Comment on Article 22 and Its Intersection with Obligations for Accessibility

G. Anthony Giannoumis – Oslo and Akershus University College of Applied Sciences

Molly K. Land – University of Connecticut

Agnieszka Kitkowska – University of Karlstad

Maria Mikhaylova – Oslo and Akershus University College of Applied Sciences

Contents

Article 22 of the United Nations (UN) Convention on the Rights of Persons with Disabilities (CRPD) guarantees the protection of persons with disabilities against unlawful and arbitrary interference with their privacy. This right can be applied in a wide range of circumstances and contexts. At its core, Article 22 follows the blueprint of Article 17 of the International Convention on Civil and

Political Rights (ICCPR).[1] There are, however, a few minor but noticeable differences from the original text of the ICCPR.

As one of the most fundamental human rights, the right to privacy is enshrined in a number of other international and regional instruments, including Article 12 of the UDHR, Article 11 of the American Convention on Human Rights (ACHR), Article 11 of the African Convention on Human and Peoples' Rights (ACHPR), and Article 8 of the European Convention on Human Rights (ECHR).[2] The application of Article 8 by the European Court of Human Rights (ECtHR) bears special significance for the development of the right to privacy.

This Chapter represents a further extension of research on the right to privacy for persons with disabilities by examining the legal and normative obligations under Article 22 in light of current technological trends and obligations for promoting ICT accessibility. It is at the intersection of privacy and disability that crosscutting obligations in the CRPD, such as ICT accessibility, become most salient. Article 9 of the CRPD obligates States Parties to ensure access to ICT for persons with disabilities. Legal scholars have argued that this obligation focuses specifically on designing ICT that is usable by persons with disabilities.[3] However, scholars have only recently begun to investigate the relationship between persons with disabilities' right to privacy and obligations for ensuring ICT accessibility.

Re-conceptualizing privacy in relation to obligations for ICT accessibility enshrined in Article 9 make it clear that ICT accessibility has the potential to simultaneously facilitate social participation as well as open up persons with disabilities to the risk of privacy violations. In other words, an individual's right to privacy may be violated if efforts to ensure accessibility proceed without consideration of the potential privacy impacts. Therefore, obligations to ensure the accessible design of ICT must be taken into consideration in light of the privacy-related contexts and activities in which persons with disabilities engage.

This Chapter considers the scope and impact of accessibility in relation to the right to privacy of persons with disabilities. The Chapter proceeds in five parts. In the first part, this Chapter reviews each of the provisions of Article 22 and considers their implications for the privacy rights of individuals with disabilities. The next section considers in particular the implication of data protection laws for individuals with disabilities. The final section evaluates the right to privacy in the context of ICT accessibility. The Chapter concludes by discussing future steps in research and practice regarding the right to privacy and obligations for ICT accessibility.

I. Drafting History of Article 22

Respect for privacy under the Comprehensive and Integral International Convention on Protection and Promotion of the Rights and Dignity of Persons with Disabilities was first formulated in the Chairman's draft as a right to respect for privacy, home, the protection of the family, and the right to marry. This draft article mostly concentrated on the right to privacy with regard to the right of

[1] Annex II, Report of the Coordinator to the Ad Hoc Committee at its fifth session, http://www.un.org/esa/socdev/enable/rights/ahc5reporte.htm

[2] Della Fina, V., Cera, R., & Palmisano, G. (2017). *The United Nations Convention on the Rights of Persons with Disabilities: A Commentary*: Springer. p. 404: "Article 12 of the UDHR, Article 16 of the CRC, and Article 14 of the CRMW, which use the same language. Regional human rights instruments also contain similar provisions. The right to privacy is protected under Article 8 of the ECHR, Article 7 of the EUCFR, Article 11 of the ACHR, and Article 11 of the ACHPR".

[3] Blanck, P. (2014). *eQuality: The struggle for web accessibility by persons with cognitive disabilities*. New York: Cambridge University Press.

persons with disabilities to form intimate relationships, the right to found a family, and the right to parenthood.

A working group was established in June 2003 by a second session of the Ad Hoc Committee on a Comprehensive and Integral International Convention on Protection and Promotion of the Rights and Dignity of Persons with Disabilities with the aim of preparing and presenting a draft text of a convention that would be the basis for negotiation by Member States. Under this draft, the right to privacy was formulated in draft Article 14 as a positive obligation for the States to take effective measures to protect the privacy of the home, family, correspondence, and medical records as well as to safeguard the freedom of persons with disabilities to make decisions on personal matters.

The Third Session of the Ad Hoc Committee continued its work on formulating the right to privacy proceeding from the draft Article 14 suggested by the working group. Through most of the drafting process, the right to privacy was seen as being closely interlinked with right to the privacy of home, right to marry and found a family, as well as the protection of family. A recurring suggestion was to explicitly formulate a separate clause providing protections for persons with disabilities from unlawful involuntary sterilization. It was eventually formulated as "a right to retain their fertility" and included as a distinct provision under Article 23 of the CRPD.

Initially the working group also raised the issue of privacy under two other Articles: draft Article 6 (Statistics and data collection)[4] and draft Article 21 (Right to health and rehabilitation).[5] Draft Article 6 provided that the process of data collection and way of maintaining information should "respect the right to privacy, the dignity and the rights of persons with disabilities." Draft Article 21 encompassed obligations for States Parties to "protect the privacy of health and rehabilitation information of persons with disabilities."

These clauses were discussed as separate provisions up until the Seventh Session, after which it was decided to merge the right to protect the privacy of health and rehabilitation information, formulated by the working group in draft Article 21, with para. 1 of Article 14 formulated at the Fifth session of the Ad Hoc Committee, which eventually became Article 22. Draft Article 6 was transformed into Article 31 of the CRPD retaining the obligation of the States Parties to ensure confidentiality and respect for the privacy of persons with disabilities in statistics and data collection.

B. Arbitrary or Unlawful Interference

Article 22 of the CRPD provides that all persons with disabilities should be protected from "arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication." The CRPD Committee has not addressed the conditions under which the right to privacy may be limited. Nonetheless, the text of Article 22 of the CRPD, like Article 17 of the ICCPR, provides that interferences with privacy are prohibited if they are "unlawful" or "arbitrary."

Pursuant to General Comment No. 16 on Article 17 of the ICCPR, "unlawful" means that no interference with privacy is allowed except in cases envisioned by law.[6] An interference is also prohibited if it is "arbitrary." According to the HRC, even an interference that is provided by law will be inconsistent with Article 17 if it is "arbitrary." Interferences that are provided by law must also be consistent with "the provisions, aims and objectives of the Covenant" and "and should be, in any event, reasonable in the particular circumstances."[7] Such interference will be "reasonable" when it is

[4] Working Group draft text, Draft Article 6 Statistics and data collection, http://www.un.org/esa/socdev/enable/rights/ahcwgreporta6.htm
[5] Working Group draft text, Draft Article 21 Right to health and rehabilitation, http://www.un.org/esa/socdev/enable/rights/ahcwgreporta21.htm
[6] Gen Comment 16, para. 3
[7] Gen Comment 16, para. 4

"proportional" to the aim the law is attempting to achieve and "necessary" in the particular circumstances of the case.[8]

Article 8(2) of the ECHR provides a more specific test for identifying the conditions under which state authorities are allowed to limit the right of an individual and interfere with his or her privacy. Interference with privacy is qualified as legitimate when it satisfies three conditions: it is in accordance with the law; it is necessary in a democratic society; and it pursues a legitimate aim, such as safeguarding the interests of national security, public safety or the economic well-being of the country, as well as the prevention of disorder or crime, protection of health or morals, or for the protection of the rights and freedoms of others.[9]

The CRPD Committee has expressed concern about both private and public interferences with the rights protected by Article 22. Among other things, the Committee has critiqued the data protection and privacy practices of hospitals and institutions[10] and expressed the need for data protection protocols in the health and banking sectors.[11] Similarly, in interpreting the scope of Article 17 of the ICCPR in General Comment No. 16, the Human Rights Committee (HRC) has said that the private life of the person should be protected from such interference independent of whether they emanate from public authorities or private or legal persons.[12] In this sense, Article 8 ECHR has a more narrow scope, as it provides protection only from "interferences … from the State authorities."

The nature of State obligations in regard to the protection of the right to privacy contains both negative and positive obligations.[13] Negative obligations of the State correspond to the obligation of the States Parties to respect the rights provided under a given instrument. Positive obligations to protect and fulfill rights in question in their turn formulate a duty of the State to take positive steps in securing a given right, namely to adopt measures to secure that neither individuals, nor other private actors will deprive an individual from their right as well as to strengthen a persons' "access" to this right.[14] The CRPD Committee's Concluding Observations have made clear that the obligation extends not only to refraining from unlawful and arbitrary attacks to protecting individuals with disabilities from violations of their right to privacy by third parties.[15]

The revelations in 2013 by Edward Snowden that the United States (US) government had used large-scale data collection projects to monitor US and foreign citizens provides a useful example of how the use of ICT for surveillance may constitute arbitrary and unlawful interference.[16] Legal scholars have provided in-depth analyses of these events showing that the US National Security Agency (NSA)

---

[8] *Rafael Armando Rojas García v. Colombia*, para. 10.3

[9] ECHR, Article 8(2)

[10] Concluding Observations on Latvia, ¶¶ 36-37 (psychiatric hospitals and institutions); Concluding Observations on Denmark, ¶¶ 50-51 (psychiatric hospitals transferring information to third parties); Concluding Observations on Armenia, ¶¶ 37-38 (display of children "for medical or charity purposes").

[11] Concluding Observations on Uganda, ¶¶ 44-45.

[12] CCPR, General Comment No. 16: Article 17 (Right to privacy), HRI/GEN/1/Rev.1 at 21 (1994), para.1

[13] UN Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 12: The Right to Adequate Food (Art. 11 of the Covenant), Document E/C.12/1999/5, 12 May 1999, para. 15

[14] Ibid.

