Security Review 218 at 223.
[544] J Ausloos, *The Right to Erasure in EU Data Protection Law* (Oxford University Press, 2020).

of the higher probability of impairment of autonomy and informational self-determination in their case.[545]

PIPEDA has a limited right to erasure. It imposes a duty under Principle 4.5 on the data controller to destroy, erase or anonymize data once it is no longer required for purposes for which it was collected.[546] Further, if an individual proves the inaccuracy or incompleteness of personal information, the organization must modify the information. This could include correction, deletion, or addition of information.[547] OPC noted in the Draft OPC *Position on Online Reputation* that data subjects can seek the erasure of their information and amendment to their personal information. Also, the word "shall" under Principle 4.5 makes it a mandatory obligation and enforceable in court under Section 14 PIPEDA. However, this right has its shortcoming under PIPEDA. First, it does not mandate data controller to inform third parties of erasure requests to which it has disclosed the data. Secondly, PIPEDA does not provide the right to erasure in case personal data is required for the purposes for which it was collected.[548]

On the contrary, GDPR provides the right to erasure (also called the right to be forgotten) and permits withdrawal of consent. The explanation of this right under GDPR states that this right helps children remove personal information they once consented to share without fully knowing the risks.[549] This highlight that the GDPR, *inter alia*, aimed at protecting at least one specific vulnerable group—children, through this right. Similar to GDPR, Canada needs to expressly expand its right to erasure under the private sector federal privacy legislation. This will especially assist PWDs to have more autonomy and control over their data and vulnerability to potential privacy risks.

5.1.1.9 Right to object or withdrawal of consent

Malgieri notes that the right to object assists vulnerable groups in two ways. First, when the data subject is incapable of understanding and deciding whether to accept the conditions of

---

[545] A Trites, "Black Box Ethics: Why the Rights to Explanation and to Be Forgotten Are Ethically Critical Components for Vulnerable Populations" (PhD Thesis, Université Saint-Paul/Saint Paul University, 2019) online: <http://ruor.uottawa.ca/handle/10393/39126>.
[546] *Supra* note 208, Schedule 1, Principle 4.5.3.
[547] *Ibid*, Schedule 1 principle 4.9.5.
[548] BLG, "The right to erasure of personal information in Canada: Between fact and fiction" (28 May 2021), online: <https://www.blg.com/en/insights/2021/05/the-right-to-erasure-of-personal-information>.
[549] *Supra* note 162, Recital 65.

data processing. In such cases, consent as a legal basis to process data becomes unfair, and the data controller or processor often opts for other legal bases, including public interest or legitimate interest. In the absence of consent as a legal basis, data subjects lose the right to withdraw consent. Thus, the right to object assists in stopping data processing at the data subject's will irrespective of the legal basis of processing. Secondly, this promotes the fairness principle by fair balancing the position of data controller and data subjects.[550] This fair balancing limits power imbalance which often exacerbates vulnerability of vulnerable groups, including PWDs and assists in fair data processing.

Under GDPR, this is the only right which mentions "on grounds relating to his or her particular situation…"[551] The GDPR text does not clarify if it considers the permanent or temporary conditions of vulnerability as a "particular situation". However, the Court of Justice of the European Union (CJEU) in the case of *Google Spain* observed that to understand the consequences of data processing on an individual's particular situation, one shall consider "the sensitivity for the data subject's private life".[552] Thus to assess a particular situation, the focus is on the sensitivity of an individual rather than the duration of their vulnerability. Reading this interpretation in the context of PWDs using AI-based ATs, which involves collection of data of sensitive nature, demonstrates that this right indirectly covers the higher vulnerability of PWDs.[553] Unfortunately, PIPEDA does not contain an express provision granting data subjects the right to object. Moreover, upon withdrawal of consent by the data subject, PIPEDA does not require data controllers or processors to notify third parties to which it had disclosed the data subject's information. Since PWDs are subject to this power imbalance dynamic and an express right to object would assist in reducing that imbalance.

To conclude, we can observe a vulnerability approach in certain upcoming legislations, especially related to AI risk regulation. However, Canada needs to focus equally on the vulnerability approach in the privacy context. To compensate for the void of a law governing

---

[550] D Clifford and J Ausloos, "Data Protection and the Role of Fairness" (2018) 37 Yearbook of European Law, 177.
[551] *Supra* note 162, art 21.
[552] JEU Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014].
[553] *Supra* note 286.

privacy rights related to AI, commissioners are issuing guidance for adapting existing laws to new circumstances. During the pendency of Bill C-27 (discussed later), OPC along with 13 other privacy regulators, released *Principles for responsible, trustworthy and privacy-protective generative AI technologies* (Principles).[554] The Principles are not binding on regulators but are likely to affect the future generative AI space. These principles ensure fairness in generative AI systems by evaluating training datasets, ensuring there is no amplification or replication of old biases or the introduction of new biases. Notably, the principles expressly impose responsibility on developers, providers and organizations using generative AI to identify and prevent risks to vulnerable groups. It further states that data controllers should take measures such as privacy impact assessments (PIAs) to mitigate risk to vulnerable populations. The principles do not define 'vulnerable groups'; however, they mention that it includes "children and groups that have historically experienced discrimination or bias."[555] Literature shows that PWDs have historically been subject to systematic discrimination. Thus, by referring to the OPC explanation, we can interpret that vulnerable groups include PWDs as well.

5.2 Pending law - Bill C-27

Bill C-27, also called the *Digital Charter Implementation Act*, if passed would significantly amend the private sector privacy legal framework in Canada. The Bill proposes three pieces of legislation:

- Consumer Privacy Protection Act (CPPA)
- Personal Information and Data Protection Tribunal Act (PIDPTA)
- Artificial Intelligence and Data Act (AIDA)

CPPA would repeal and replace the parts of the current PIPEDA and provide authority to impose penalties for its violation. PIDPTA would establish an administrative tribunal for hearing appeals related to the decisions of the OPC under CPPA. Lastly, AIDA would establish obligations regarding AI systems (discussed broadly below). Since Bill C-27 is still pending, this thesis focuses on amendments made until December 31, 2023.

