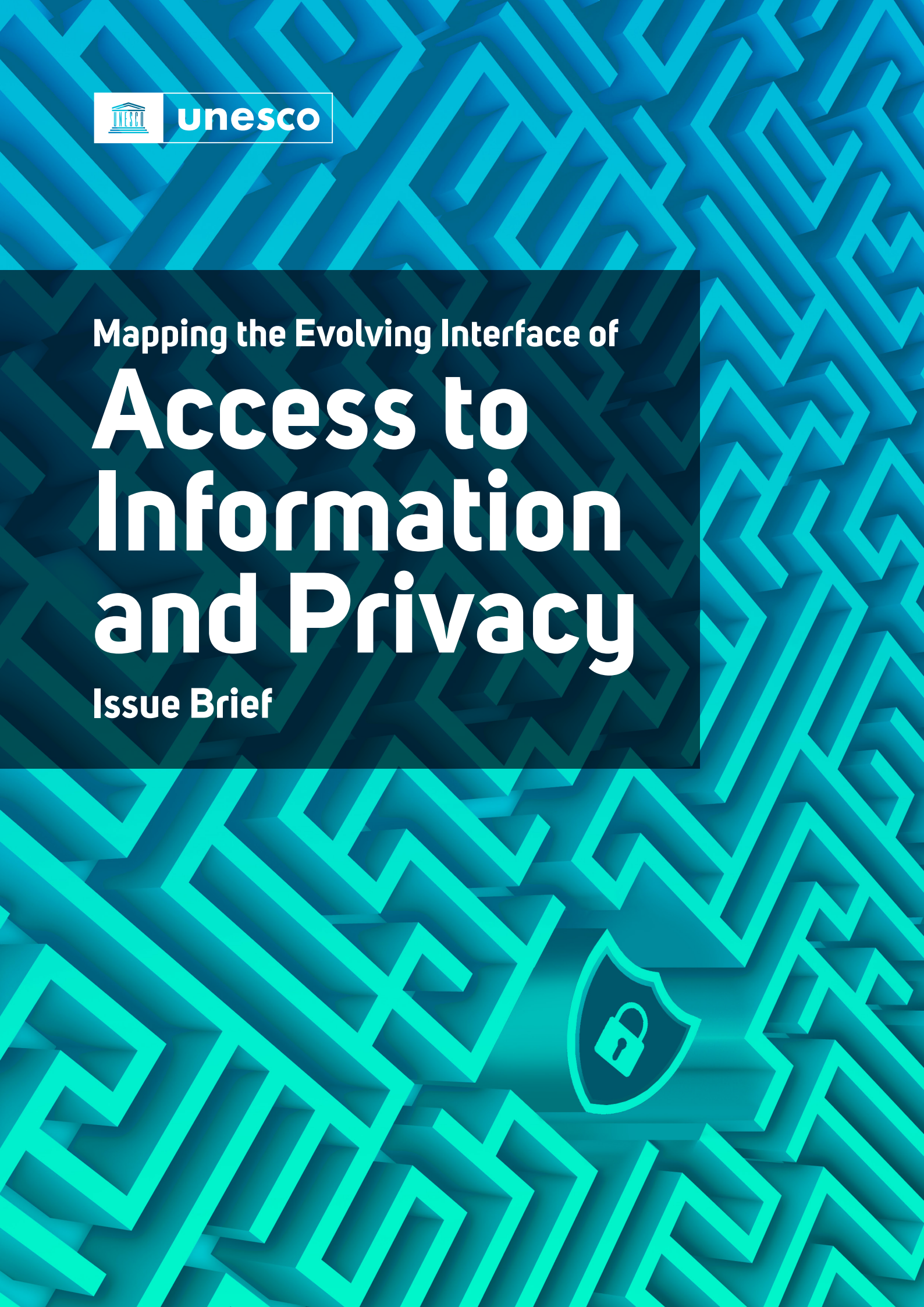
unesco

Mapping the Evolving Interface of

Access to Information and Privacy

Issue Brief

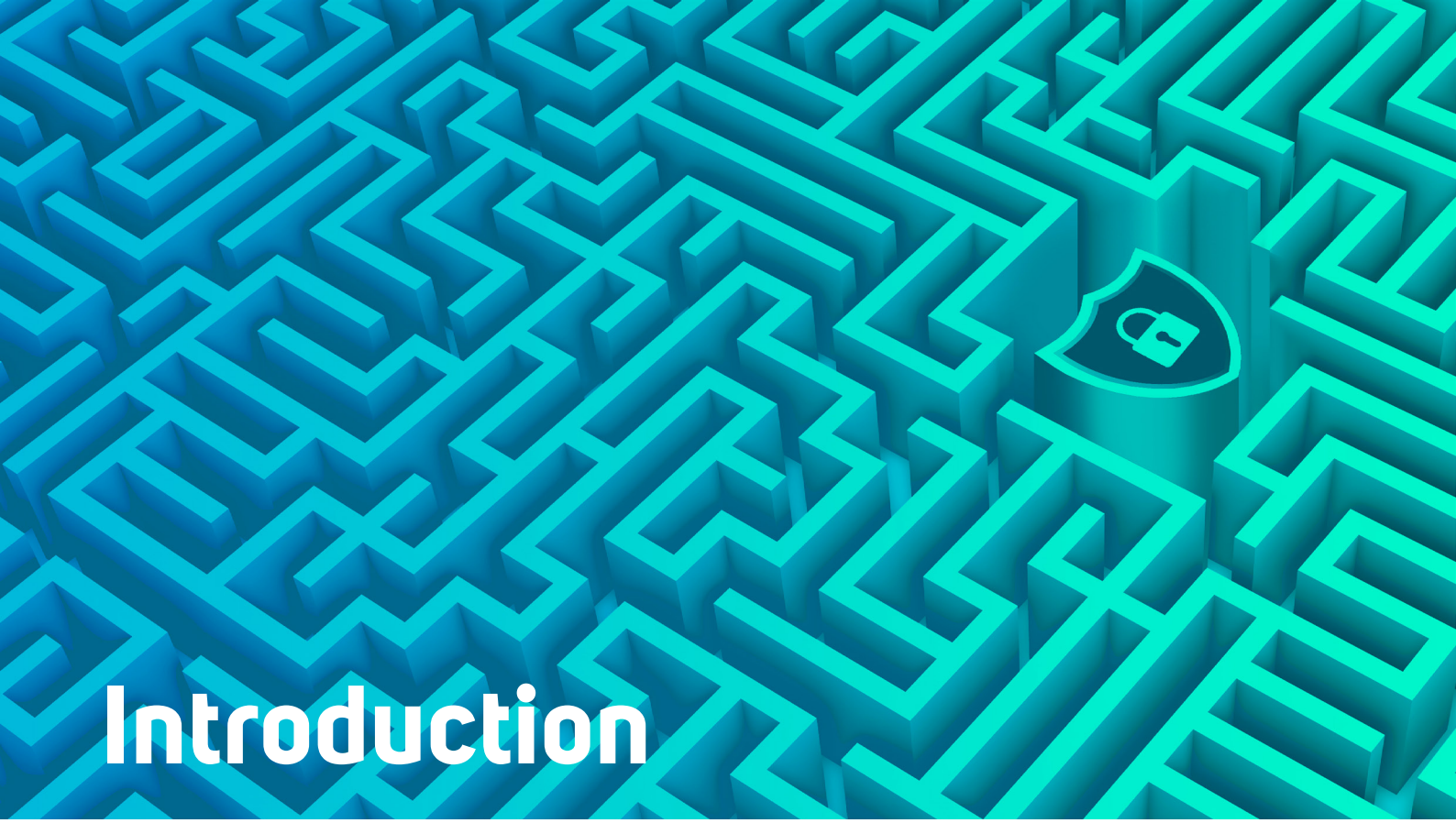


Document code: CI/UAI/2022/56

About the Author:

Dr Lida Ayoubi is a Senior Lecturer in Law at the Auckland University of Technology (AUT) Law School in New Zealand, specialising in public international law and human rights law, including the right to access to information and its interface with other human rights. She has researched, published, and presented extensively on various human rights issues. She holds a PhD in Law from the Victoria University of Wellington in New Zealand, an LLM in International Human Rights Law from Lund University in Sweden where she was also a research intern at the Raoul Wallenberg Institute of Human Rights, and an LLB from the University of Tehran in Iran.

Design and layout: Trigeon



Introduction

Access to information (ATI) is integral to the realisation of human rights. Much like other human rights, however, the right to access to information (RTI) is not without limits. Legal, justifiably necessary, and proportionate limits can be imposed on the public's right to access to information. One such limit is when there is a need to ensure the respect for and protection of the individual's right to privacy.

That the rights to information and to privacy intersect has become increasingly obvious and important, in no small part due to the growth of the Internet and digital technologies, particularly in relation to the collection and use of personal data. The evolving landscape of communication and access to information means that digital and online tools and platforms continue to further dominate how information is created and shared. With that come challenges of protecting privacy while maximising access to information.