[15] Concluding Observations on Latvia, ¶¶ 36-37 (psychiatric hospitals and institutions); Concluding Observations on Denmark, ¶¶ 50-51 (psychiatric hospitals transferring information to third parties); Concluding Observations on Armenia, ¶¶ 37-38 (display of children "for medical or charity purposes"); Concluding Observations on Uganda, ¶¶ 44-45 (need for data protection policies in the "health and banking sectors").

[16] Posner anticipated the Snowden revelations stating in a 2008 article on privacy and surveillance law "[s]uppose that the listening devices of the National Security Agency (NSA) gathered the entire world's electronic communications traffic, digitized it, and stored it in databases; […] (For all one knows, the NSA is doing all these things.)" See Posner, R. A. (2008). Privacy, surveillance, and law. *The University of Chicago Law Review, 75*(1), 245-260.

had, since 2010, been collecting and storing approximately 2 billion digital communications every day.[17] The data collection included a variety of metadata, which provided information about those communications such as the time and date when the communications were created.

Sinha argues that the NSA surveillance violates the right to privacy under Article 17 of the ICCPR and that due to the increased role of government surveillance, the HRC must provide more detailed guidance on the right to privacy under the ICCPR.[18] In particular, the NSA collected data without a warrant from US citizens not suspected of wrongdoing. This included direct access to a variety of communications including emails, voice calls, and documents via a many popular channels including platforms owned and operated by the largest ICT companies such as Microsoft, Yahoo, Google, Facebook, and Apple.

For persons with disabilities, this large-scale data collection by government actors poses a substantial threat to their privacy. As pointed out by Lazar et al., persons with disabilities rely on ICT to a greater extent than others.[19] This means that persons with disabilities may be disproportionately affected by the NSA's surveillance. For example, recent clinical research has shown that persons with psychosocial disabilities such as bipolar disorder use social media platforms such as Facebook for self-care.[20] The NSA's surveillance therefore may disproportionately violate the right to privacy for persons with disabilities when compared to others.

In addition, the HRC has argued that in order to realize a right to privacy everyone has the right to information "in an intelligible form" about "whether, and if so, what personal data is stored … for what purposes" and by whom – e.g., which public or private sector organization controls and stores this data.[21] The HRC has gone on to state that individuals have the right to request changes to or elimination of data that contains incorrect information or that was collected or processed unlawfully.

While the HRC does not explicitely mention that information about data collection and storage should be accessible for persons with disabilities, the intersection of a right to privacy for persons with disabilities with obligations for ensuring accessibility under Article 9 of the CRPD point to the need for ensuring the accessibility of information about data collection and storage conducted by State or non-State actors. However, to date, goverments have yet to provide information about the operations of mass surveillance programs.

State-based surveillance programs have particular relevance for persons with disabilities and provide a useful basis for legal scholars and the CRPD Committee to consider the interaction between Article 22 and state obligations for accessibility under Article 9 in three respects. First, the revelations about the NSA surveillance largely emerged in media reports. These reports provided the first documentation of the scale and impact of the NSA's surveillance. The accessibility of ICT used to communciate these reports, such as media websites and social media accounts, are consequently relevant not only for ensuring access to the reports themselves but also for the right to privacy for persons with disabilities.[22] Second, where States voluntarily disclose information about surveillance and other data collection activities, that information must be provided in ways that are accessible to

---

[17] See Sinha, G. A. (2013). NSA Surveillance since 9/11 and the Human Right to Privacy.; Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2), 2053951714541861.

[18] Sinha (n 59) This Chapter takes up the limitations to the right to privacy in Section 2.

[19] Lazar, et al., (n 3)

[20] See for example Naslund, J., Aschbrenner, K., Marsch, L., & Bartels, S. (2016). The future of mental health care: peer-to-peer support and social media. *Epidemiology and psychiatric sciences, 25*(2), 113-122.; Parikh, S. V., & Huniewicz, P. (2015). E-health: an overview of the uses of the Internet, social media, apps, and websites for mood disorders. *Current opinion in psychiatry, 28*(1), 13-17.

[21] See Sinha (n 59).

[22] The issue of accessible media reporting is particularly relevant for international media conglomerates as the NSA and other surveillance programs affect both nationals and citizens of other countries.

persons with disabilities. Third, the revelations that State authorities conduct mass surveillance on digital communications has given rise to the adoption and development of new tools for securing privacy online.[23] In order to realize a right to privacy for persons with disabilities, these tools and other ICT used to ensure privacy online must be accessible for persons with disabilities.

C. Privacy, Family, Home, Correspondence and Communication Privacy

The text of Article 22 further provides that "privacy, family, home or correspondence and other types of communication" are protected from such interferences. Although the CRPD does not define any of these terms, General Comment No. 16 on right to privacy in the ICCPR provides clarification.

1. Family

In its General Comment No. 16, the HRC does not formulate any precise definition of the term "family." Instead, it provides for a broader interpretation of this concept and notes that it should be defined "as understood in the society of the State party concerned."[24]

2. Home

"Home" is given a particularly broad scope in Article 22, which specifies that the right to privacy must be protected "regardless of [the individual's] place of residence or living arrangements." Among other things, this phrase extends respect for privacy to persons living in institutions or in any other arrangements, where there is a greater risk of arbitrary infringement of privacy for persons with disabilities as such intrusions may be seen as justifiable.[25]

The term "home" within the meaning of Article 17 of the ICCPR refers to a place where person resides on a permanent basis. It is, however, also understood that the term "home" includes the place where a person "carries out his usual activities,"[26] which indicates a need for a wider application of the term. The ECtHR has also adopted a more comprehensive interpretation of concept of "home." In accordance with ECtHR case law, the "home" may include business premises, social housing, and non-traditional residences, such as caravans and other temporarily inhabited spaces.[27]

3. Correspondence and Communication

Regarding correspondence and other means of communication, Article 17 obliges States to guarantee confidentiality and the security of communication of the person. According to the HRC, the term "correspondence" in the ICCPR also includes communications via tax, fax and mail.[28] The drafters of the CRPD, however, decided to make this development more explicit by specifying "correspondence or other types of communication" in order to indicate that protection is provided not only to the traditional means of communication, but also to those made possible by

---

[23] See for example the use of virtual private networks, privacy enhanced web browsers and other privacy technologies available at https://www.privacytools.io/, https://www.epic.org/privacy/tools.html, and https://www.techworld.com/security/best-online-privacy-tools-3633529/

[24] General Comment No. 16, para. 5

[25] Draft Article 14: Respect for privacy, the home and the family, Comments on the draft text, Working Group on , Third Session, http://www.un.org/esa/socdev/enable/rights/wgdca14.htm

[26] General Comment No. 16, para. 5

[27] Roagna, I (2012) Protecting the right to respect for private and family life under the European Convention on human rights. Council of Europe, Strasbourg, p.31

[28] Gisvold G, Carlson SN (2003) Practical Guide to the International Covenant on Civil and Political Rights. Transnational Publishers, New York, p.110

technological advances.

According to European human rights law, the content of any particular communication is not relevant, as the focus of Article 8 of the ECHR is on protecting the communication itself, regardless of its subject.[29] Furthermore, Article 8 protects not only the privacy of communications but also the privacy of information.

4. Privacy

Neither the CRPD nor the ICCPR provide any definition of the term "privacy."[30] Thus far, the CRPD Committee has primarily identified risks of privacy associated with sharing or disclosing personal data or other information about an individual's disability or health status.[31] In its Concluding Observations on Denmark, for example, the Committee expressed concern about the transfer of "strictly private and confidential information" by psychiatric hospitals to third parties without the consent of the person concerned, and it urged the state to prohibit such practices.[32] In its Concluding Observations on Latvia, the Committee expressed concern about the lack of safeguards to protect the privacy of individuals who were listed on a "Register of Patients Suffering from Certain Diseases" in light of the impact this listing had on their employment and access to services.[33] In its recommendations to Latvia, the Committee also expressed concern about the inability of individuals to contest third party access to data that hospitals had collected about them without their consent.[34] The concept of "privacy" in the CRPD also relates to sharing of information that harms the dignity of individuals with disabilities. In its Concluding Observations on Armenia, for example, the CRPD Committee expressed concern that "children with disabilities are publicly displayed for medical or charity purposes" and urged the state to adopt more rigorous privacy protections.[35]

Although the HRC in General Comment No. 16 also refrains from defining "privacy," it noted in *Coeriel and Aurik v. The Netherlands* that "the notion of privacy refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with

---

[29] Roagna (n 12) 33

[30] One of the main difficulties of privacy is its complex nature and lack of one, comprehensive definition. According to Holvast (2009), privacy can be considered across three dimensions: environment (the physical area surrounding individual), individual (protection sphere preventing physical search and potential abuse), and information. Smith, Milberg, & Burke characterize privacy as "the ability of the individual to personally control information about one's self." This definition of information privacy can be applied to various types of technologies that collect personal data, from computers, including personal computers, laptops and mobile devices, through the broad range of technologies associated with the Internet of Things, wearables and smart environments, including the assistive technologies necessary for persons with disabilities to make full use of their features and functions. These technologies gather personal information, some of which is required to utilize the full functionality of the technology product or service, however, some of it may be collected for other purposes, such as the secondary use of data, statistics, product improvements and more. There are instances, where the design (both at the functional as well as user interface level) and implementation of technology may potentially violate privacy principles. These "by design" privacy violations as well as the potential for security and data breaches may affect users' well-being, expose them to risks and result in harms. See Holvast, J. (2009). History of Privacy. In *The Future of Identity in the Information Society* (pp. 13–42).; Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196.