---

[554] Office of the Privacy Commissioner of Canada, "Principles for responsible, trustworthy and privacy-protective generative AI technologies" (7 December 2023), online: <https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/#fn1>.
[555] *Ibid.*

5.2.1 Consumer Privacy Protection Act (CPPA)

CPPA will reform the private sector data protection law in Canada. It focuses on the privacy rights of individuals concerning their personal information. It additionally governs the commercial needs of organizations to collect, use and disclose personal information for appropriate or reasonable purposes.[556]

CPPA adds a list of new consent requirements. Earlier these requirements were a part of non-binding guidelines issued to obtain meaningful consent. This would make the process and requirement of consent more rigorous. Further, the proposed Act includes various provisions in the text. For instance, now CPPA explicitly obligates data controllers and processors to maintain a privacy management program, rather than listing this as a CSA Model Code principle.[557] The proposed act under an analogous provision empowers OPC to create "no-go zones." These measures, though not specifically aimed at PWDs, would certainly improve data protection by ensuring better organizational accountability in place. However, unlike GDPR, CPPA retains the notice-consent model.

According to the Innovation Minister's remarks, the bill's 'biggest legacy' is the express extra protection provided to minors. Even though OPC has considered minors' data as sensitive, incorporating an express provision designating children's data as sensitive and recognition of this vulnerable group is a step in the right direction.[558] This would provide additional protection to children's data and impose certain disposal obligations on the data controller or processor. It would be interesting to note if the legislature would interpret the sensitive data provision to cover other vulnerable groups, like the GDPR provision interpretation. However, CPPA still neither defines the term 'sensitive information' nor the criteria to assess the sensitivity of information.

The new bill expands the role and powers of the PC, permitting her to adjudicate violation of the Act and prosecute violators. It also permits a private cause of action against organizations that contravene CPPA. As a result, affected individuals, PC, or complainant would have the right

---

[556] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act, 2022)*, 1st sess, 44th Parl, 2021, Part 1 CPPA, s. 5(1).
[557] The Canadian Standards Association (CSA) ten privacy principles are based on the OECD Guidelines and serve as the basis of Canada's PIPEDA.
[558] *Supra* note 555, Part 1 CPPA s. 2(2).

to file a private claim against the organization before either the Federal Court or a Superior Court of a province. This provision expands the scope of plaintiffs permitted to bring an action and the jurisdiction of the court. This would be in addition to common law actions, for instance, claims under intentional tort. The proposed mechanism to enforce rights or seek claims would avoid complications faced under tort claims. For instance, in the *Del Giudice* case, establishing a violation under tort law was challenging.[559] Moreover, organizations would have the right to appeal the findings of the PC with the establishment of the Personal Information and Data Protection Tribunal. This proposed mechanism bolsters the enforcement and accountability principle. The act increases the powers of the OPC, and penalty amounts for non-compliance to further improve enforcement. However, the market frowns upon these hefty penalties. Some people believe this would hinder the functioning of companies in Canada and impact foreign companies' and countries' trade with Canada. From PWDs' perspective, penalties would ensure that data controllers sufficiently protect user data under the law; however, this could also hinder innovation in the AI-based ATs' space.

CPPA extends the rights of data subjects by adding rights of disposal (right to deletion) of their data and transfer (data portability) of personal information between organizations, subject to restrictions. These rights could help PWDs have greater control over their personal and sensitive data for while using AI-based ATs. However, it remains uncertain whether certain types of AI systems can ever fully delete data.[560]

To cater the AI concerns, CPPA requires organizations to add details of any automated decision-making system used to make "predictions, recommendations, or decisions about individuals that could have a significant impact on them" in their privacy policies. Upon an individual's request for further information, organizations must explain the source and type of information collected, factors that led to that prediction, and other information. CPPA provides a broader definition of 'automated decision making' including technology where human

---

[559] *Supra* note 538.

[560] Antonio A. Ginart, et. al., "Making AI Forget You: Data Deletion in Machine Learning" (33rd Conference on Neural Information Processing Systems (NeurIPS 2019), Vancouver, Canada), online: < https://proceedings.neurips.cc/paper_files/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf >.

intervention is present.[561] This algorithmic transparency is a significant step; however, the Act does not address the data scrapping issue discussed in the Clearview AI case, wherein defendants scraped the data of millions of Canadians off the internet.[562] Similar to PIEPDA, Bill C-27 does not mandate privacy-by-design framework,[563] thereby, continuing the lacuna of an express mandate.

Furthermore, CPPA retains the accessibility provision under PIPEDA. It notes that "alternative format, with respect to personal information, means a format that allows an individual with a sensory disability to read or listen to the personal information." This definition mentions only reading and listening and leaves out understanding the personal information. Similar to PIPEDA, this is a limited definition because, according to direct interpretation, it leaves out people with cognitive impairment or other forms of disabilities. In conclusion, CPPA does not necessarily have a vulnerability approach, however, certain provisions could assist in better protection of the personal data of users, including PWDs.

5.2.2 AIDA

AIDA, if passed, would establish obligations related to the use of anonymized data in AI systems, and the design, development and making available for the use of AI systems and high-impact AI systems. The proposed AIDA does not cover privacy safeguards even if privacy is a noteworthy part of AI. This Act focuses more on the regulation of AI risks. The expectation is that the existing privacy legislation and the proposed CPPA will cover privacy regulation. Scassa exclaims that this is problematic for a few reasons.[564] First, Canada, apart from Quebec, has a highly scattered privacy law framework. Second, despite strong data protection legislation, even the EU has incorporated certain limiting provisions for surveillance activities under the EU AI

---

[561] "S. 2(1) CPPA: *automated decision system* means any technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique. (*système décisionnel automatisé*)"

[562] Teresa Scassa, "AI, Human Rights, and Canada's Proposed AI and Data Act" (19 March 2024) online (blog): <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=380:ai-human-rights-and-canadas-proposed-ai-and-data-act&Itemid=80>.

[563] Section 100 of the Bill would introduce a new s. 9.1 of Québec's private sector data protection law which would require anyone collecting personal information when offering a technological product or service "must ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned." See Bill 64, An Act to modernize legislative provisions as regards the protection of personal information (1st Sess., 42nd Leg. Quebec, 2020).

[564] *Supra* note 561.

Act. Thus, the Act should have addressed privacy obligations, especially in the context of AI. Linking the focus of the Act back to the two phases of vulnerability discussed in the third chapter of this thesis: processing-based and effects-based. This Act caters to or attempts to prevent both processing and effects-based vulnerability. Whereas CPPA primarily deals with processing-based vulnerability.

AIDA divides AI systems into different layers based on their impact and only applies to the high-impact (HI) systems. To promote the objective of analytical transparency, HI systems must publish transparency description on a public website in plain-language description of the system. This description shall enlist "a) how the system is intended to be used; (b) the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make; (c) the mitigation measures established under section 8 in respect of it; and (d) any other information that may be prescribed by regulation". To further the accountability principle, persons responsible for the AI system must conduct an impact assessment to assess if it is an HI system.