This policy brief examines the interface of the right to access to information with the right to privacy, including the right to the protection of personal data, with a focus on access to information and privacy legislation globally. Other UNESCO publications, in particular targeting judicial actors, have previously examined the interface of access to information and privacy as it relates to the use of surveillance technologies for national security purposes, press freedom and privacy of individuals, the protection of journalists and their sources, access to public data, and cross-border data flow.[1]

Both access to information and privacy are human rights that are essential to sustainable development and to the achievement of the Sustainable Development Goals (SDGs), in particular the SDG 16 for the promotion of just, peaceful and inclusive societies. However, the interests that each right protects may pull in different directions. This policy brief canvases the main themes at the intersection of the rights to information and privacy, while providing examples from legislative frameworks of the UN Member States. It concludes by identifying normative steps that Member States can take in better addressing the identified challenges.

1. UNESCO, Guidelines for Judicial Actors on Privacy and Data Protection, (UNESCO, 2022); See also, UNESCO, Global Toolkit for Judicial Actors: International legal standards on freedom of expression, access to information and safety of journalists, (UNESCO, 2021).

1. Background and context

The ever-growing technological developments in the creation, storage and communication of information and data, especially online, have created novel challenges for the protection of the public's access to information, the privacy of the individuals, and the balancing of the two. The increasing challenges to securing the freedom of the press and the provision of accurate and accessible information, particularly in the current complex landscape of the prevalence of disinformation and misinformation, amplified during and in the aftermath of the COVID-19 pandemic, add to the difficulty of protecting and balancing of the two rights.