[31] Concluding Observations on Uganda, ¶ 45 (protecting personal data in "health and banking sectors"); Concluding Observations on Armenia, ¶ 38 (calling on state to protect the "personal, health, habilitation and rehabilitation status" of children).

[32] Concluding Observations on Denmark, ¶¶ 50-51.

[33] Concluding Observations on Latvia, ¶ 37 (a).

[34] Ibid. ¶ 37(b).

[35] Concluding Observations on Armenia, ¶¶ 37-38.

others or alone."[36] The HRC's definition of privacy parallels the ECtHR's interpretation of the term "private life" used in Article 8 of the ECHR. Proceeding from the case law of the ECtHR, the notion of "private life" encompasses such facets as physical and psychological integrity of a person,[37] individual's physical and social identity,[38] including ethnic identity,[39] the right to personal development and the right to establish and develop relationships with other human beings and the outside world, [40] name,[41] gender identification, sexual orientation and sexual life,[42] medical treatment and mental health;[43] as well as right to one's image[44] and right to data protection[45]. The provision also covers the right to personal development and the right to establish and develop relationships with other human beings and the outside world.[46] In this context, the right to privacy enshrined in the CRPD may be narrower than that provided in the ECHR as Art. 23 of the CRPD includes protections for the right to personal development and the right to establish and develop relationships.

The scope of the term "private life" provided under Article 8 of the ECHR is wider in scope than the term "privacy" under both Article 17 of the ICCPR and Article 22 of the CRPD.[47] It is suggested, however, that the notion of privacy under the CRPD can be interpreted in the same manner as the concept of "private life," when read together with other relevant provisions of the CRPD.[48]

D. Unlawful Attacks on Honor and Reputation of Persons with Disabilities

Finally, Article 22 prohibits unlawful attacks on honor and reputation of persons with disabilities. Protection of honor and reputation is accorded in other main human rights instruments such as the ICCPR, and was formulated for the first time in the UDHR. Terms such as honor and reputation are extremely broad, and are not defined by the CRPD. In connection with Article 17 of the ICCPR, it was presumed that such notions should be better defined within the framework of national legislation in accordance with the cultural and social norms of a given State party.[49] In the context of the ICCPR, some maintained that the notion of honor was already encompassed by the notion of reputation and therefore was superfluous to the text of Article 17. Other delegates pointed out that term "honor" described the judgment of the individual morals of a person, whereas reputation referred to upholding or failing to uphold professional or social standards, and therefore both concepts should

---

[36] UN HRC 09.12.1994, Communication No. 453/1991, *Coeriel v. The Netherlands*, U.N. Doc.; CCPR/C/52/D/453/1991 (1994)
[37] *X and Y v. the Netherlands* (1985) 22 Series A 91
[38] *Mikulić v. Croatia* (2002) 53 ECHR 2002-I
[39] *S. and Marper v. the United Kingdom [GC]* (2006) 66 ECHR 2008
[40] *Mikulić v. Croatia* (2002) 53 ECHR 2002-I, *Peck v. the United Kingdom* (2003) 57 ECHR 2003 I
[41] *Burghartz v. Switzerland* (1994) 24 Series A 280-B, *Guillot v. France* (1996) 22 Reports of Judgments and Decisions 1996-V
[42] *Dudgeon v. the United Kingdom* (1981) 41 Series A No 45, *B. v. France* (1992) 63 Series A No. 232-C, *Peck v. the United Kingdom* (2003) 57 ECHR 2003 I
[43] *Bensaid v. the United Kingdom* (2001) 47 ECHR 2001 I
[44] *Sciacca v. Italy* (2005) 29, ECHR 2005-I
[45] *Z v. Finland* (1997) 95 Reports of Judgments and Decisions 1997 I
[46] Della Fina, 405: *X and Y v. the Netherlands, Mikulic v. Croatia*
[47] Roagna (n 12) 12
[48] Della Fina, p. 406 Della Fina provides the following list of relevant Articles: Article 16 prohibiting all forms of exploitation, violence, and abuse towards persons with disabilities; Article 23 on the respect for home and the family; Article 25, para. (d), requiring health professionals to provide care of the same quality to persons with disabilities as to others on the basis of free and informed consent; and Article 31, para. 1, stating that the process of collecting and maintaining data must comply with legally established safeguards, including legislation on data protection, to ensure confidentiality and respect for the privacy of persons with disabilities.
[49] General Comment No. 16, para. 11

be reflected in the text of the Article.[50]

The corresponding provision of the ECHR on the right to privacy does not explicitly formulate a right to protection of honor and reputation, however the ECtHR in its judgment *Pfeifer v. Austria* recognized that reputation represents a part of "individual identity and psychological integrity" of a person, and therefore falls under the concept of private life.[51] The ECtHR however, also deals with issues of reputation under Article 10(2), which serves as a limitation clause for the right to freedom of expression, and pronounces protections of ones reputation as a legitimate aim for restriction of free speech.[52]

E. Right to Protection of Law Against Interference

The CRPD imposes positive obligations to safeguard the right to privacy of individuals by providing an appropriate legal framework. In its Concluding Observations, the CRPD Committee has called on states to create legal structures and protocols to protect the right to privacy of individuals with disabilities.[53] In General Comment No. 16, the HRC noted that Article 17 also "require[s] the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right."[54] The HRC puts significant responsibility on the legislative branches of States Parties to develop adequate laws and regulations and notes that "it is precisely in State legislation above all that provision must be made for the protection of the right set forth in that article."[55] Since the right to privacy is not absolute and can be limited, it is noted that legislation must contain specific details and precise circumstances in which interference can considered legitimate.[56]

It was recognized in *Malone v. the United Kingdom* that administrative measures cannot provide a sufficiently clear framework according to which the authorities are allowed to interfere with one's privacy, as it can be altered by governmental decision at any given point of time.[57] In addition, legal norms also have to satisfy a requirement of foreseeability of the consequences of their actions, which may arise in accordance with the law.[58] Furthermore, as provided under General Comment No. 16, the State is under the obligation to provide an effective remedy against those conducting unlawful attacks on reputation and honor of a person.[59]

---

[50] Draft International Covenants on Human Rights. Report of the Third Committee, A/4625, 8 December 1960, para. 38

[51] *Pfeifer v. Austria* (App no. 12556/03) (2007) 35

[52] ECHR, Article 10(2); ECtHR, Factsheet - Protection of reputation, Unite de la press, July 2017

[53] Concluding Observations on Paraguay, ¶ 77 (expressing concern with the lack of progress in implementing Article 22); Concluding Observations on Latvia, ¶ 37 (calling for the state to "reinforce the protection of privacy, including personal data, including in psychiatric hospitals and institutions"); Concluding Observations on Denmark, ¶ 51 (calling for an amendment to the Psychiatric Act to protect personal data of patients in hospitals); Concluding Observations on Uganda, ¶¶ 44-45 (calling for "protocols" in the "health and banking sectors").

[54] Gen Comment 16, para. 1

[55] Gen Comment 16, para. 2

[56] Gen Comment 16, para 8

[57] *Ibid.*

[58] *Andersson v. Sweden* (2010) (App. no. 17202/04) 75

[59] General Comment No. 16, para 11

F. Protection of Personal, Health and Rehabilitation Information

One of the other very important aspects of right to privacy is reflected in paragraph 2 of Article 22 granting the right to protection of personal, health, and rehabilitation information of the person with disability on the equal basis with others. The CRPD Committee has emphasized the importance of protecting personal data, particularly information about an individual's disability or health status, in several Concluding Observations.[60]

The CRPD Committee has emphasized the importance of access to grievance procedures regarding the collection, use, and sharing of personal data. In its Concluding Observations on Latvia, for example, the Committee critiqued the "[r]eported ineffective means of recourse to contest third party access to personal data of persons with intellectual and/or psychosocial disabilities collected by hospitals without the authorization of the individual concerned."[61]

Despite the fact that the ICCPR does not explicitly provide this same protection, General Comment No. 16 asserts the right for protection of personal information as a part of the right to privacy enshrined under Article 17 of the Covenant. It provides that States Parties must adopt legal regulations regarding the gathering, processing, and storing of personal information acquired by public authorities as well as by private bodies with a view to ensuring the safety of such information.[62]

General Comment No. 16, interpreting Article 17 of the ICCPR, also pronounces the right of the person to know which of his or her personal data is being collected and stored, by which authorities or private actors and for what purposes, as well as the right to rectification and elimination of individuals information in cases where such information appears to be incorrect or where it has been gathered in a manner inconsistent with the adopted laws and regulations.[63]

Guarantees for data protection in Europe have been developed under the ECHR through the ECtHR's rich and extensive case law on Article 8. The ECtHR has dealt with cases regarding the collection and storage of medical data; the recording of genetic and biometric data such as fingerprints; the interception of private communications including phone tapping, video surveillance and secret surveillance by authorities; the compulsory collection of information on personal expenditure for fiscal purposes; the compulsory collection of sensitive information for official census, and more.[64] A large number of the cases have been initiated in the context of criminal investigations.[65]

The right to protection of personal data has been explicitly formulated as separate right on par with the right to respect for private life under the Charter of Fundamental Rights of the European Union, which reflects an ongoing trend for treating the right to data protection as a separate right.[66]

---

[60] *See, e.g.*, Concluding Observations on Uganda, ¶ 45 (protecting personal data in "health and banking sectors"); Concluding Observations on Armenia, ¶ 38 (calling on state to protect the "personal, health, habilitation and rehabilitation status" of children); Concluding Observations on Denmark, ¶ 50 (protecting "strictly private and confidential information" by psychiatric hospitals).

[61] Concluding Observations on Latvia, ¶ 37(b).

[62] General Comment No. 16, para.

[63] General Comment No. 16, para.