As per many, the objective of creating an agile regulation that would flexibly respond to rapid changes in business and technical domains[565] led to AIDA missing the mark for various reasons. The primary reason is that it leaves a lot of details to be decided under the regulations. Act's lack of interoperability with the EU and the US is a problem not just from the Canadian perspective but also for world governance of AI. Furthermore, similar to CPPA, AIDA also permits the imposition of hefty penalties in case of contravention of the law. Again, this might hinder AI innovation, including AI-based ATs, negatively impacting PWDs. Unlike the EU's AI Act, which has created 'no-go zones', meaning prohibiting AI activities falling under that zone, AIDA has no such categorization. Scassa rightly notes that from a human rights perspective, we need to consider if regulation of such AI systems is the right approach or whether there should be limits on their use and deployment.[566]

---

[565] Torgeir Dingsoyr et al, "A decade of agile methodologies: Towards explaining agile software development" (2012) 85:6 J of Systems and Software 1213 at 1214.
[566] *Supra* note 561.

The Minister of Innovation, Science and Industry (ISED)[567] proposed certain amendments in December 2023 to AIDA in response to heavy criticism of Bill C-27. A significant step was the inclusion of a definition of "high-impact systems." The definition covers, *inter alia*, AI systems used for—employment, service eligibility checks, healthcare and emergency services, and biometric analysis to assess an individual's behavior or state of mind. Moreover, the Act explicitly excludes AI-enabled medical health devices (a significant part of AI-based ATs) from the HI system definition because that comes under the jurisdiction of Health Canada to regulate. Moreover, the Act does not apply to AI-enabled medical devices not involved in international or interprovincial trade and commerce. This leaves out a significant part of AI-based ATs from the scope of AIDA. No application of AI targeted regulation under AIDA might negatively impact PWDs, such as, in terms of seeking remedy for breach. Furthermore, questions like what would convert a general-purpose AI system to HI system remains unanswered. For instance, AI-based ATs that use speech recognition technology are under general purposes AI systems category; it remains unclear if they will become HI systems if they use sensitive data of PWDs.

5.3 Conclusion to the legal framework discussion

The current and proposed pending laws do not specifically consider PWDs under their provisions. Neither of the regimes considers vulnerable individuals' data, especially PWDs, separately. The accessibility provision under PIPEDA, which requires organizations to provide information in an alternate format, does not cover all forms of disabilities. The current Canadian legal framework does not explicitly cover the most recognized vulnerable group under GDPR: children. However, the pending bill includes express provisions to protect children's data. This would also assist children with disabilities who extensively use AI-based ATs in their personal lives and for educational purposes. Since this group faces additional layers of vulnerabilities (minority and disability), this step will protect them from additional risks. This also leaves room for incorporation of other vulnerable groups for certain additional protections under the proposed bill. Furthermore, challenges in this new AI era arise because of the absence of express regulations for automated decision-making and the lack of strong enforcement and accountability provisions.

---

[567] Minister of Innovation, Science and Industry, online: <https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf>.

However, the pending bill contains provisions expressly addressing these aspects, among others. To note, this bill has faced heavy criticism for its shortcomings and lack of interoperability with other jurisdictions' AI laws, mainly the EU's AI Act. The analysis of the pending bill in this chapter was limited because of its evolving nature and this thesis's limited scope to PWDs.

It is important to note that Canada's private sector privacy law, PIPEDA, came into existence before the internet boom in the 2000s, let alone the subsequent waves of big data and AI. The approach back then was more focused on balancing the privacy interests of individuals and businesses. However, with the increased risks to the rights and freedoms of data subjects because of emerging technologies, we see more consumer protection-focused approach with the pending CPPA.

Privacy in Canada exists in an extensive legislative framework, including data protection legislation, Charter rights, criminal law, tort law, and human rights. The reason for seeking or suggesting express rights under data protection law is to ensure that seeking remedy is easier. If the new bill creates a stronger enforcement mechanism, then express provisions would mandate the PC while considering a complaint to follow a vulnerability approach. The following epilogue discusses some solutions or recommendations promoting this vulnerability approach.

6 Conclusion

This section summarizes the findings of three different objectives of this thesis in relation to the use of AI-based ATs by PWDs. It additionally offers brief suggestions related to issues discussed while analyzing those aims.

The first aim of this thesis was to understand the privacy concerns faced by PWDs while using AI-based ATs. Findings of my research revealed that the privacy risks faced by PWDs are not a separate set of new risks; instead, these risks exist in the use of any AI technology in general. What distinguishes the case of PWDs is their heightened vulnerability while using AI technology that relies on personal and sensitive data. The third chapter, while analyzing the specific privacy and associated risks that arise from using AI-based ATs, discussed implications of data protection principles. This chapter concluded that developers must comply with data protection principles in case of AI development to ensure development of responsible AI-based ATs for PWDs.

One of the principles discussed in this chapter was the accountability (organizational accountability) principle, which forms the core of privacy, data protection regulation and compliance. To strengthen compliance with the accountability principle, data controllers and processors should take measures to mitigate privacy risks for vulnerable individuals,[568] including PWDs.[569] This concept has become more prominent in the private sector with the rapid use of AI. CIPL rightly notes that this is equally crucial for AI governance[570] and proposes seven core elements to organizational accountability: leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement.

---

[568] ME Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability" (2019) 92 Southern California Law Review 15.
[569] *Ibid.*
[570] Centre for Information Policy Leadership, "Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework" (February 2024), online: < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_feb24.pdf>.

Figure 6: A diagram of the Accountability framework with 7 core elements proposed by CIPL[571]

These measures could vary based on the specific vulnerability. For instance, the data controller could conduct periodic audits to assess any discriminatory practice against individuals at risk of discrimination or arrange specific privacy disclosure measures or consent collection mechanisms with PWIDD.[572] Furthermore, timely revision or assessment of such measures is necessary to stay abreast of emerging risks.[573] Thus, it becomes the duty of organizations to be accountable for their AI practices and data processing.