Access to information, as part of the right to freedom of expression,[2] is the right to seek, receive and impart information including an individual's own personal data. According to the Human Rights Committee in its General Comment No. 34, "such information includes records held by a public body, regardless of the form in which the information is stored, its source and the date of production."[3] All branches of the government, as well as other entities that perform public functions, have an obligation to facilitate access to information they hold.[4]

There is a strong connection between the right to access to information and the right to privacy,[5] and since they both enable the realisation of other human rights, they should be considered as complementary rights.[6] The Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted in 2019 by the African Commission on Human and Peoples' Rights, states that "freedom of expression [that encompasses the Right To Information] and privacy are mutually reinforcing rights that are essential for human dignity and the overall promotion and protection of human and peoples' rights".[7]

Notwithstanding both rights' complementarity, each right has also been used to limit the enforcement of the other. Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR) stipulates that the right to information can be limited, only if provided by law and necessary for respect of the rights or reputations of others or for the protection of national security, public order, or of public health or morals.[8] Each of these terms are open for interpretation in the context of the national legislation of the respective Member State. Political systems could also determine the application of the exceptions. The Human Rights Committee has also recognised the need for such limits to be proportionate.[9] While such restrictions in some cases may be legitimate, limiting the public's right to access to information to protect the privacy of an individual is not without harm.

On the other hand, access to information of public

2. Universal Declaration of Human Rights (UDHR), Article 19; International Covenant on Civil and Political Rights (ICCRP), Article 19.

3. Human Rights Committee (HRC), General Comment No. 34 on Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011, at [18].

4. Ibid, at [7] and [18].

5. UDHR, art 12; ICCPR, art 17; International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families 1990, art 14; Convention on the Rights of the Child (CRC), art 16; American Convention of Human Rights (ACHR), art 11.2, European Convention on Human Rights (ECHR), art 8; African Charter on Human and Peoples' Rights; Arab Charter on Human Rights arts 16 and 8.

6. UNESCO, Guidelines for Judicial Actors on Privacy and Data Protection, (UNESCO, 2022), at 4.

7. Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples' Rights at its 65th Ordinary Session held from 21 October to 10 November 2019 in Banjul, The Gambia.

8. The test for the legitimacy of a limit on the rights in article 19 is sometimes referred to as a three-part test which requires that any restriction on freedom of expression should be provided for by law, pursue a legitimate aim, and be necessary for a legitimate purpose. See UNESCO, The Legitimate Limits to Freedom of Expression: the Three-Part Test, https://www.youtube.com/watch?v=Wg8fVtHP-Dag, accessed 2 August 2022.

9. HRC, General Comment No. 34, at [22].

interest can be used to limit an individual's right to privacy. Both these issues and their respective complexities are discussed in this policy brief. International standards advise that restrictions on rights should be the least intrusive possible, in other words respecting the essence of the affected right to the maximum degree.

The right to information and the right to privacy are increasingly interconnected in relation to the collection, storing, processing, and use of personal data. In principle, individuals should be able to ascertain whether, and how, any of their personal data is stored by public bodies in accordance with Article 17 of the ICCPR,[10] and to be able to access that data as part of their right to access to information.[11] Treatment of personal data also creates privacy concerns which intertwines with the right to access to information. The rise of massive data operations in the private sector, including the commoditisation of data by specialised brokers and aggregators, is a recent factor. Some data brokers engage in the collection of personal information to be sold on to others for different purposes[12]. It raises questions of how the public's right to information may apply to this sphere and/or how it may apply when Governments are purchasers of such services[13].

Some of the privacy concerns regarding the use of big data that focuses on particular individuals or groups may be addressed through anonymizing the date. This does not, however, address access to personal information concerns as by doing so it may become difficult for individuals or even the data holder to access the personal data.

Another concern is the governments' use of big data, especially that held by private sector, for intelligence and surveillance purposes which may not be the use individuals agreed to or are aware of. As Reyman explains, much of the commodified data collected by private sector, e.g. on social media platforms, is collected through "tacit agreements that users enter into, and a set of unspoken assumptions that govern who owns what is created and how it circulates"[14]. This lack of transparency would also impact individuals' right to access to personal information due to the lack of transparency around whether a public or private entity is holding and using the personal data.

Finally, another concern is the bulk collection of personal data by private sector entities, such as data brokers, from public records creating what commentators call a "digital biography" of an individual. This raises privacy concerns as well as access to the digital biography and therein contained personal data and information by the targeted individual[15].

The 2030 Agenda for Sustainable Development, in its Sustainable Development Goal 16, aims to ensure public access to information as part of the realisation of the broader right to access to information. The SDG Indicator 16.10.2 is used for assessing progress on the reporting on statutory and/or policy guarantees for public access to information. One of the "Principles of Access to Information"[16] which is of relevance to this policy brief is the principle of "limited exemptions" to the right to information.

10. HRC, General Comment No. 16 on Article 17: Right to Privacy, UN Doc HRI/GEN/1/Rev.9 (Vol.1) (1988), at [10].
11. Universal Declaration of Human Rights (UDHR), Article 19; International Covenant on Civil and Political Rights (ICCRP), Article 19.
12. HRC, General Comment No. 34, at [18].
13. Ibid, at 2.
14. Jessica Reyman, "User Data on the Social Web: Authorship, Agency, and Appropriation" (2013) 75(5) College English, at 514.
15. Kirsten Martin and Helen Nissenbaum, "Privacy Interests in Public Records: An Empirical Investigation" (2017) 31 Harvard Journal of Law and Technology, at 120.
16. SDG indicator metadata, 2021

2. Challenges and themes at the interface of ATI and privacy

2.1 Diverse definitions

Many of the concepts at the intersection of the right to information and the right to privacy do not have a universal definition. In their Access to Information and/or privacy laws, countries have adopted varying definitions of privacy,[17] personal data, personal information, information authority, public authority, private body or entity, and confidential information, among others. Some laws may not provide a definition altogether.