[64] ECtHR, Factsheet – Protection of reputation*: S. and Marper v. the United Kingdom [GC]* ECHR 2008*, M.K. v. France* (2013) (App no. 19522/09), *Klass and Others v. Germany* (1978) Series A 28*, Kruslin v. France* (1990) Series A 176-A*;* Roagna (n 17) 19: *X v. the United Kingdom* (1981) Series A 46*, X v. Belgium* (dec.).

[65] ECtHR, Factsheet - Protection of reputation

[66] Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right Maria Tzanou, https://academic.oup.com/idpl/article-abstract/3/2/88/709116/Data-protection-as-a-fundamental-right-next-

In addition to the guarantees provided by the ECHR and Charter of Fundamental Rights of the European Union in regard to protection of personal information, there are a number of common European regulations that have played a significant role in developing and ensuring the right to data protection.[67]

III. Data Protection and Persons with Disabilities

Article 22 explicitly protects the personal data of individuals with disabilities in two ways. First, arbitrary or unlawful interferences with personal data can be understood as violations of the right to "privacy" in Article 22(1). Second, Article 22(2) explicitly requires states to protect "the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others." This section will explicitly consider the law that has developed around data protection and whether those protections respond fully to the privacy needs of individuals with disabilities.

Protection of personal data is essential to the rights of individuals with disabilities. Disclosure of personal information could be used to discriminate against them on the basis of their disability, or it could be incorrect or misleading. There are also dignitary harms associated with privacy breaches. This includes loss of dignity inherent in the revelation of personal information without one's consent, as well as harms to one's ability to control their information or to control the portrayal of their identity in public. This section illustrates these issues with the example of the EU General Data Protection Regulation (GDPR), which comes into force in May 2018, as well as privacy protection goals defined by Standard Data Protection Model (SDM).[68] Despite the fact that the GDPR is an EU regulation, it will have an influence on data collection practices for ICT service providers located outside the EU, as long as they process information from EU citizens. As the core of this Chapter is to examine privacy in relation to accessibility, the analysis will focus on privacy principles that may affect diverse users, including people with disabilities. This approach will enable greater understanding of privacy issues related to Article 22, as well as enable the identification of potential harms that may result from privacy violations in the context of accessibility.

To identify potential harms resulting from the privacy violations, we aim to discuss the GDPR and its privacy principles. Although the GDPR does not include provisions related to accessibility, in this chapter, we will demonstrate that the guidelines provided in the GDPR could ensure a right to privacy when obligations for accessibility are taken into account. There are six privacy principles enshrined in the GDPR that focus on data collection and processing: lawfulness, fairness and transparency; data purpose limitation; data minimization; accuracy; storage limitation; *integrity and confidentiality*.[69]

---

to?redirectedFrom=fulltext; The Emergence of Personal Data Protection as a Fundamental Right of the EU Authors (view affiliations) Gloria González Fuster, https://link.springer.com/book/10.1007%2F978-3-319-05023-2

[67] Further analysis of these acts and regulations are included in Section 2.

[68] See Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings (pp. 21–37). http://doi.org/10.1007/978-3-319-06749-0; European Commission. (2016). Regulation (EU) 2016/679 Of The European Parliament AND Of The Council of 27 April 2016. *Official Journal of the European Union*, (April).

[69] European Commission (n 100)

Additionally, the GDPR clearly defines the rights of the data subject (user) in relation to data protection. These are divided into the following groups: *transparency and modality of data*; *information and access to personal data*; *rectification and erasure*; *object and automated individual decision-making*. As we aim to concentrate our discussion on the user's perspective of privacy and on the identification of privacy risks and harms in relation to accessibility, we will consider these rights in the analysis.

The principle of the GDPR are closely related to Art 22, according to which "no person with disabilities [...] shall be subjected to arbitrary or unlawful interference with his or her privacy," and should be protected against attacks on privacy.[70] The issue at stake is how to provide such protections in relation to modern technologies? How can users' privacy be protected in a technological environment, where ubiquitous data collection, analysis, and distribution occurs, and where this process is hidden from the human eye within business models, commercialization strategies and trade secrets?

ICT service providers that follow the specific guidelines defined in legal and technical frameworks, such as GDPR and additionally comply with accessibility guidelines may ensure privacy protections for their users. However, convincing service providers to implement measures for ensuring privacy and accessibility has been an uphill battle for advocates on both sides of the issue. Additionally, lawfulness and fairness can be enhanced by implementing transparency measures, which may result in higher privacy awareness among both users' and service providers.

A. Privacy of Personal Information

In recent research, legal scholars have investigated the impact of new and emerging technologies on privacy.[71] Search engines, used to organize and access content on the web, have now emerged as one of the leading stakeholders in realizing a right to privacy. Google, the most used search engine, processes 1.2 trillion searches per year according to the latest statistics.[72] Each search has the potential to reveal not only basic demographic information about the user, but can be used to produce detailed profiles of an individual's personal beliefs, values, and behaviors.

The data collection practices of Google and other search engines raise several salient problems for privacy. The aggregation of search behaviors over time provides an intimate and comprehensive profile of an individual. Incorrect information or misleading search behaviors may result in potential harms. Search-related data is often used for secondary purposes—e.g., to influence purchasing behavior—and is often disclosed for both commercial and non-commercial purposes.

More recent ICT developments raise even further privacy concerns. The Internet of Things (IoT) is an emerging Internet-based information system that integrates sensors and devices in everyday objects. These objects may interact with individual users through a variety of visual, auditory, or tactile interfaces or may passively collect and distribute data unbeknownst to the user. Media analysts expect the data collection and distribution of IoT devices to significantly expand the collection, analysis, and use of personal information.[73]

These privacy considerations highlight the complex and multifaceted challenges to realizing a right to privacy for persons with disabilities. Persons with disabilities, in particular persons with cognitive disabilities, may experience barriers to accessing information and communications about the privacy practices of ICT goods and services providers. Individuals with disabilities may experience privacy

---

[70] United Nations (n 1)

[71] See Tene, O. (2012). What Google Knows: Privacy and Internet Search Engines. *Utah Law Review, 4*, 1433, 1438.; Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30.

[72] See https://www.reliablesoft.net/top-10-search-engines-in-the-world/ and https://www.reliablesoft.net/top-10-search-engines-in-the-world/

[73] See https://www.theguardian.com/technology/2015/sep/14/data-generation-insights-internet-of-things

violations if they do not have access to accessible information and communication about data aggregation, uses, potential harms, and disclosures.

Fundamentally, whether using a search engine, mobile device or IoT device, the privacy concerns over ICT use revolve around not only the collection of the data but the analysis of the data through a set of techniques known as data mining.[74] Data mining refers to creating new and predictive knowledge by analyzing large-scale data sets using techniques such as machine learning. The analysis of these "big data" sets attempts to uncover relationships between complex behavioral patterns and trends. The question that legal scholars have attempted to answer is whether and to what extent data mining acts as a violation of privacy that ought to be limited by law?

It is worth pointing out that data mining differs substantively from other forms of statistical or demographic analysis. For example, in order to understand the likelihood of someone purchasing an article of clothing online versus in a store, traditional statistical analyses would use data on a generalizable sample's purchasing behaviors to show how often a person from a particular demographic background purchases clothing online versus in a store. Data mining differs by analyzing data that is not directly linked to the outcome in question and uses the relationships among a wide variety of variables to predict and model future behaviors and trends.

The concern over privacy in data mining arises not only due to the collection of an individual's data but also the semantic relationship of the data being collected. Hypothetically, a person with a psychosocial disability, such as autism or bipolar disorder, may decide to publish a blog post under a pseudonym about their experience in psychotherapy. The same person may also maintain various publicly facing social media accounts, such as a LinkedIn account. While the blog posts and the social media accounts are both publicly available, no user accounts or documentation connect the two. Nonetheless, data mining provides an opportunity for service providers to infer an association between the individual's identity as the blogger and the owner of the LinkedIn account through a variety of potential tertiary behavioral variables such as location based data that reveal the individual's movements to and from their psychotherapist's office and place of employment.

In relation to ICT accessibility, data mining is particularly relevant as data about a person with a disability may reveal implicit knowledge about their behavior and disclosure of that knowledge could result in potential harms. In order to fully realize the right to privacy for persons with disabilities, information and communications about how and to what extent data mining could reveal personal information about a person with a disability must be provided in accessible formats including in easy-to-read formats.

B. Protecting Personal Information via Notice and Consent

According to legal scholars such as Reidenberg, Russell, Callen, Qasir, and Norton, providing notice is a fundamental principle of online privacy.[75] Notice and consent mechanisms assume that people have the ability to make decisions about the collection and use of their personal information. [76]

---

[74] See Fulda, J. S. (2000). Data mining and privacy. *Alb. LJ Sci. & Tech., 11*, 105.

[75] Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S., & Norton, T. B. (2015). Privacy harms and the effectiveness of the notice and choice framework. *ISJLP, 11*, 485. Sloan and Warner use to the term informational privacy to describe an individual's decisions about when and how ICT service providers collect and use personal information. See Sloan, R. H., & Warner, R. (2014). Beyond notice and choice: Privacy, norms, and consent. *J. High Tech. L., 14*, 370.

[76] Nissenbaum argues that the typical approach to ensuring privacy online is through transparency and choice. ICT service providers typically provide transparency by issuing a "notice" i.e., - presenting an individual with a privacy policy or terms of service agreement - and an individual makes a choice or "consents" by selecting an option to agree to the notice. Sloan and Warner (n 70) argue that notice and consent relies on an individual's free and informed consent to data collection and use and an individual is aware of the trade-off they are

However, notice and consent has come under criticism, as people typically do not read or understand the complex language and legal jargon used in privacy policies. As a result, people typically do not know the full scope of the privacy rights or the use of their data by ICT service providers. Given the importance of the services provided by ICT vendors and the fact that these services and the accompanying privacy policies are often presented in a "take it or leave it" format, notice and consent may not be meaningful.