The second aim was to understand what exacerbates PWDs' vulnerability to potential privacy risks, especially while using AI-based ATs. The fourth chapter, while answering this, concluded that neither the universal nor the traditional vulnerability theory is responsive in the current data-driven world. While the universal vulnerability approach ignores the injustices that vulnerable groups face, the traditional vulnerability approach makes application of law too fragmented and challenging for organizations to comply with. Thus, a middle-ground "layered vulnerability" theory proposed by Luna best suits the needs of our data-driven world. The

---

[571] *Ibid.*
[572] Malgieri, *supra* note 286; Chalghoumi et al, "Information Privacy for Technology Users With Intellectual and Developmental Disabilities", *supra* note 317.
[573] Van der Hof and Eva Lievens, "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR" (2018) 23:1 Comm L; KC Montgomery and Jeff Chester, "Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework" (2015) 1:4 European Data Protection L Rev 277.

additional layers, such as personal characteristics (disability), social factors (systemic oppression or accessibility issues), and economic factors together exacerbate the vulnerability of PWDs in the world of technology, especially with AI-based ATs or ATs. The thesis divided the reasons for exacerbated vulnerability of PWDs into two sets: processing-based and effects-based. The processing-based set discussed reasons that are equally applicable to general data users but exacerbate the vulnerability of PWDs to privacy risks. These included reasons such as the trade-off PWDs make between privacy and independence or convenience, lack of choice in the case of using AI-based ATs, the purpose of use of ATs, the issue of informed consent, and the nature of highly sensitive and personal data collected by AI-based ATs. The effects-based part discussed reasons more specific to PWDs. These included rights, freedoms or principles affected by privacy violation, such as loss of autonomy, discrimination and lack of equal opportunity, lack of accessibility, and compounded vulnerability. Thus, privacy risks in the case of PWDs are not merely limited to privacy violations, they also affect other rights and freedoms of PWDs.

To address the issue of informed consent and accessibility discussed in the fourth chapter, organisations should make privacy policies more accessible. They can do this by notifying users in a manner readable by web browsers or machines. To do so, they would have to use computer, mobile or other technology as an intermediary. Such an intermediary would first understand a user's privacy preferences and then manage that user's preferences while interacting with websites or devices. As an alternative, organizations could write privacy policies in a way that optimizes automation. For instance, they could train AI models like ML to read, understand, and classify information from various privacy policies.[574] Regulators could further use such a model to create auditing tools or visualization or accessibility tools to assist users. The legislature could also adopt regulations to standardize privacy policies which would assist in creating transparency or automation tools.[575] These measures can include provisions related to transparency requirements, privacy-by-design, and others ensuring informed consent.

---

[574] Lisa Austin, "Who decides? Consent, meaningful choices, and accountability — Schwartz Reisman Institute" (22 December 2020), online: <https://srinstitute.utoronto.ca/news/austin-consent-meaningful-choice-accountability>.
[575] *Ibid.*

Another issue discussed in the fourth chapter is providing consent on a take-it-or-leave-it basis. Drawing inspiration from a paper analyzing privacy and independence in AI-based AAL,[576] AI-based ATs could provide PWDs the choice to intentionally opt for or against the sharing of their data. This could be done through two approaches. First, designing the AI-based AT system in a way that permits PWDs to switch on or off the data-sharing feature. PWD participants in a study also preferred the installation of video-based ATs in a way where they could control the on and off features and decide the data collection period.[577] Under the second approach, instead of giving blanket consent, PWDs provide granular consent where they may choose "what data to share with whom for what purpose for every single application."[578] As researchers suggest, consent in AT should not follow the blanket consent system. Instead, organizations should regularly review it with users providing the opportunity to opt-out at their will during any stage, irrespective of inconvenience to developers.[579] For instance, Oasis Labs partnered with Nebula to enable its data subjects to control their genomic data (sensitive personal information). Oasis verifies the user's permission every time it uses that genomic data, and Nebula further provides users access to data processing reports.

The third research aim was to analyze the current legal framework in Canada, note if there are any provisions specifically addressing PWDs or vulnerable data subjects, and highlight gaps in legislation that could pose high privacy risks for data subjects, especially for PWDs. Analysis of the current federal private sector privacy law—PIPEDA revealed that it does not provide sufficient protection to PWDs given their exacerbated vulnerability to privacy risks. It only contains one explicit provision addressing PWDs – Section 10, which mandates that information shall be provided in an alternative format for people with sensory disability. Even this provision does not cover all kinds of disabilities. Moreover, the proposed bill does not have provisions specifically targeted at PWDs. PIPEDA currently has many gaps in the legislation that pose high privacy risks to data subjects. Since the privacy risks are higher and more serious in the case of

---

[576] Mujirishvili et al, "Acceptance and Privacy Perceptions Toward Video-based Active and Assisted Living Technologies", *supra* note 331.
[577] *Ibid*.
[578] Hartmann, Primc & Rubeis, "Lost in translation?", *supra* note 322; This could be a challenge with AI often because of a lack of transparency in its operation.
[579] J Perry, S Beyer and S Holm, "Assistive technology, telecare and people with intellectual disabilities: ethical considerations" (2009) 35:2 J of Med Ethics 81.

PWDs, these gaps amplify their vulnerability to these risks. Comparing PIPEDA's provisions with GDPR's provisions, the thesis found that GDPR has more provisions that consider the vulnerability of data subjects.

To protect rights of data subjects including PWDs better, legislation should provide data subjects with more express control over their personal information. For instance, California's privacy law provides an explicit right to opt-out and obligates organizations to inform data subjects of this right. The objective is to inform data subjects of their rights and to put a majority of the onus on organizations to protect user data. The focus of legislation should be to inform users of the actions they can take to control their data, instead of merely knowing how their data is being managed.[580] This would reduce the power imbalance problem. Additionally, the legislation should focus on increasing knowledge, skills, and awareness of PWDs, their caregivers and organizations to empower greater self-advocacy.[581]

This section offered some suggestions for better protection of PWDs' privacy rights, especially while using AI-based ATs or AI in general. However, detailed solutions were beyond the scope of this research. Further research is required to propose detailed and feasible solutions. In addition to new, practical solutions, the following questions warrant further investigation:

1. Whether PWDs need special/additional protection under the privacy legal framework. If yes, should the umbrella term "vulnerable individuals" explicitly encompass PWDs under the privacy legal framework, or should the legislation expand its additional protection beyond children alone to other vulnerable groups?
2. Whether Canada should adopt a risk-based approach as opposed to the current notice-consent approach, given the increased risks to vulnerable individuals, including PWDs, with technological advancement.
3. Whether, to what extent and in what sense the trade-off made by PWDs between privacy rights and independence or convenience they gain while using AI-based ATs is fair. Or, is that a useful conceptual framework to use?

---

[580] *Supra* note 358.
[581] Khanlou, Nazilla et al, "Protection of Privacy of Information Rights among Young Adults with Developmental Disabilities" (2018) 16:3 Int'l J Mental Health Addiction 545–572.