The concept of privacy and its precise parameters are hard to define. The ambiguity in the concept of privacy has led to a myriad of definitions that are "so wide-ranging and diverse that they have significantly contributed to the [...] common claim that the concept of privacy is incoherent."[18] Scholars have considered the different ways that countries have approached the definition of privacy and the merits and shortcomings of each of these approaches.[19]

International and regional human rights instruments do **not** define the concept of privacy itself but provide similar keywords when referring to privacy interests that have shaped the formation of an understanding of the concept. These keywords include one's family,[20] home,[21] correspondence,[22] honour and reputation,[23] dignity,[24] and private and family life.[25]

While the African Charter on Human and Peoples' Rights does not mention privacy or any of the abovementioned keywords, its Article 4 states that every human being is entitled to respect for "the integrity of his person". The concept of integrity can arguably extend to include one's privacy.

When discussing the privacy exemptions to access to information, the 2020 Inter-American Model Law 2.0 on Access to Public Information mentions the protection of "the right to privacy, including privacy related to life, health or safety, as well as the right to honor and to one's image".[26]

The 'conceptual plasticity' of the concepts of "privacy" and "private life" has meant that the judicial interpretation of these concepts is constantly evolving.[27] In a recent judgment, the EU General Court considered whether the publication of a press release regarding the discovery of research funding fraud at a Greek university constituted a breach of privacy of the lead researcher with regard to the processing of their personal data, under the EU Regulation 2018/1725. The press release did not provide the name or other specific identifying information of the researcher but included the amount of funding, the number of researchers involved, and other additional information.

17. Toby Mendel et al., "Global Survey on Internet Privacy and Freedom of Expression" (UNESCO Series on Internet Freedom, UNESCO, 2012) at [9].
18. Bert-Jaap Koops and Maša Galič, "Unity in Privacy Diversity: A Kaleidoscopic View of Privacy Definitions" (2021) 73(2) South Carolina Law Review, at 4.
19. See for a discussion of the different approaches to defining privacy: Adam Moore, "Toward Informational Privacy Rights" (2007) 44 San Diego Law Review, at 811-818; Daniel Solove, "A Taxonomy of Privacy" (2006) 154(3) University of Pennsylvania Law Review 477; James Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 The Yale Law Journal 1151;and, Bert-Jaap Koops et al., "A Typology of Privacy" (2017) 38(2) University of Pennsylvania Journal of International Law 483.
20. UDHR, art 12; ICCPR, art 17; Convention on the Rights of the Child (CRC), art 16; ACHR, art 11.
21. Ibid; European Convention on Human Rights (ECHR), art 8; American Convention on Human Rights (ACHR), art 11.
22. Ibid.
23. UDHR, art 12; ICCPR, art 17; CRC, art 16; ACHR, art 11.
24. ACHR, art 11
25. ECHR, art 8; ACHR, art 11.
26. Art 32(1)(a). The 2010 Model Inter-American Law on Access to Public Information in its art 41(a)(1) also mentions the protection of "right to privacy, including life, health, or safety"
27. Guidelines for Judicial Actors on Privacy and Data Protection, supra note 1, at 5.

The Court held that personal data relates to "any information relating to an identified or identifiable person" which "directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more specific elements specific to his physical, physiological, genetic, psychological, economic, cultural or social identity" would help identify an individual.[28]

In this case, the Court concluded that the information in the press release did not constitute personal data and subsequently there was not a breach of privacy.[29]

Lack of clear definitions in privacy and/or ATI laws means that the scope of the interests protected would be open to interpretation by information officers, commissioners, ministers, courts, or other stakeholders, creating fragmented and potentially conflicting approaches to access to information and privacy.

The relative incoherence of the definition of privacy and other related concepts also means that their definition may vary greatly from State to State. A clear example of this would be the difference in countries' legislative approaches where the concepts of personal information or personal data are used. In New Zealand, for example, the Privacy Act 2020 refers to "personal information" and defines it as "information about an identifiable individual"[30] while in Europe, the terminology used is "personal data".[31]

This and other discrepancies would create difficulties when implementing rules and regulations around access to information and privacy, particularly in relation to cross-border flow and protection of information, and can lead to unintended breaches of one or both rights. This may also lead to additional challenges for effective impact assessment, data collection, reporting, and review of appeal requests related to these rights.

2.2. Safeguarding the right to access to personal data

Access to information is recognised by the Human Rights Council as crucial for the "promotion of personal autonomy".[32] The principle of habeas data is widely recognised as an essential part of the right to information.[33] Habeas Data is an action that is brought before the courts to allow the protection of the individual's image, privacy, honour, self-determination of information and freedom of information of a person. In his 2021 Our Common Agenda report, the UN Secretary-General specifically highlighted the need for protection of personal data in the digital and online spheres. The report recommends the development of internationally shared principles to address complex digital issues including "providing people with options as to how their data is used".[34]

The positive obligation on States to safeguard personal information and facilitate access for individuals to their own data is also a sign of "the move from a diminutive conceptualization of privacy as the right to be let alone to an expanded sphere of private life rooted in the realization of human dignity".[35]