This is further compounded by the vast number of privacy policies that an individual may encounter in a day, given that an individual would seemingly have to read, understand, and track the variations among privacy policies for interactions with hundreds or thousands of different ICT service providers.[77] In addition, privacy policies may not indicate whether, how, and when ICT service providers' contract with third parties around the use their data. As a result, an individual is often unaware of the network of ICT service providers that have access to their data. Finally, through data mining techniques discussed previously, an individual's disclosure of information may reveal private information about another individual who was previously unidentified and thus cannot consent in advance.

Advocates,[78] legal scholars,[79] and in some cases regulators such as the US Federal Trade Commission have recommended clearer, shorter, and more standardized privacy policies. However, despite these efforts, no clear guidance exists on whether obligations for accessibility apply to notice and consent frameworks. Clearer, shorter, and more standardized privacy policies would likely ensure the accessibility of information about how ICT service providers are using personal data for some persons with disabilities. However, self-regulatory frameworks for notice and consent[80] have the potential to violate the right to privacy for persons with disabilities if privacy policies are not fully accessible. Accessibility, in this context, must provide a person with a disability, including persons with cognitive or psychosocial disabilities,[81] sufficient knowledge and understanding of an ICT service provider's

---

making in exchanging their private information for access to an ICT service. However, as Nissenbaum questions whether individual's are able to consent freely as the cost of withholding consent may mean being denied the opportunity to participate in the information society. See Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, 140*(4), 32-48.

[77] According to Lazar et al. (no 3), research has shown that it would take 76 working days for an individual to read all of the privacy policies they would encounter in a year.

[78] While privacy advocates such as the Electronic Frontier Foundation have argued that ICT service providers intentionally draft privacy policies to be unreadable (see https://www.eff.org/mention/real-reason-website-and-app-terms-service-are-so-confusing), organizations such as Terms of Service Didn't Read (see https://tosdr.org/) and TOSBack (see https://tosback.org/) provide tools that enable people to interpret and track ICT service providers' privacy policies. However, as Reidenberg et al. (n 70) points out, these tools have had little success.

[79] Sloan and Warner (n 70) have argued for regulating ICT service providers in order to more fully develop set of norms around privacy.

[80] Reidenberg et al. (n 70) has argued that the US has adopted both a regulatory as well as a self-regulatory approach to protecting information privacy through statutory rights and notice and consent respectively.

[81] Legal scholars have extensively analyzed issues related to legal capacity and supported decision making for persons with disabilities, which are highly relevant for notice and consent. See Devi, N., Bickenbach, J., & Stucki, G. (2011). Moving towards substituted or supported decision-making? Article 12 of the Convention on the Rights of Persons with Disabilities. *ALTER-European Journal of Disability Research/Revue Européenne de Recherche sur le Handicap, 5*(4), 249-264.; Flynn, E. (2010). A socio-legal analysis of advocacy for people with disabilities–competing concepts of 'best interests' and empowerment in legislation and policy on statutory advocacy services. *Journal of Social Welfare & Family Law, 32*(1), 23-36.; Flynn, E., & Arstein-Kerslake, A. (2014). Legislating personhood: Realising the right to support in exercising legal capacity. *International Journal of Law in Context, 10*(1), 81-104.; Gooding, P. (2013). Supported decision-making: a rights-based disability concept and its implications for mental health law. *Psychiatry, Psychology and Law, 20*(3), 431-451.

practices around data collection and use and any associated risks and benefits of consent.[82] Under Article 9 of the CRPD, States have an obligation to promulgate privacy relevant accessibility laws and policies.

C. Purpose Limits, Minimization and the Collection of Personal Information

The purpose limitation principle enshrined in some data protection laws such as the EU's General Data Protection Regulation, aims to ensure that the companies collect data only for a specific, explicit and legitimate purpose and that such data will not be processed for other, previously unstated purposes. In a way, this relates to the transparency principle. Considering the end-user, the purpose of the data collection is described in the informed consent, frequently provided as a long and ambiguous text. On the other hand, the purpose limitation principle is addressed to the ICT service providers who must ensure that collected information is purpose-limited and provide privacy protections such as unlinkability or intervenability.

Article 22 clearly defines, that people with disabilities have the same privacy rights as others, and their 'health and rehabilitation information' must be protected. Therefore, companies complying with the purpose limitation principle decrease the risks of potential misuse of secondary data use by ensuring that is it used only for lawful and appropriate purposes.

To illustrate how the purpose limitation relates to information accessibility, consider the following hypothetical case. Two years ago, Bob was involved in a car accident where his daughter and wife were killed. As a result of the accident, Bob was paralyzed and now uses a wheelchair. Since the accident, Bob suffers from severe depression. In order to improve his emotional condition, Bob participates in group therapy provided by a mental health clinic. The clinic uses a third party contractor to store his personal information. The purpose of the information collection has been described to Bob in brief, and he is under the impression that only doctors have access to his personal data and that it will be used solely to improve his well-being. However, after a couple of months of therapy, Bob starts to receive marketing messages from various health insurance companies and health stores. The advertisements are personalized, indicating the fact that he recently lost family, and that he should insure against future accidents as well as insure his wheelchair. These marketing messages increase his depressive episodes and decrease the chance of recovery.

The example illustrates potential harms related to the data purpose limitation when collected information is transferred to a third party. It demonstrates that the violation of this principle may lead to damages resulting from the secondary use of data or misuse of data. The abuse of the principle may result in more tangible harms when it involves health data.

This principle has been reflected in legislation preceding the GDPR.[83] The directive states that ICT service providers must ensure that data is adequate, relevant and not excessive in relation to the purposes for which they are collected or processed. The change brought in by the GDPR is that the data should be limited to what is necessary. The data minimisation principle together with purpose

[82] However, as Nissenbaum (n 71) points out, a transparency paradox exists where plain-language privacy policies may ensure accessibility while simultaneously masking important details. The author argues that an antagonism exists between transparency in textual meaning and practice.
[83] See European Commission. (1995). *EUR-lex, Access to European Union Law.* [Online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 [Accessed September 2017].

limitation, increase the compatibility between the two privacy protection targets - anonymity and unlinkability.

In addition, according to the Article 22, not only the privacy of persons with disabilities but also the communication with that person's family should be protected. Therefore, through principles such as data minimization, online services must ensure the privacy of a particular data subject, as well as communications with their family, friends, and acquaintances.

To emphasize the necessity of data minimization for people with disabilities, consider the following scenario. Alice is 70 years old and as she has aged, she has developed a mobility impairment. To help Alice improve her mobility and autonomy, her family has purchased a smart walking stick, which connects to Alice's mobile device and to send reminders to both Alice and her daughter to go for a walk. The cane additionally measures distances and frequencies of daily exercises and sends alerts if the user has fallen. The information about this data collection was provided to Alice's family during the item purchase. Upon the installation and set-up via a mobile device, Alice did not realize that other data may also be collected. The detailed information about the installation and data processing was included only in the instruction book, written in a small font and with ambiguous language and as such Alice has not read it. The cane manufacturers did not implement appropriate measures for data minimisation and gathered extensive information from the mobile device, such as Alice and her family's names, phone numbers, digital and physical addresses, locations and contacts. Due to a security breach, the collected data became publicly available making her a target for burglary as information about Alice's physical location and behavioral patterns provided an opportunity for someone to break into her house.

The above example illustrates the importance of the data minimization principle. The extensive data collection, poor security measures (e.g., such as weak encryption) and lack of feedback about data breaches may cause serious harms. The collection of unnecessary data, which separately may not be harmful, if aggregated might lead to severe risks and harms, for instance, financial loss, identity theft, blackmail or psychologic injuries, such as insecurity, fear and more.

D. Maintaining Accuracy and Confidentiality of Personal Information

According to the data protection regulations such as the GDPR, the data collected from each user must be accurate and, if necessary, kept up to date. The principle of accuracy enhances some of the privacy rights, such as the right to rectification and erasure of data. The GDPR requires online service providers to enable access to the data in order to amend or erase it in a timely manner. Additionally, accuracy promotes integrity, one of the privacy protection targets defined in the SDM, which states that data should be intact, complete and up-to-date.

The right to data rectification and erasure has strong implications for all users, not to mention people with disabilities, whose personal information frequently contains sensitive, health-related data. Considering such data, inaccuracy may lead to the risks of misdiagnosis from healthcare providers. On the other hand, if such data would become available to the public, it may result in tangible and non-tangible harms.

Consider the following case. John is a young man who has a neuromuscular disorder. As a result, he is continuously on strong medication. As he recently finished his university education, he is searching for a new job. To manage this task he uses an online platform. During the registration for the job-search service, he was required to provide details about his health status. One of the forms required Bob to provide information about his medication, which he was willing to disclose since he wanted to find employment as soon as possible. However, what Bob did not realize, is that this data was aggregated with data from other users and processed by an algorithm. The algorithm incorrectly interpreted Bob's medication as being used to reduce the effects of depression and mental illness.

Such information was sent to his potential employers. As a result of this inaccurate information, Bob, without realizing it, lost his employment opportunity.[84]

In the above scenario, the algorithm aggregating data around users' health information concluded in error that Bob experienced mental illness. Naturally, there are many instances where inaccurate information may expose users to various risks and harms. For instance when an ICT service provider does not comply with the right to data rectification or erasure, exposing false information, which may cause harms such as social exclusion.

In addition, according to the GDPR, data must be processed in a secure manner. Security includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The principle of confidentiality also included in the SDM relates to access control and appropriate methods of authorization. In relation to Article 22 and in general to accessibility, if integrity and confidentiality are violated, there is a danger that personal information of people with disabilities is exposed. This may result in harms, such as financial losses, psychological effects and more.