To conclude, a "privacy first" approach to AI innovation can help build trust with the user base while considering privacy as the absolute first priority.[582] From a practical real-world approach, it is crucial to find a balance between permitting organizations to access data for AI innovation and privacy protection. Scientists and researchers[583] often highlight the difficulties in accessing and using data for ATs, precision medicine and other purposes. In AI's case, we need a balance between the right to privacy and the requirement to process sensitive personal information to prevent AI risks such as marginalization and bias.[584] This is because prohibiting data processing of vulnerable groups' sensitive personal data might deepen the AI bias. Moreover, we also need to consider commercial realities along with human rights protection. Future developments should aim to protect the right to privacy while also attempting to prevent AI risks such as bias, discrimination and marginalization.

---

[582] Tarini Kaur Dang, "Why Privacy-First Approach Is Critical For Data-Based Innovation?" (27 May 2021), online: <https://www.forbes.com/sites/taarinikaurdang/2021/05/27/why-privacy-first-approach-is-critical-for-data-based-innovation/>.

[583] "Breaking down barriers: Exploring the role of equity in the future of precision medicine" conference at SICKKids that I attended in person on 18th September 2023.

[584] Sebastião Barros, *Vulnerable People, Marginalization, and Data Protection Symposium Report: Brussels Privacy Symposium* (Brussels: The Future of Privacy Forum & Brussels Privacy Hub 2022) online: <https://fpf.org/wp-content/uploads/2023/03/FPF-Brussels-Privacy-Symposium-2022-R3.pdf>.

BIBLIOGRAPHY

Legislation

1. Accessible Canada Act, S.C. 2019, c. 10
2. *Ontario Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A
3. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5

Bill

1. Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act, 2022)*, 1st sess, 44th Parl, 2021, to enact the *Artificial Intelligence and Data Act, Consumer Privacy Protection Act*, and the *Personal Information and Data Protection Tribunal Act*.

Jurisprudence

1. *R v Dyment*, [1988] 2 S.C.R. 417
2. *R v. Plant* [1993] 3 SCR 281
3. *R v. Tesling* 2004 SCC 67
4. *Royal Bank of Canada v. Trang* [2016] 2 SCR 412
5. *Del Giudice v. Thompson* 2021 ONSC 5379

International Material

1. *Americans with Disabilities Act of 1990*, 42 USC
2. *Bloom v. ACT*, Inc., Case No.: CV 18-6749-GW-KSx
3. *Convention on the Rights of Persons with Disabilities*, 12 December 2006, 61st sess, A/RES/61/106
4. *Dudgeons v. The United Kingdom* (1981) ECHR A59 7525/76, [1981] ECHR 5
5. EU, Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 1

6. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

7. *International Covenant for Civil and Political Rights,* 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976, accession by Canada 19 May 1976).

8. OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: Organisation for Economic Co-operation and Development, 2002).

9. "Transparency and explainability (OECD AI Principle) - OECD.AI", online: <https://oecd.ai/en/dashboards/ai-principles/P7>.

10. "UN Enable - Ad Hoc Committee - Rights of Persons with Disabilities - Danish Institute for Human Rights Contribution (A/AC.265/2003/CRP/9)", online: <https://www.un.org/esa/socdev/enable/rights/a_ac265_2003_crp9.htm>.

11. Department of Economic and Social Affairs, "Transforming our world: the 2030 Agenda for Sustainable Development", online: <https://sdgs.un.org/2030agenda>.

Secondary Material – Articles (Journals and Conferences)

1. Ahmed, Tousif et al, "Understanding the Physical Safety, Security, and Privacy Concerns of People with Visual Impairments" (2017) 21:3 IEEE Internet Computing 56–63.

2. Akter, Taslima et al, "Privacy Implications of Artificial and Human Intelligence Assistive Tools for Visually Impaired People" (2019).

3. Akter, Taslima et al, "Shared Privacy Concerns of the Visually Impaired and Sighted Bystanders with Camera-Based Assistive Technologies" (2022) 15:2 ACM Trans Access Comput 11:1-11:33.

4. Akter, Taslima, Bryan Dosono & Tousif Ahmed, "'I am uncomfortable sharing what I can't see': Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications".

5. Bariffi, Francisco Jose, "Artificial Intelligence, Human Rights and Disability" (2021) 26:2 Pensar - Rev Ciênc Juríd 14–1.

6. Bartolini and L Siry, "The Right to Be Forgotten in the Light of the Consent of the Data Subject" (2016) 32 Computer Law & Security Review 218 at 223.

7. Beach, Scott et al, "Disability, Age, and Informational Privacy Attitudes in Quality of Life Technology Applications: Results from a National Web Survey" (2009) 2:1 ACM Trans Access Comput 5:1-5:21.

8. Bragg, Danielle et al, “The FATE Landscape of Sign Language AI Datasets: An Interdisciplinary Perspective” (2021) 14:2 ACM Trans Access Comput 1–45.

9. Chalghoumi, Hajer et al, “Information Privacy for Technology Users With Intellectual and Developmental Disabilities: Why Does It Matter?” (2019) 29:3 Ethics Behav 201–217.

10. Colonna, Liane, “Legal and regulatory challenges to utilizing lifelogging technologies for the frail and sick” (2019) 27:1 Int J Law Inf Technol 50–74.

11. Faisal, Kamrul, “Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective” (2023) 28:1 Commun Law Policy 67–97.

12. Freitas, Maurício Pasetto de et al, “Artificial Intelligence of Things Applied to Assistive Technology: A Systematic Literature Review” (2022) 22:21 Sensors 8531.

13. Hartmann, Kris Vera, Nadia Primc & Giovanni Rubeis, “Lost in translation? Conceptions of privacy and independence in the technical development of AI-based AAL” (2023) 26:1 Med Health Care Philos 99–110.

14. Hayes, Jordan et al, “Cooperative Privacy and Security: Learning from People with Visual Impairments and Their Allies”.

15. Holm, Sune, “Should People Have a Right Not to Be Subjected to AI Profiling based on Publicly Available Data? A Comment on Ploug” (2023) 36:2 Philosophy Technology 38.

16. Khanlou, Nazilla et al, “Protection of Privacy of Information Rights among Young Adults with Developmental Disabilities” (2018) 16:3 Int’l J Mental Health Addiction 545–572.

17. Kokolakis, Spyros, “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon” (2017) 64 Computer Security 122–134.

18. Kuner, Christopher et al, “Expanding the artificial intelligence-data protection debate” (2018) 8:4 Int’l Data Privacy L 289–292.

19. Martin, Kirsten, “Understanding Privacy Online: Development of a Social Contract Approach to Privacy” (2016) 137:3 J Bus Ethics 551–569.