The right to access to an individual's own personal data has multiple components. First, every individual should "have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes". Second, every individual should be able to find out which public authorities or private individuals or bodies own, control and/or access their personal data, or may do so. Finally, every individual should have the right to request the rectification or elimination of incorrect data or data "collected or processed contrary to the provisions of the law".[36]

28. OC v European Commission, Case T-384/20, Judgment of the General Court (Ninth Chamber) of 4 May 2022, at [44].
29. Ibid, at [91].
30. Privacy Act 2020, s 7.
31. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, art 4.
32. Human Rights Council, Report of the Office of the UN High Commissioner for Human Rights: Freedom of opinion and of expression, A/HRC/49/38, at [12].
33. See for example, HRC, General Comment No. 34, at [18]; The Inter-American Commission on Human Rights and Office of the Special Rapporteur for Freedom of Expression, Standards for a Free, Open and Inclusive Internet (2017), at [178].
34. UN, Our Common Agenda - Report of the Secretary-General, 2021, at 63.
35. UNESCO, Guidelines for Judicial Actors on Privacy and Data Protection, (UNESCO, 2022), at 14.
36. HRC, General Comment No. 16, at [10]..

States parties to the ICCPR are required to give effect to the right to access to information in their domestic laws, including access to personal data.[37] Therefore, lack of specific provisions for access to personal data or for habeas data in Access to Information laws,[38] or inclusion of brief or vague provisions,[39] creates a risk for the violation of the right to access to information. Furthermore, this would also impact the right to privacy if individuals were unable to ascertain whether their personal data is collected, held and used in a legitimate way.

2.3. Misuse of privacy exemptions

As part of an individual's right to privacy, States have an obligation to protect the personal data of individuals from unauthorised disclosure.[40] To this end, countries may adopt the right to privacy as a ground for refusal to grant access to certain documents and information. It is worth noting that the Human Rights Committee has recognised that any restriction on ATI must be included in "laws of parliamentary privilege and laws of contempt of court" and cannot be "enshrined in traditional, religious or other such customary law".[41]

A difficulty that arises at the interface of access to information and privacy, in relation to personal data specifically, is the issue of what has come to be known as the "right to be forgotten". The right to be forgotten refers to the right to have private information about a person be removed from Internet searches. Although not a right recognised explicitly in an international or regional human rights instrument, the European Court of Human Rights has over the years developed and bolstered the right. In a recent decision in 2021, the Court ordered a newspaper to anonymise the identity of a rehabilitated offender, who was involved in a fatal car crash in 1994, in the archived version of the newspaper online. The newspaper argued that doing so would be against the right to freedom of expression (and arguably against the public's right to access to information) but the Court, referring to the right to be forgotten, found the restriction was a proportionate limit for the protection of the former offender's privacy.[42] It is imaginable that the right to be forgotten could be misused to restrict access to private information which may be of public interest. This further highlights the significance of a correct application of the proportionality test when limiting the right to access to information for privacy reasons.

While a legitimate ground for refusal of access,[43] the privacy exemption may also be abused in other contexts to halt access to information which have public interest value. The misuse of privacy exemptions takes many forms including relying on privacy exemptions to avoid releasing information on corruption, abuse of power by public figures or politicians, or human rights or humanitarian law violations as well as invoking data protection laws to undermine investigative journalism, the latter being a concern, for instance, regarding the misuse[44] of the European Union's General Data Protection Regulation (GDPR).[45]

When the privacy exemptions are too broad and have no limiting factors or are not subject to a public interest test, they may be misused. Therefore, any legal restriction of ATI based on privacy must provide sufficient clarity and guidance for information officers or others enforcing the law to "enable them, to ascertain what sorts of expression are properly restricted and what sorts are not".[46]

37. HRC, General Comment No. 34, at [8].
38. See for example Afghanistan Access to Information Law 2014; Bahamas Freedom of Information Act 2017; Bangladesh The Right to Information Act 2009; Law of the Kyrgyz Republic on access to information held by state bodies and local self-government bodies of the Kyrgyz Republic 2007; Liberia Freedom of Information Act 2010; The Law of Mongolia on Information Transparency and Right to Information 2011; Mozambique Right to Information Law 2014.
39. See for example Saint Vincent and the Grenadines Freedom of Information Act 2003, s 30(2).
40. HRC, General Comment No. 16, at [11].
41. HRC, General comment No. 34, at [24].
42. ECtHR, Hurbain v. Belgium (application no. 57292/16), 22 June 2021. See also, Global Toolkit for Judicial Actors, supra note 1, at 160-162.
43. ICCPR, art 19(3)(a) allows restrictions to right to information "for respect of the rights or reputation of others". This is mirrored in European Convention on Human Rights, art 10.
44. See for example Raluca Radu, How The GDPR Can Be Used To Threaten Investigative Journalists, (European Journalism Observatory, 26 November 2018), https://en.ejo.ch/media-politics/press-freedom/how-the-gdpr-can-be-used-to-threaten-investigative-journalists, accessed 2 August 2022.
45. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
46. HRC, General Comment No. 34, at [25].

To address this, some ATI laws have limited the scope of the privacy exemption in various ways, including through imposing a timeframe,[47] differential treatment of personal data of deceased persons[48] or that of public figures where the data relates to their activities in their role,[49] the release of personal information when it has implications for someone's life, health and safety,[50] or through other measures.[51] Finally, it is important to ensure that a privacy (or other) exemption is not utilised **for covering up human rights violations or crimes against humanity**, as acknowledged in some ATI legislation.[52] That the right to privacy cannot be used for limiting ATI when such crimes are in line with the view expressed by the Human Rights Committee that privacy cannot be "a justification for the muzzling of ... human rights".[53] While useful in preventing the likely misuse of privacy exemptions, the correct application of these limits may prove challenging in some instances, for example regarding a determination of whether the health, personal wealth or marital status of a politician or public servant is relevant to their public functions.