To understand the value of this principle consider the following scenario. Alice lost her vision 20 years ago. As everyone else, she uses online banking. While in a bank, Alice tries to log in to her personal banking account. To do that, she must use an authorization device. However, she forgot to bring her headset, which she uses to operate her mobile phone and hence, while using the accessibility mode on her mobile phone, she increases the volume and listens to the prompts from the online form. The form asks for her Personal Identification Number (PIN) and password. As she cannot see the keyboard, she uses the text-to-speech option and loudly announces her PIN and password. Alice has no idea about the surroundings and is not aware who can hear her, trusting that she is in a secure environment inside the bank. Unaware of the potential risk, Alice manages to log in and use her bank services. However, days later she becomes the victim of identity theft because someone heard her PIN and password, which Alice re-used in different applications, such as her email account and social media profiles.

The risks and harms resulting from violation of the confidentiality principle may be different. The above example illustrates one potential scenario. There are also harms resulting from unauthorized access to information that may expose and identify and individual and lead to embarrassment or social exclusion, which may disproportionately impact people with disabilities.

E. Transparency

Transparency, as already mentioned, is one of the rights guaranteed to data subjects. In this context, transparency is a guarantee that any information and communication related to data processing is easily accessible, and provided in an understandable manner, with the use of plain and simple language. Perhaps this is one of the most important privacy principles for users, particularly persons with disabilities.

To understand the importance of transparency we can consider the following hypothetical scenario. Alice, who has Parkinson's disease, which typically results in cognitive impairments such as memory losses, wants to install a mobile health application that helps manage symptoms of Parkinson's on her smartphone. In order to install the application, she must agree to the application provider's

[84] While the potential harms resulting from Bob's situation are not exclusively related to his disability, the hypothetical scenario is given to demonstrate that the risks of inaccurate information must be communicated to persons with disabilities in accessible formats and any grievance mechanisms must be accessible to persons with disabilities on an equal basis with others.

privacy policy, which includes provisions to share Alice's data without liability with third-party organizations. Alice, careful about her privacy due to bad experiences in the past, decides to read the policy. She soon discovers that reading the policy is a cumbersome task since the policy's language is complex and uses legal jargon, long sentences and abstract concepts. Additionally, the policy is long and Alice struggles with the cognitive demands to read it. After reading the policy, or more likely skimming it, she decides simply to agree to the policy in order to satisfy her primary goal – to install and use the application. The application provider sells Alice's data to a third party organization that encounters a security breach and exposes Alice's data. Alice receives phishing emails that use information about her Parkinson's to create a fraudulent bill and charge Alice. Suffering from memory issues, Alice pays the bill and becomes a victim of the phishing attempt.

If the information about the application's use of Alice's data would have been provided to her in a transparent – i.e., accessible – manner, Alice would have known that the service provider shares data with third party organizations and that it takes no responsibility for data storage and security breaches. Therefore, considering Alice's bad privacy experiences, it is possible that if she had understood the privacy policy, she may not have installed the application.

This is a simple example of the potential consequences related to transparency and accessibility. There are other aspects of accessibility that could be considered in a similar scenario. For example, the information about data processing could have been inaccessible to people using assistive technologies, such as hearing aids, text-to-speech readers or braille displays. In terms of harms related to the lack of transparency, the financial damages resulting from the security breach could be considered a tangible harm. However, the same scenario could also result in intangible harms, such as loss of confidence, emotional insecurity, loss of trust, or dependence on others to use health and other technologies.

IV. Relationship with Article 9

Privacy law scholar Daniel Solove has argued that traditional ways of understanding privacy are no longer relevant due to the systematic collection of personal information by information and communication technology (ICT) goods and service providers.[85] According to Solove existing privacy theories are "too narrow, too broad, or too vague". The author claims that theorists have attempted to conceptualize the essence of privacy as a single idea applicable across multiple contexts. Solove argues for re-conceptualizing privacy from the bottom-up, as a pluralistic concept shaped by the experiences of individuals and within specific sociocultural contexts. As such, the author argues that privacy consists of a set of factors and interrelated ideas about the collection, analysis and dissemination of information, in particular personal information.

Building on Solove's argument, this Chapter maintains that privacy should be conceptualized based on the experiences of people, in individual contexts, rather than from the abstract language of human rights documents. Realizing the right to privacy for persons with disabilities relates to the invasions of privacy that occur when persons with disabilities engage in social activities. In essence, privacy invasions can substantively affect how and to what extent persons with disabilities participate in society on an equal basis with others. Solove's conceptualization of privacy provides a pluralistic frame for realizing the right to privacy that takes into account the contextual and individual

[85] See Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*: NyU Press.; Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev., 44*, 745.; Solove, D. J. (2009). *Understanding Privacy*: Harvard University Press.

determinants, including social environments and attitudes, of how people interact in society. Rather than focusing on a single overarching connection, Solove recognizes the need for flexibility in realizing a right to privacy as the importance of privacy changes depending on the activity, the individual and their environment.[86]

With the social and political transformations associated with the growth of the information society, the right to privacy has become a pressing legal and social issue. The information society is characterized by exponential growth of ICT, particularly the rapid development, scaling, and mass consumption of portable sensors, as well as the accompanying growth in the capacity to store, communicate, and compute information.[87] Legal scholars have argued that the growth in the adoption of consumer ICT has brought with it the slow but inexorable erosion of personal privacy.[88]

Developments in ICT have significantly affected the right to privacy for persons with disabilities.[89] Lazar, Wentz, and Winckler point out that the right to privacy for persons with disabilities is deeply intertwined with their participation in the information society.[90] They argue that information privacy is relevant for persons with disabilities due to, among other things, their reliance on ICT to a greater degree than others to participate in social life. At the same time, ICT service providers typically do not consider the right to privacy for persons with disabilities. As a result, persons with disabilities are exposed to privacy risks to a greater extent than others. In addition, privacy violations could lead to potential discrimination, in particular in employment, if information about the individual's disability is revealed.

At the crux of the right to privacy for persons with disabilities is the inaccessibility of privacy information and security features.[91] Lazar et al. suggest that as a consequence, a person with a disability will either be deterred from using an ICT product or service or will choose to disclose personal information to someone else in order to use the ICT.[92] Either scenario has the potential to further exclude a person with a disability from society or expose them to privacy threats.

A. Accessibility

Accessibility is a central component of state obligations under the CRPD to ensure that individuals with disabilities are able to participate fully in society and enjoy their rights. Article 9 of the CRPD

---

[86] It is worth pointing out that Solove's reconceptualization of privacy is compatible and in many ways parallels the conceptualization of disability used in the CRPD. In the Preamble, the CRPD recognizes that "disability is an evolving concept and that disability results from the interaction between a person with impairments and the attitudinal and environmental barriers that hinders their full and effective participation in society on an equal basis with others".

[87] See ITU. (2014). *Measuring the information society report*. Retrieved from Geneva, Switzerland; ITU. (2015). *Measuring the information society report*. Retrieved from Geneva, Switzerland; ITU. (2016). *Measuring the information society report*. Retrieved from Geneva, Switzerland.

[88] Koops, B.-J., & Leenes, R. (2005). Code and the slow erosion of privacy. *Mich. Telecomm. & Tech. L. Rev., 12*, 115.

[89] *See, e.g.*, Committee on the Rights of Persons with Disabilities, Concluding Observations in Relation to the Initial Report of Latvia, CRPD/C/LVA/CO/1, ¶ 36 (Aug. 29, 2017) (expressing concern about the privacy of individuals listed on a register and the inability of those individuals to challenge the data collection practices of hospitals) (hereinafter "Concluding Observations on Latvia")

[90] Lazar, J., Wentz, B., & Winckler, M. (2017). Information Privacy and Security as a Human Right for People with Disabilities. In J. Lazar & M. A. Stein (Eds.), *Disability, human rights, and information technology*: University of Pennsylvania Press.

[91] Lazar et al. (n 3) point out that privacy policies online are often provided in a way that is inaccessible to persons with disabilities either due to small text size, complex wording, or incompatibility with the specialized software that persons with disabilities use to access the web such as screen readers.

[92] Lazar, et al., (n 3)

requires states to "take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public."

The obligation to ensure accessibility is reflects the social model of disability that forms the foundation of the CRPD. The social model of disability emphasizes that disability is not a function of any individual's physical or mental condition but is rather a product of barriers in the environment that prevent him or her from participating fully and on a basis of equality with others. (CRPD, Preamble.) This approach to disability requires the state to remove barriers to the enjoyment of rights and to affirmatively create the conditions needed for all to be able to participate meaningfully in society.

Accessibility is important both as a freestanding right and as a precondition for the realization and enjoyment of rights protected under the CRPD.[93] As the CRPD Committee has noted, the accessibility of information is a necessary precondition for a variety of rights, including rights to freedom of expression, to education, and to participation in culture.[94] For example, ninety percent of all books published globally are not available in formats accessible to individuals with print disabilities.[95] This situation—also called the global "book famine"—leaves many of the 285 million blind and visually impaired people around the world unable to participate meaningfully in society. Thus, "Article 9 in particular, cannot be read in isolation, and therefore accessibility has to be applied when other rights in the CRPD such as rights to employment and work, rehabilitation, education and health are applied."[96]

Pursuant to Article 9, states are required to ensure not only the accessibility of physical spaces but also of information and communication technologies. As these forms of technology evolve, individuals with disabilities are increasingly left out of education, professional, social, and cultural opportunities if they are not able to fully participate in the digital world on a basis of equality.[97] Article 9(1) specifically requires the accessibility of "to information and communications, including information and communications technologies and systems," and Article 9(1)(b) calls on states to take appropriate measures, including measures aimed at the "identification and elimination of obstacles and barriers to accessibility," regarding "Information, communications and other services, including electronic services and emergency services." Article 9(2)(g) requires states to take appropriate measures "[t]o promote access for persons with disabilities to new information and communications technologies and systems, including the Internet."