20. Marwick, Alice E & danah boyd, “Networked privacy: How teenagers negotiate context in social media” (2014) 16:7 New Media Soc 1051–1067.

21. Massara, Francesco, Francesco Raggiotto & W Gregory Voss, “Unpacking the privacy paradox of consumers: A psychological perspective” (2021) 38:10 Psychol Mark 1814–1827.

22. Mattson, P et al, “MLPerf: An Industry Standard Benchmark Suite for Machine Learning Performance” (2020) 40:2 IEEE Micro 8–16.

23. McDonald, Nora, Aaron Massey & Foad Hamidi, “Elicitation and Empathy with AI-enhanced Adaptive Assistive Technologies (AATs): Towards Sustainable Inclusive Design Method Education” (2023) 11:2 J Probl Based Learn High Educ 78–99.

24. Meredith, Stephanie et al, “The impact of implicit and explicit bias about disabilities on parent experiences and information provided during prenatal screening and testing” (2024) 17:1 Disabil Health J 101514.

25. Morris, Meredith Ringel, “AI and accessibility” (2020) 63:6 Commun ACM 35–37.

26. Mujirishvili, Tamara et al, “Acceptance and Privacy Perceptions Toward Video-based Active and Assisted Living Technologies: Scoping Review” (2023) 25:1 J Med Internet Res e45297.

27. Mulvenna, Maurice et al, “Views of Caregivers on the Ethics of Assistive Technology Used for Home Surveillance of People Living with Dementia” (2017) 10:2 Neuroethics 255–266.

28. Nam Kim, Hyung, “Digital Privacy of Assistive Technology Users with Visual Disabilities” (2022) 66:1 Proc Hum Factors Ergon Soc Annu Meet 1105–1109.

29. Reidenberg, Joel R et al, “Ambiguity in Privacy Policies and the Impact of Regulation” (2016) 45:S2 J Leg Stud S163–S190.

30. Singh, Pushpa et al, “Artificial Intelligence for Smart Data Storage in Cloud-Based IoT” in Fadi Al-Turjman et al, eds, *Transform Manag AI Big-Data IoT* (Cham: Springer International Publishing, 2022) 1.

31. Sony, Reeta, Kan Sri & D Bhukya, “Data Protection and Cloud Computing: a Jurisdictional Aspect” (2013) Право Журнал Высшей Школы Экономики 81–91.

32. Spezialetti, Matteo, Giuseppe Placidi & Silvia Rossi, “Emotion Recognition for Human-Robot Interaction: Recent Advances and Future Perspectives” (2020) 7 Front Robot AI 532279.

33. Stangl, Abigale et al, “Privacy Concerns for Visual Assistance Technologies” (2022) 15:2 ACM Trans Access Comput 1–43.

34. Vieira, Alessandro Diogo, Higor Leite & Ana Vitória Lachowski Volochtchuk, “The impact of voice assistant home devices on people with disabilities: A longitudinal study” (2022) 184 Technol Forecast Soc Change 121961.

35. Wang, Yang & Charlotte Emily Price, “Accessible Privacy” in Bart P Knijnenburg et al, eds, *Mod Socio-Tech Perspective Privacy* (Cham: Springer International Publishing, 2022) 293.

36. Wangmo, Tenzin et al, “Ethical concerns with the use of intelligent assistive technology: findings from a qualitative study with professional stakeholders” (2019) 20:1 BMC Med Ethics 98.

37. Weinmann, Markus, Christoph Schneider & Jan vom Brocke, “Digital Nudging” (2016) 58:6 Business Information System Engineering 433–436.

38. Witte, Luc de et al, “Assistive technology provision: towards an international framework for assuring availability and accessibility of affordable high-quality assistive technology” (2018) 13:5 Disability Rehabilitation Assistive Technology 467–472.

39. Yang, Fei, Kaili Zheng & Yu Yao, “Protecting people with disabilities’ data privacy in government information disclosure: facilitation by procurator-led public-interest litigation” (2024) 39:3 Disability Soc 811–816.

40. Zezulak, Alisa, Faiza Tazi & Sanchari Das, “SoK: Evaluating Privacy and Security Concerns of Using Web Services for the Disabled Population*”* (arXiv, 2023).

Secondary Material – Books

1. Andrews, Erin E, Disability As Diversity: Developing Cultural Competence (Oxford University Press, 2019).

2. Claypoole, Ted & American Bar Association, eds, The law of artificial intelligence and smart machines: understanding A.I. and the legal impact (Chicago, Illinois: American Bar Association, Business Law Section, 2019).

3. Herring, Jonathan, “Introducing Vulnerability” in Jonathan Herring, ed, Vulnerable Adults Law (Oxford University Press, 2016).

4. Malgieri, Gianclaudio, “Who is the vulnerable individual?” in Gianclaudio Malgieri, ed, Vulnerability Data Prot Law (Oxford University Press, 2023).

5. Richards, Neil, Why Privacy Matters, (The United States of America: Oxford University Press, 2022).

6. Quintavalla, Alberto & Temperman, Jeroen, eds, Artificial Intelligence and Human Rights (Oxford, New York: Oxford University Press, 2023)

Secondary Material – Reports

1. AI Now Institute, “Disability, Bias, and AI - Report”, (20 November 2019), online: *AI Inst* <https://ainowinstitute.org/publication/disabilitybiasai-2019>.

2. Carine Marzin, “Plug and Pray?”, (15 December 2020), online: European Disability Forum <https://www.edf-feph.org/publications/plug-and-pray-2018/>.

3. Directorate-General for Parliamentary Research Services (European Parliament) et al, Assistive technologies for people with disabilities. Part I, Regulatory, health and demographic aspects (LU: Publications Office of the European Union, 2018).

4. Directorate-General for Parliamentary Research Services (European Parliament) et al, Assistive technologies for people with disabilities. Part II, Current and emerging technologies (LU: Publications Office of the European Union, 2018).

5. Directorate-General for Parliamentary Research Services (European Parliament) et al, Assistive technologies for people with disabilities. Part IV, Legal and socio-ethical perspectives (LU: Publications Office of the European Union, 2018).

6. House of Commons, Canada, "Report of the Standing Committee on Access to Information, Privacy and Ethics, Towards Privacy By Design: Review of the *Personal Information Protection and Electronic Documents Act*" (House of Commons 2018) 50

7. Report of the Special Rapporteur on the rights of persons with disabilities, UNGA, 49th Sess, UN Doc A/HRC/49/52 at 8.

8. "Resolution on the EU Artificial intelligence Act for the inclusion of persons with disabilities", (1 April 2023), online: *European Disability Forum* <https://www.edf-feph.org/publications/resolution-on-the-eu-artificial-intelligence-act-for-the-inclusion-of-persons-with-disabilities/>.