In addition to, or in lieu of the above limits on the privacy exemption, a "public interest override" is introduced in some ATI legislation.[54] Where available, the public interest override provisions raise questions

47. For example, Pakistan Freedom of Information Ordinance, s 16(c); Saint Kitts and Nevis Freedom of Information Act 2018, s 26
48. For example, Uganda Access to Information Act 2005, s 26.
49. For example, Ethiopia Freedom of the Mass Media and Access to Information Proclamation No. 590/2008m, art 16; Lithuania Law on the Provision of Information to the Public 1996, s 14(3); Pakistan Right of Access to Information Act 2017, s 16(c); Poland Act on Access to Public Information 2001, art 5(2); Seychelles Access to Information Act 2018, s 21; South Africa Promotion of Access to Information Act 2000, s 34; South Sudan Right of Access to Information Act 2013, s 25(2); Uganda Access to Information Act 2005, s 26.
50. For example, Armenia Law on Freedom of Information 2003, s 8(3); Ireland Freedom of Information Act 2003, s 37(2).
51. For example, under Islamic Republic of Afghanistan Access to Information Law (May 2018 Decree as amended in October 2019), art 15(2) a court can approve the disclosure of personal information.
52. See for example Argentina Law on Access to Information 2016, art 8; Bolivia Supreme Decree No. 28168 of 2005, art 3; Guatemala Ley de Acceso a la Información Publica 2008, art 24; India The Right to Information Act 2005, art 24; Mexico General Act of Transparency and Access to Public Information 2002, art 115; Tajikistan Law of the Republic of Tajikistan on The Right to Access to Information2002, art 5; Tunisia Loi organique n. 22-2016 du 24 Mars 2016 relative au droit d'Access á l'information 2011, art 26; Uruguay Ley Nº 18.381 Derecho de Acceso a la Información Pública 2008, art 12.
53. HRC, General Comment No. 34, at [23].
54. See "Public interest override" ATI legislation examples.

"Public interest override" ATI legislation examples

- Albania Law No. 119/2014 on the Right to Information 1999, art 17(1);
- Antigua and Barbuda The Freedom of Information Act 2004, art 24;
- Argentina Law on Access to Information 2016, art 1;
- Belgium Law N° 94-1724 of 11 April 1994 on the Publicity of the Administration, art 6;
- Bulgaria Access to Public Information Act , s 37;
- Canada Access to Information Act 1983, ss 19 and 26;
- China Open Government Information Regulations of the P.R.C. 2019, art 15;
- Croatia Right of Access to Information Act 2003, art 16;
- Dominican Republic Ley General de Libre Acceso a la Información Pública, No. 200-04 2004, art 18;
- Estonia Public Information Act 2000, s 38;
- Fiji Information Act 2018, art 20(k);
- Germany Freedom of Information Act 2005, s 5;
- Ghana Right to Information Act 2019, ss 17 and 78;
- Hungary Act CXII of 2011On Informational Self-determination and Freedom of Information 1992, s 5;
- India Right to Information Act 2005, art 8;
- Israel Freedom of Information Law 1998, s 10;
- Kenya Access to Information Act 2016, s 6;
- Liberia Freedom of Information Act 2010, s 4.8;
- Lithuania Law on the Provision of Information to the Public 1996, art 14(3);
- Malawi Access to Information Act 2016, art 37;
- Maldives Right to Information Acy 2014, s 23;
- Mexico General Act of Transparency and Access to Public Information 2002, art 120;
- New Zealand Official Information Act 19823, s 9;
- Nigeria Freedom of Information Act 2011, s 15;
- North Macedonia Law on Free Access to Information of Public Character 2006, s 6;
- Poland Act on Access to Public Information 2001, s 5;
- Republic of Korea Act on Disclosure of Information by Public Agencies 1996 , art 9(6);
- Republic of Moldova The Law on Access to Information 2000, art 8(8);
- Rwanda Law No. 04/2013 Relating to Access to Information 2013, art 4(3);
- Serbia Law on Free Access to Information of Public Importance 2003, art 14(2);
- Sierra Leone The Right to Access Information Act 2013, s 21(2);
- Slovenia Access to Public Information Act 2003, s 6(2);
- South Africa Promotion of Access to Information Act 2000, s 46;
- South Sudan Right of Access to Information Act 2013, s 25(2);
- Sri Lanka Right to Information Act 2016, s 5(1);
- Switzerland Freedom of Information Act 2004, art 7(2);
- Tajikistan Law of the Republic of Tajikistan on The Right to Access to Information2002, s 14(1);
- Thailand Official Information Act 1997, s 15;
- Türkiye Turkish Law On The Right To Information 2003, art 21;
- Uganda Access to Information Act 2005, s 34;
- Vietnam Law on Access to Information 2016, s 7.3.

of proportionality, reasonableness, and equity. The complexities of balancing the right to privacy and public interest in personal data are discussed below.

2.4. Balancing public interest, RTI, and privacy interests

On the one hand, public interest can limit access to information by preventing the disclosure of information when doing so would be against the public interest. On the other hand, public interest can override other grounds for refusal of an access to information request, for instance on the basis of protection of privacy. This section focuses on the latter role of public interest in the ATI and privacy debate.