States have several different kind of state obligations under Article 9(2). They are required to respect the right to accessibility by, among other things, creating and monitoring accessibility standards and guidelines, training relevant stakeholders, and ensuring that public buildings and services are accessible. States are also obligated to protect the right to accessibility by ensuring that private entities that provide facilities or services that are open to the public ensure accessibility. Finally, they are also obligated to fulfill the right by promoting assistance and support to individuals with disabilities.

---

[93] General Comment No. 2, para. 36.

[94] *Id.* para. 37, 38, 44.

[95] World Blind Union, http://www.worldblindunion.org/English/our-work/our-priorities/Pages/right-2-read-campaign.aspx

[96] See Della Fina, Cera, and Palmisano (2017).

[97] See Fruchterman (n 81); Jaeger, P. T., Wentz, B., & Bertot, J. C. (2017). The Intersection of Human Rights, Social Justice, the Internet, and Accessibility in Libraries: Access, Educati'on, and Inclusion. In J. Lazar & M. A. Stein (Eds.), *Disability, human rights, and information technology*: University of Pennsylvania Press..

Finally, states are also obligated to seek ways of building accessibility into the design of both physical and digital spaces. Article 9(2)(h) calls on states "[t]o promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and systems become accessible at minimum cost." Design that incorporates accessibility at the outset will be far more effective and cost efficient than efforts to retrofit physical or digital infrastructure after the fact.[98]

Ensuring a right to privacy for persons with disabilities is an important part of States Parties' obligations regarding ICT accessibility. This is demonstrated by the CRPD Committee's General Comment on Article 9. According to paragraph 21 of this Comment, the Committee recognizes that "the [CRPD] includes accessibility as one of its key underlying principles" and acts as "a vital precondition for the effective and equal enjoyment of civil, political, economic, social and cultural rights by persons with disabilities."[99] In other words, in line with prevailing legal scholarship on the topic, accessibility is a cross-cutting issue that relates to all other rights and obligations enshrined in the CRPD.[100] Therefore, obligations for accessibility act as a necessary foundation for effectively realizing a right to privacy for persons with disabilities.

However, the relationship between obligations for ensuring accessibility and realizing a right to privacy for persons with disabilities is not a simple linear relationship. The CRPD Committee recognizes the complicated relationship between accessibility and the other rights enshrined in the CRPD and argues for accessibility to be "addressed in all its complexity, encompassing the physical environment, … information and communication, and services." In order to realize the right to privacy for persons with disabilities, the many possible accessibility-related outcomes must be taken into account across a range of privacy-related contexts.[101] In many social activities, the lack of accessibility of the built environment, of information and communication, and of services may inherently violate a person with a disability's right to privacy.[102]

The CRPD Committee also focuses its analysis of the accessibility of goods and services on an equal basis with others and the identification and elimination of obstacles and barriers to accessibility. These principles—that access should be on an equal basis with others and that access requires the elimination of barriers—delineate the relationship between obligations for accessibility and the right to privacy. Essentially, these principles suggest that barriers to accessibility must be eliminated in order to ensure that persons with disabilities have equal access to goods and services. This means that all information and communications associated with the use or consumption of any goods and services, which may include information and communications related to how ICT service providers use personal information, must be accessible for persons with disabilities on an equal basis with

---

[98] See Lazar, J., & Stein, M. A. (2017). Disability, human rights, and information technology: University of Pennsylvania Press.

[99] The CRPD Committee goes on to state that accessibility acts as a "pre-condition for persons with disabilities to participate fully and equally in society and enjoy effectively all their human rights and fundamental freedoms".

[100] See Blanck (2014).

[101] Winance has argued that conceptualizations of accessibility have yet to fully account for the variety of contextual factors that interact with and frame the experiences of persons with disabilities. In addition, the author argues that accessibility involves a reciprocal interaction between an individual and their environment, which changes over time. In terms of privacy, the accessibility of ICT service providers' privacy policies vary depending on the particular context and the interaction between the individual and the physical and digital environments. That these interactions and contexts change over time further complicates how policymakers and ICT developers understand and ensure a right to privacy in light of the myriad potential accessibility barriers that a person with a disability may experience using ICT. See Winance, M. (2014). Universal design and the challenge of diversity: Reflections on the principles of UD, based on empirical research of people's mobility. Disability and rehabilitation, 36(16), 1334-1343.

[102] Examples of these activities are considered in more detail in Section 2.

others and that any barriers that persons with disabilities experience accessing information and communications must be removed.

The CRPD Committee argues that barriers to accessibility constitute discrimination. Persons with disabilities should have equal access to goods, products, and services that are open or provided to the public in a manner that ensures their effective and equal access and respects their dignity. The Committee recognizes the relevance of ICT as a means for participating in society, arguing "[n]ew technologies can be used to promote the full and equal participation of persons with disabilities in society, but only if they are designed and produced in a way that ensures their accessibility." ICT accessibility is a relevant aspect of realizing the right to privacy as new ICT has provided ever-increasing and potentially harmful ways for businesses, government and other citizens to collect, analyze, and disseminate personal information.[103]

The CRPD Committee goes on to argue that accessible information and communications "should be available in easy-to-read formats and augmentative and alternative modes and methods to persons with disabilities who use such formats, modes and methods." Therefore, one mechanism for realizing the right to privacy is by providing information and communications in accessible and alternative formats including easy-to-read formats.

However, the CRPD Committee's focus on the design of technology as a mechanism for social participation does not consider the impact that obligations for ICT accessibility may have on the realization of other rights, such as the right to privacy.[104] While the Committee has not explicitly recognized the relationship between ICT accessibility and the right to privacy, legal scholars have, for nearly 50 years considered the relationship between ICT service providers' collection and analysis of personal information and privacy.[105]

B. The Marrakesh Treaty

A new international treaty addressing the accessibility of printed materials illustrates some of the ways in which the privacy of individuals with disabilities can be affected by measures to ensure greater accessibility.

Although the digitization of books and other printed material means that there are greater opportunities for accessibility than ever before, roadblocks remain.[106] A significant roadblock to the accessibility of digital works is copyright law. Even though new technologies make it relatively easy for many of those with print disabilities to convert digital works to accessible forms, copyright law requires that they obtain a license from the copyright owner before doing so. A separate license is also required any time an accessible version is shared across borders.

A new international treaty—the Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired, or Otherwise Print Disabled (the Marrakesh Treaty)—is aimed at addressing the role that copyright plays in limiting the accessibility of printed works. The Marrakesh Treaty creates mandatory exceptions to copyright for the benefit of individuals with print

---

[103] This issue is further explored in the rest of this Section.

[104] The CRPD Committee recognizes the intersection of Article 9 with many of the other rights and obligations enshrined in the CRPD including, among others, equality and non-discrimination (Article 5); humanitarian emergencies (Article 11); access to justice (Article 13); independent living (Article 19); freedom of expression and opinion (Article 21); access to information (Article 21); education (Article 24); health (Article 25); employment (Article 27); social protection (Article 28); participation in political and social life (Article 29); and participation in cultural life, recreation, and leisure and sport (Article 30).

[105] See for example Miller, A. R. (1969). Personal privacy in the computer age: The challenge of a new technology in an information-oriented society. *Michigan Law Review, 67*(6), 1089-1246.

[106] See Fruchterman, J. (2017). E-Books and Human Rights. In J. Lazar & M. A. Stein (Eds.), *Disability, human rights, and information technology*: University of Pennsylvania Press. p. 145 "Given the incredible accessibility advantages of the e-book, it has been a great irony that the e-book has not been very accessible."

disabilities. States that ratify the treaty are required to enact exceptions to copyright that allow beneficiaries — individuals with print disabilities and institutions that provide services to them — to create accessible versions of printed works and also share them across borders. The primary objective of the Marrakesh Treaty is to expand the availability of copyrighted works to individuals with print disabilities around the world.

The Marrakesh Treaty uses the legal tools of copyright to advance human rights ends.[107] In particular, it is one of the steps that States Parties to the CRPD can take to ensure that intellectual property laws do not prevent disabled persons from accessing books and other cultural materials. Article 30(3) of the CRPD provides that States "shall take all appropriate steps, in accordance with international law, to ensure that laws protecting intellectual property rights do not constitute an unreasonable or discriminatory barrier to access by persons with disabilities to cultural materials." Over fifty countries signed the treaty at the conclusion of the diplomatic conference in Marrakesh in June 2013. As of September 2017, eighty countries had signed and thirty-one had ratified or acceded to the treaty.

The Marrakesh Treaty reaffirms the importance of privacy of those who are the beneficiaries of the treaty. Article 8 provides, "In the implementation of the limitations and exceptions provided for in this Treaty, Contracting Parties shall endeavor to protect the privacy of beneficiary persons on an equal basis with others." Thus, the treaty explicitly requires States Parties to ensure that in the process of ensuring accessibility, they do not infringe on the privacy rights of those benefitted by the treaty.

There are several ways in which the privacy of treaty beneficiaries may be affected by the treaty. First, the legal obligations of the treaty impose data collection requirements that could implicate privacy. The treaty allows both beneficiaries and "authorized entities" to make and share accessible format versions of books. Article 2(c)(iv) of the treaty defines an authorized entity as one that "establishes and follows its own practices . . . to maintain due care in, and records of, its handling of copies of works, while respecting the privacy of beneficiary persons in accordance with Article 8 on respect for privacy." Although the treaty explicitly provides that authorized entities should develop and implement their own procedures for protecting privacy, copyright owners may pressure these entities to collect and keep data about beneficiaries in order to guard against the possibility that a work may be accessed by an individual who is not a beneficiary under the treaty. Data collection may also be required to monitor the extent to which the treaty is being used to benefit individuals with print disabilities.[108]

Efforts to implement the Marrakesh Treaty also illustrate the particular challenges of protecting privacy while ensuring accessibility of information and communication technologies. Threats to privacy for persons with disabilities are to some extent general threats, since digitization and new technologies for collecting, storing, and sharing information affect the privacy rights of every individual. Individuals with disabilities are particularly impacted by these developments, however. First, they are more likely to rely on new technologies for accessibility purposes, thus increasing the opportunities for data about them to be collected, stored and shared. Second, efforts to render digital information accessible could create new opportunities for data collection and processing. Unless remedied, the differential impact of these developments on the privacy of individuals with disabilities can constitute discrimination.