9. Rights of persons with disabilities-Report of the Special Rapporteur on the rights of persons with disabilities, HRC, 49th sess, UN Doc A/HRC/49/52 (2021).

10. World Intellectual Property Organization, WIPO Technology Trends 2021- Assistive Technology, online: <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055_2021.pdf>.

Secondary Material – Government websites

1. "16. Consent and capacity | Ontario Human Rights Commission", online: <https://www.ohrc.on.ca/en/policy-preventing-discrimination-based-mental-health-disabilities-and-addictions/16-consent-and-capacity>.

2. "Frequently Asked Questions: Personal Health Information Protection Act | Information and Privacy Commissioner of Ontario", online: <https://www.ipc.on.ca/en/resources-and-decisions/frequently-asked-questions-personal-health-information-protection-act>.

3. "Getting Accountability Right with a Privacy Management Program", (17 April 2012), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/>.

4. “Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)”, (24 May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>.

5. “Interpretation Bulletin: Sensitive Information”, (16 May 2022), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/>.

6. “News Release: Privacy Commissioner releases finding on a bank’s refusal to release credit score - PIPEDA Case Summary #2002-39”, (22 February 2002), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/pipeda-2002-039/>.

7. Office of the Privacy Commissioner of Canada, “Cloud computing and privacy”, (4 October 2011), online: <https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/cloud-computing/02_05_d_51_cc/>.

8. “PIPEDA Fair Information Principle 3 – Consent”, (8 January 2018), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/>.

9. “PIPEDA Findings #2020-004: Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia - Office of the Privacy Commissioner of Canada”, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/>.

10. “PIPEDA interpretation bulletins - Office of the Privacy Commissioner of Canada”, online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/>.

11. “Protecting the privacy rights of young people”, (28 November 2023), online: <https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20231128/>.

12. “Rights of people with disabilities - Canada.ca”, online: <https://www.canada.ca/en/canadian-heritage/services/rights-people-disabilities.html>.

13. “Summary of privacy laws in Canada”, (15 May 2014), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/>.

14. “Sustainable Development Goal 10: Reduced inequalities - Canada.ca”, online: <https://www.canada.ca/en/employment-social-development/programs/agenda-2030/reduced-inequalities.html>.

Secondary Material – Other Material

1. "Accountability (OECD AI Principle) - OECD.AI", online: <https://oecd.ai/en/dashboards/ai-principles/P9>.

2. "Accountability principle", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accountability-principle/>.

3. Aboulafia, Ariana, "Internet Privacy Is A Disability Rights Issue | TechPolicy.Press", (19 January 2024), online: *Tech Policy Press* <https://techpolicy.press/internet-privacy-is-a-disability-rights-issue>.

4. AIPRM, "Artificial Intelligence and Assistive Technologies · AIPRM", (22 August 2023), online: <https://www.aiprm.com/education/artificial-intelligence-and-assistive-technologies/>.

5. "AI and Its Implications for Data Privacy", online: <https://www.routledge.com/blog/article/ai-and-its-implications-for-data-privacy>.

6. "AI language models show bias against people with disabilities, study finds | Penn State University", online: <https://www.psu.edu/news/information-sciences-and-technology/story/ai-language-models-show-bias-against-people-disabilities/>.

7. Baskin, Jonathan Salem, "The Privacy Debate Isn't About Secrets, It's About Control", online: *Forbes* <https://www.forbes.com/sites/jonathansalembaskin/2014/07/22/the-privacy-debate-isnt-about-secrets-its-about-control/>.

8. "Canada - Data Protection Overview", (26 January 2024), online: *DataGuidance* <https://www.dataguidance.com/notes/canada-data-protection-overview>.

9. "Canadian Bar Association - The privacy paradox", online: <https://www.cba.org/Sections/Privacy-and-Access/Articles/2022/The-privacy-paradox>.

10. Cameron, Lori, "Artificial Intelligence and Consent: Navigating The Ethics of Automation and Consumer Choice", (16 September 2018), online: *IEEE Comput Soc* <https://www.computer.org/publications/tech-news/research/ai-and-the-ethics-of-automating-consent/>.

11. Copper, Cathryn, "Research guides: Artificial Intelligence for Image Research: Datasets, Bias, Discrimination", online: <https://guides.library.utoronto.ca/c.php?g=735513&p=5297043>.

12. Dick, Ellysse, *How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces*, by Ellysse Dick, itif.org (2020).

13. Forum, World Economic, “Generative AI holds great potential for those with disabilities – but it needs policy to shape it”, (6 November 2023), online: *Eur Sting - Crit News Insights Eur Polit Econ Foreign Aff Bus Technol - Eur* <https://europeansting.com/2023/11/06/generative-ai-holds-great-potential-for-those-with-disabilities-but-it-needs-policy-to-shape-it/>.

14. Gonzalez, Wendy, “Council Post: Three Ways AI Is Improving Assistive Technology”, online: *Forbes* <https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/21/three-ways-ai-is-improving-assistive-technology/>.

15. Google tells Parliament IT Panel that its employees listen to some Ok Google queries”, online: <https://www.indiatoday.in/technology/news/story/google-tells-parliament-it-panel-that-its-employees-listen-to-some-okay-google-queries-1820975-2021-06-30>.

16. “Google’s New Glasses Can Translate Speech in Real Time | IoT World Today”, online: <https://www.iotworldtoday.com/iiot/google-s-new-glasses-can-translate-speech-in-real-time->.

17. “Guidelines for the Regulation of Computerized Personal Data Files | Refworld”, online: <https://www.refworld.org/policy/legalguidance/unga/1990/en/13761>.

18. Guynn, Jessica, “Facebook taps artificial intelligence for users with disabilities”, online: *USA TODAY* <https://www.usatoday.com/story/tech/news/2016/03/23/facebook-accessibility-people-with-disabilities/82026554/>.

19. Harkous, Hamza et al, *Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning* (arXiv, 2018).

20. Healey, Formiti-Robert, “GDPR and the Accountability Principle”, (12 December 2020), online: *Lexology* <https://www.lexology.com/library/detail.aspx?g=34144a92-3aa2-4c75-b1c3-346be0719117>.

21. “How do we ensure lawfulness in AI?”, (7 February 2024), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/>.

22. “How do we ensure transparency in AI?”, (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-transparency-in-ai/>.

23. “How Fast Is Technology Growing Statistics [Updated 2023]”, online: <https://leftronic.com/blog/how-fast-is-technology-growing-statistics/>.