As mentioned in the previous section, many ATI laws contain public interest tests or "override" provisions.[55] Striking a balance between the privacy interests of an individual and the interests of public in access to personal data of that individual is arguably one of the most challenging aspects of the ATI and privacy interface. Where such information is provided in ATI legislation with regards to public interest, this would prove useful: for example, a definition of public interest, when public interest tests and overrides are applicable, or reference to any additional guidelines.

The Human Rights Committee **in *Toktakunov v. Kyrgyzstan*** expressed the view that a limit on ATI on the ground of national security cannot be justified when the information is of public interest and relates to violations of human rights or international humanitarian law.[56] This principle could be said to be relevant and extend to any limits based on privacy. Furthermore, jurisprudence of courts should inform an assessment of public interest. The European Court of Human Rights famously provided some guidance in its *Von Hannover v. Germany* (No. 2) judgment regarding a public interest override of the privacy of public figures.[57]

In the United States of America, the "Hubbard factors" first established in *United States v. Hubbard* are considered as part of a public interest test for disclosure of information.[58]

Disclosure "notices" are also another measure to ensure that a reasonable balance is struck between ATI and right to privacy. An information officer may issue a notice to an individual when granting access to documents containing that individual's personal data to a third party, if, on balance, the public interest in the disclosure of information outweighs the individual's privacy interests. In some cases, this would allow the individual to challenge the decision of the information officer, or at least alert the individual in question of the potential arm following the disclosure of that information. [59] The notice function, however, is not currently adopted in the ATI legislation of all the countries where a public interest override of privacy is provided for.

Section 5 of the German Federal Freedom of Information Act 2005 provides a clear normative basis for a balancing of ATI and privacy by stating that "access to personal data may only be granted where the applicant's interest in obtaining the information outweighs the third party's interests warranting exclusion of access to the information". The ATI legislation in Honduras uses the same balance but in reverse, focusing on whether the potential harm of disclosure is greater than the public interest in accessing the information.[60] While the broad language of the section provides information authorities with a wide discretion in considering and applying a multitude of public interest grounds for overriding the privacy exemption, it may cause difficulties in determining the scope of the override. Further clarification of the public interest override may help alleviate these difficulties. For instance, as discussed above, direct reference to information relating to human rights or humanitarian violations, as included in the laws of several Latin American countries as well as India and Tunisia, would help clarify the scope of a public interest override.[61]

55. See supra note 52 for examples of countries.
56. Human Rights Committee, Communication No. 1470/2006, CCPR/C/101/D/1470/2006; See also Human Rights Council, Report, A/HRC/49/38, supra note 32, at [6].
57. ECtHR, Von Hannover v. Germany (no. 2) [GC] - 40660/08 and 60641/08, Judgment 7.2.2012 [GC].
58. United States v. Hubbard, 650 F.2d 293, 317-22 (D.C. Cir. 1980).
59. See for example Saint Vincent and the Grenadines Freedom of Information Act 2003, s 30(3); Australia Freedom of Information Act 1982, s 41(4)(c); Bosnia and Herzegovina Law on Freedom of Access to Information for Bosnia and Herzegovina 2000, art 9(3).
60. Honduras Ley de Transparencia y Acceso a la Información Pública 2006, art 17.
61. See supra note 50.

Under international human rights law a three-part test for limits on the right to access to information and the public interest provides a framework for the application of the public interest test:

1 **Identifying the applicable privacy ground/exemption**	This should be provided for by law, pursue a legitimate aim, and be necessary for a legitimate purpose.
2 **Identifying any public interest override provisions in the applicable law**	This could act as the starting point for an assessment of the relative weight of the competing interests.
3 **Assessing the weight of the third party or public interest in accessing the information**	This involves an assessment of whether the third party or public interest in disclosure outweighs the individual's privacy interest in withholding of the information or their personal data.
4 **Assessing the potential harm to the individual as a result of the disclosure**	This can be done before or after step 3, depending on the wording of the legislation.
5 **Considering any mitigating actions permissible under the law**	This may include subjecting the release to deletions, viewing, copying or distribution conditions, specific forms of release, or release after a "disclosure notice" is issued to the individual whose information is being released.
6 **Making an informed and balanced decision**	The decision should be communicated to the party requesting the information in a timely and clear manner.

2.5. Digital and online technologies

While the Internet and new technologies have facilitated access to information online, the large scale and digital collection, storage, processing and sale or transfer of personal data pose privacy risks and new challenges for information authorities managing and using such datasets and assessing their authorised disclosure as part of their obligations to respect, protect and fulfil the RTI. As Cannataci and others noted in 2018, "[t]he conflicts between privacy and freedom of expression are intensified by the combination of the virtual and physical spheres."[62]

During the ongoing COVID-19 pandemic, concerns have been raised in many countries regarding the risk to privacy of individuals whose personal health, movement, and vaccination data was collected as part of scanning and tracing practices to halt the spread of the virus,[63] reflecting concerns voiced previously regarding the "death of privacy" in the 21st century as a result of technological and online developments.[64] The 2020 UNESCO Guidelines on the role of judicial operators in the protection and promotion of the right to freedom of expression during the COVID-19 pandemic emphasise the importance of the provision of accurate information to the media and the public in general, and the need to ensure that any restrictions on ATI are compliant with the above-mentioned three-part test.[65]

The main difficulties relate to ensuring that personal data that may be accessed under ATI guarantees is only collected for the intended purpose, is properly anonymised, is not held for longer than legal, and is

62. UNESCO, Joseph A Cannataci and others, "Privacy, free expression and transparency: Redefining their new boundaries in the digital age" (December 2016, UENSCO Publishing), at 2.4.