C. Accessibility of Notice and Consent

[107] See Helfer, L. R., Land, M. K., Okediji, R. L., & Reichman, J. H. (2017). *The World Blind Union Guide to the Marrakesh Treaty*: Oxford University Press.
[108] Id.

The deployment of digital technologies creates particular privacy challenges in two ways. First, digitized information is much easier to collect. New technologies — whether internet technologies, physical sensors, or electronic books — can capture, record, and store a range of data about users without their knowledge. Second, digitized information is also much more easily stored and shared online. Libraries with digitized records can much more easily share information about patrons than those with paper records. The result is that using new technologies to increase accessibility can also magnify and exacerbate privacy challenges for individuals with disabilities.

Despite technology trends that have given rise to the potential for State and non-State actors to use ICT to surveill the public and potentially violate the right to privacy for persons with disaiblities, recent policy innovations and research have provided a framework for securing a right to privacy for persons with disabilities in light of obligations for ICT accessibility. Crawford and Schultz have argued for adopting procedural data due process as a mechanism for mitigating potential privacy harms associated with data mining.[109] Procedural data due process acts as a form of ex-post regulation where ICT service providers issue notice about their data collection and analysis processes and provide an opportunity for individuals to petition ICT service providers for information about the collection of their personal information and to correct any potential inaccuracies.

Recent policy innovations have included mechanisms for providing notice as a part of a procedural data due process requirement. In 2015, the California legislature passed the California Electronic Communications Privacy Act (CalECPA), which, among other things, protects information privacy for electronic communications by regulating service providers. CalECPA requires service providers, including organizations or intermediaries that send, store, or receive electronic communications, to get a warrant before requiring a third party to disclose information or directly accessing information on a device.[110] CalECPA goes further than prior laws protecting communications privacy by requiring unrelated information obtained by public sector organizations to be made unavailable and providing that those organizations obtaining information must notify the intended targets as to the type of information that has been requested. In addition, in the event that a target cannot be identified, the California Department of Justice must publish a public announcement reporting on the information that was obtained.

In the context of ensuring a right to privacy for persons with disabilities, policy innovations such as CalECPA provides a useful opportunity to provide information about the surveillance activities conducted by the California State government. However, provisions for disclosure of surveillance activities such as those provided for in CalECPA must be accessible to persons with disabilities. California's Unruh Civil Rights Act, the US Rehabilitation Act, and the Americans with Disabilities Act require public and private sector organizations in California to ensure access to ICT for persons with disabilities.[111] Presumably, disclosing surveillance activities would also fall under this requirement. Therefore, in order to ensure a right to privacy for persons with disabilities in California, State and non-State organizations must identify an effective mechanism for ensuring access to surveillance related disclosures including by providing easy-to-read versions and making available electronic information that adheres to international standards for accessibility.[112]

---

[109] Due process typically involves different forms of notification and adjudication. See Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev., 55*, 93.

[110] Freiwald provides further detail on the provisions of CalECPA regarding the standard procedures for warrant applications in California including probably cause and the filing of an affidavit, see Freiwald, S. (2017). At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA). *BERKELEY TECHNOLOGY LAW JOURNAL, 31*(1).

[111] For a full analysis of US legislation concerning ICT accessibility, see Blanck (2014).

[112] For example, accessible information could adhere to Section 508 of the Rehabilitation Act or to ISO/IEC 40500:2012

At best, providing notice and consent provides an incomplete mechanism for preventing harms related to breaches of information privacy. Empirical legal scholars have investigated the relationship between notice and consent frameworks and practical privacy concerns by examining privacy-related litigation and enforcement actions in the US.[113] From a dataset of complaints, legal scholars have created a typology of latent privacy harms, which includes unauthorized disclosure of personal information, surreptitious collection of personal information, and unlawful retention of personal information.

Scholars have argued that unauthorized disclosure and surreptitious collection harms may be avoided by providing an effective mechanism for notice and consent.[114] Unauthorized disclosure harms typically involve personal information collected through websites and distributed to third parties without permission. Surreptitious collection harms typically involve personal information collected without the knowledge of the individual. Notices must be "complete, accurate and specific" to avoid unauthorized disclosure harms and must describe "how, with whom, and for what purpose" personal information will be shared. Similarly, if the notice covers all the data and methods used to store and share personal information, surreptitious collection harms may also be avoided.

However, notice and consent may only partially resolve the harms associated with unlawful data retention. Unlawful retention harms relate to personal information that is stored after an individual terminates their relationship with the ICT service provider. While notices that provide accurate inforation regarding the duration that data will be retained may alleviate privacy harms, notices that assert the right to retain data indefinitely or only vaguely define the period of retention may be perceived as a privacy violation.

In the context of the right to privacy for persons with disabilities, privacy harms associated with unauthorized disclosure, surreptitious collection, and unlawful retention of personal information cannot be mitigated by a mechanism for notice and consent where the information being provided is not designed to be accessible for persons with disabilities. The challenge, as Nissenbaum points out, is that a paradox arises around the level of detail included in the notice.[115] Essentially, plain-language notices may hide details around data collection, storage, and distribution and may result in a potential harm. The issue of providing complete, accurate, and specific notices is particularly relevant for persons with cognitive disabilities as accessibility advocates have argued for providing information clearly and simply in order to ensure persons with cognitive disabilities have access to that information.[116] However, the extent to which a notice can be written clearly and simply without hiding details around an organization's privacy practices has yet to be taken up in the research literature or in policy.

V. Concluding Remarks

This Chapter has argued that for persons with disabilities living in the information society, the right to privacy and ICT accessibility are inextricably linked. The examples provided in Section 2 demonstrate a variety of potential risks and harms for people with disabilities that may result from the interaction between a failure to ensure accessibility and a violation of privacy. The risks and harms may include social exclusion, economic loss, physical harm, exposure of personal information and more. One way to overcome the challenges and ensure information privacy for people with disabilities is to follow accessibility guidelines defined in law and policy.

---

[113] See Reidenberg et al. (n 70).
[114] Ibid.
[115] Nissenbaum (n 71)
[116] WebAIM's position on writing clearly and simply is available at https://webaim.org/techniques/writing/.

While laws such as the GDPR and CalECPA provide an overview of principles and requirements guaranteeing ICT users' privacy, they do not explicitly deal with the issue of accessibility. To achieve 'privacy for all' the systems' designers and developers must comply national and international privacy laws as well as follow international accessibility standards, which typically aim to ensure that ICT is perceivable, operable, understandable and robust.[117] Industry standards such as the Authoring Tool Accessibility Guidelines (ATAG) also provide technical specifications to ensure that ICT is usable with assistive technologies.[118] There are also national standards providing guidance on accessibility requirements, for instance the British Standard (BS) 8878 and Section 508 of the US Rehabilitation Act.

However, due to the complex and multidimensional nature of the relationship between privacy and accessibility, legal compliance and industry guidelines may not sufficiently ensure a person with a disability's privacy. To improve privacy, ICT designers should follow well-defined approaches for ensuring usability such as following a human-centered design approach to ICT development. The design of human-centered privacy enables the identification of privacy issues that may occur among diverse populations, including people with disabilities.

To conclude, a right privacy may only be realized when the ICT goods and services are designed according to privacy, accessibility and usability guidelines. However, ICT service providers frequently do not comply with privacy requirements, the information provided to end users is not transparent, users are not aware of how their data is used, the risks of data disclosure or the potential harms that may result from it.[119]

As people lose control over their personal information, the numbers of problems around privacy in ICT grows further complicated by the constantly evolving technological landscape.[120] IoT devices, such as interconnected applications and smart homes have the potential to collect ever more increasing volumes of data. In such environments, which often lack traditional screen-based interfaces, data collection is ubiquitous, and it is difficult to provide users with adequate notice about the processing of their personal information. It is also practically problematic for ICT service providers to ensure data minimization and data rectification or erasure.

In regards to Article 22 and accessibility, there is a necessity for future research and policymakers to develop guidelines and good practices concerning the right to privacy for people with disabilities in the information society. Their data is especially exposed to risks, since they frequently depend on assistive technologies and are forced to disclose large volumes of sensitive information to technology providers.

Acknowledgements

[117] ISO/IEC 40500:2012

[118] For example accessible Rich Internet Applications.

[119] See Sun Lim, Hichang Cho, & Rivera-Sanchez, M. (2009). A multinational study on online privacy: global concerns and local responses. *New Media & Society*, *11*(3), 395–416. http://doi.org/10.1177/1461444808101618; Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. *Usable Privacy and Security.* 39–52.; European Union. (2016). Directive 2016/680 of the European Parliament and the Council of the European Union. *Official Journal of the European Communities*, *2014*(April), 1–43.

[120] See Abaker, I., Hashem, T., Yaqoob, I., Anuar, B., Mokhtar, S., Gani, A., & Khan, S. U. (2014). The rise of "big data" on cloud computing_ Review and open research issues. Information Systems, 47, 98–115. http://doi.org/10.1016/j.is.2014.07.006; Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. http://doi.org/10.1016/j.chb.2008.08.006.

The authors would like to express their sincere gratitude to the editors of this volume as well as the peer-reviewers without whose substantive and useful feedback, this contribution would not have been possible. In addition, the authors would like to recognize that this work is partially funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 675730.