24. “How ‘Notice and Consent’ Fails to Protect Our Privacy”, online: *New Am* <http://newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/>.

25. “How should we assess security and data minimisation in AI?”, (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-

intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/>.

26. "How sovereign funds could empower the future of assistive technology and disability AI", (15 August 2023), online: *World Econ Forum* <https://www.weforum.org/agenda/2023/08/sovereign-funds-future-assistive-technology-disability-ai/>.

27. Hub, Global Disability Innovation, "Physiological computing, artificial intelligence and empowering our capability", online: *Glob Disabil Innov Hub* <https://www.disabilityinnovation.com/projects/physiological-computing-artificial-intelligence-and-empowering-our-capability>.

28. "I tried to read all my app privacy policies. It was 1 million words.", (31 May 2022), online: *Wash Post* <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>.

29. "Interview with Kave Noori and Marine Uldry from the European Disability Forum: 'Nothing about us without us', including AI - EAISF", (31 October 2023), online: *EAISF* - <https://europeanaifund.org/newspublications/interview-with-kave-noori-and-marine-uldry-from-the-european-disability-forum-nothing-about-us-without-us-including-ai/>.

30. Land, Molly et al, "Art.22 Respect for Privacy", online: *Oxf Public Int Law* <https://opil-ouplaw-com.ezproxy.library.yorku.ca/display/10.1093/law/9780198810667.001.0001/law-9780198810667-chapter-23>.

31. LG, "What data is used to train an AI, where does it come from, and who owns it?", online: *Potter Clarkson* <https://www.potterclarkson.com/insights/what-data-is-used-to-train-an-ai-where-does-it-come-from-and-who-owns-it/>.

32. Martin, Kirsten, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online* (Rochester, NY, 2014).

33. Mühlhoff, Rainer & Hannah Ruschemeier, *Updating Purpose Limitation for AI: A normative approach from law and philosophy* (Rochester, NY, 2024).

34. Napoli, Daniela et al, *"I'm Literally Just Hoping This Will {Work:'}' Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities* (2021).

35. Noone, Cat, "Flawed data is putting people with disabilities at risk", (19 April 2021), online: *TechCrunch* <https://techcrunch.com/2021/04/19/flawed-data-is-putting-people-with-disabilities-at-risk/>.

36. "Principle (b): Purpose limitation", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/>.

37. “Principle (d): Accuracy”, (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/>.

38. “Principle (e): Storage limitation”, (4 August 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/>.

39. “Principle (f): Integrity and confidentiality (security)”, (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/integrity-and-confidentiality-security/>.

40. “Office for Victims of Crime - Multidisciplinary Response to Crime Victims With Disabilities”, online: <https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/victimswithdisabilities/stateguide/risk-factors.html>.

41. “Osler AI Series Module 2 – Data, Intellectual Property and Privacy”, online: *Osler Hoskin Harcourt LLP* <http://www.osler.com/en/events/2023/osler-ai-series-module-2-data-intellectual-property-and-privacy-en>.

42. “Purpose limitation, data minimisation and storage limitation”, (19 May 2023), online: <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/purpose-limitation-data-minimisation-and-storage-limitation/>.

43. “Re-Identification of ‘Anonymized’ Data”, (12 April 2017), online: *Georget Law Technol Rev* <https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/>.

44. Review, Stanford Law & tribe, “Privacy in the Age of Big Data”, (2 February 2012), online: *Stanford Law Rev* <https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/>.

45. Secretariat, Treasury Board of Canada, “Guide on the Scope of the Directive on Automated Decision-Making”, (18 July 2024), online: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-scope-directive-automated-decision-making.html>.

46. Team, IBM Data and AI, “Shedding light on AI bias with real world examples”, (16 October 2023), online: *IBM Blog* <https://www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples/www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples>.

47. Team, Insights, “Forbes Insights: Rethinking Privacy For The AI Era”, online: *Forbes* <https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/>.

48. Touzet, Chloé, *Using AI to support people with disability in the labour market: Opportunities and challenges*, by Chloé Touzet, OECD iLibrary (Paris: OECD, 2023).

49. Turner, Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica, "4. Americans' attitudes and experiences with privacy policies and laws", (15 November 2019), online: *Pew Res Cent* <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>.

50. UCL, "Policy brief: Powering Inclusion: Artificial Intelligence and Assistive Technology", (23 November 2022), online: *UCL Dep Sci Technol Eng Public Policy* <https://www.ucl.ac.uk/steapp/policy-brief-powering-inclusion-artificial-intelligence-and-assistive-technology>.

51. "Updates to the OECD's definition of an AI system explained", online: <https://oecd.ai/en/wonk/ai-system-definition-update>.

52. "Using privacy laws to regulate automated decision making | McCarthy Tétrault", online: <https://www.mccarthy.ca/en/insights/blogs/techlex/using-privacy-laws-regulate-automated-decision-making>.

53. "Warren and Brandeis, 'The Right to Privacy'", online: <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

54. "What do we need to know about accuracy and statistical accuracy?", (19 May 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-do-we-need-to-know-about-accuracy-and-statistical-accuracy/>.

55. "What is AI? / Basic Questions", online: <http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html>.

56. "What Is AI Model Training & Why Is It Important? | Oracle Canada", online: <https://www.oracle.com/ca-en/artificial-intelligence/ai-model-training/>.

57. "What Is Data Privacy? | IBM", (12 March 2024), online: <https://www.ibm.com/topics/data-privacy>.

58. "What is federated learning?", (9 February 2021), online: *IBM Res* <https://research.ibm.com/blog/what-is-federated-learning>.

59. "What is Streaming Data? - Streaming Data Explained - AWS", online: *Amaz Web Serv Inc* <https://aws.amazon.com/what-is/streaming-data/>.

60. "Why privacy is particularly crucial for people with disabilities", online: *Eur Digit Rights EDRi* <https://edri.org/our-work/why-privacy-is-particularly-crucial-for-people-with-disabilities/>.

61. “Why Privacy-First Approach Is Critical For Data-Based Innovation?”, online: <https://www.forbes.com/sites/taarinikaurdang/2021/05/27/why-privacy-first-approach-is-critical-for-data-based-innovation/>.

62. “Working Together: People with Disabilities and Computer Technology | DO-IT”, online: <https://www.washington.edu/doit/working-together-people-disabilities-and-computer-technology>.

63. “You’re very easy to track down, even when your data has been anonymized”, online: *MIT Technol Rev* <https://www.technologyreview.com/2019/07/23/134090/youre-very-easy-to-track-down-even-when-your-data-has-been-anonymized/>.