63. B Sowmiya et al "A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19" (2021) 2(136) SN Computer Science; Eugene Y Chan and Najam U Saqib "Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high" 119 (2021) Computers in Human Behaviour.

64. See for a discussion of this point Cannataci, supra note 62, at 2.1.

65. UNESCO, COVID-19: The role of judicial operators in the protection and promotion of the right to freedom of expression: Guidelines, (UNESCO, 2020) at 7.

protected from unauthorised access and security leaks and breaches (through the use of malware, spyware, or other hacking methods).

In many instances, where information and data are collected by information authorities online, users may be asked to cede a degree of privacy by way of accepting cookies which collect data about them and their activity in exchange for access to proactively released information. This may relate, for example, to the online submission of an access to information request which is common in some countries, even if the requested information is then provided in another manner. In these cases, duty bearer institutions need to indicate to users how personal privacy will be protected in regard to disclosure practices, for example, by proven anonymisation techniques.

Another emerging trend is the increasing role of private entities in gatekeeping personal information by way of collecting and storing personal data of individuals. This has implications for both the right to access to information and the right to privacy. With regards to the former, the right to access to information is traditionally viewed as relating to information held by public authorities which is the view many ATI laws adopt. This view, however, no longer reflects the reality of how private companies collect and store personal information. Therefore, access to information legislation should address the role of private entities as information authorities generally, and in relation to private data more specifically.

Similarly, to ensure the protection of personal data collected, held and used by private companies, a new legislative approach in adopting or amending privacy legislation is needed to ensure respect for and protection of the right to privacy. This is particularly significant considering the collection of data by social media platforms and apps that collect data (e.g. weather apps concerning geo-location, menstruation apps recording intimate personal information, etc) where users provide identification information or data knowingly or not,[66] and the increasing use of artificial intelligence (AI) in the collection and use of personal data.[67] UNESCO has previously called for greater transparency in this field.[68]

This change in approach is already under way in countries where the ATI legislation refers to private bodies holding personal data and in those where the national law mirrors the provisions in the GDPR which replaced the EU Data Protection Directive of 1995.[69] In addition to State entities, the provisions on access to information in the Model Inter-American Law on Access to Public Information apply to "private organizations which operate with substantial public funds or benefits (directly or indirectly) or which perform public functions and services insofar as it applies to those funds or to the public services or functions they undertake".[70] Similarly, the Model Law on Access to Information for Africa (discussed further below) also applies to private bodies and the information they hold which "may assist in the exercise of protection of any right".[71] The significance of all this is that going forward ATI legislation may need to grapple with this issue of privately-held data and information which has a bearing on the public interest.

66. Human Rights Council, "Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" UN Doc A/HRC/47/25 (13 April 2021) at [66].
67. See for a discussion of the relevance of AI to ATI and privacy, Article 19 and Privacy International, "Privacy and freedom of expression in an age of artificial intelligence" (London, 2018); Human Rights council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" UN Doc A/73/348 (29 August 2018).
68. UNESCO, Letting the Sun Shine In: Transparency and Accountability in the Digital Age (UNESCO, 2021).
69. European Parliament, Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (adopted on 24 October 1995, entered into force 13 December 1995).
70. Model Inter-American Law on Access to Public Information, AG/RES. 2607 (XL-O/10), (Adopted at the fourth plenary session, held on June 8, 2010), art 3
71. African Commission on Human and Peoples' Rights, Model Law on Access to Information for Africa, s 2(b).

3. Mapping the legal landscape

3.1. ATI and privacy legislation

As of August 2021, 132 UN Member States have adopted access to information legal guarantees.[72] Additionally, as of May 2022, 141 UN Member States were identified to have adopted privacy legislation which means that 107 countries - slightly over half of the UN Member States - have legislative frameworks covering both the right to information and the right to privacy.

Among the States with ATI legislation, almost all (130 States) appear to have included direct or indirect exemptions for the protection of privacy in their laws.[73] While there are some similarities between these provisions, the scope of the exemptions, the language used, and the limitations placed upon them are greatly varied. This shows the lack of a universal and coherent approach to balancing ATI and the protection of the privacy interests of individuals in their private information and personal data.

3.2. Soft law approaches to ATI and privacy

A number of soft law initiatives address the interface of ATI and privacy. An early example of this is the 1990 UN Guidelines for the Regulation of Computerized Personal Data Files which, among other things, address the interface of access to information and privacy in its principle 4 on access to one's own personal data, and principle 6 on exceptions to privacy for public interest reasons.[74]

The Declaration of Principles on Freedom of Expression in Africa adopted in 2002 "sets out core elements of the right of access to information."[75] Later on in 2010, the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and People's Rights (correct?) created the Model Law on Access to Information for Africa, with access to information laws being adopted consequently in 10 African countries.[76] The 'boom' in adoption of ATI legislation in Africa is partly attributed to the adoption of the Model Law, which highlights the importance of soft law measures to the creation of legal frameworks.[77]

While the African Model Law does not explicitly mention privacy, it allows the refusal of an access to information request if it "would involve the unreasonable disclosure of personal information".[78] This privacy exemption, however, is not adopted by all African countries with ATI legislation. The same is true about the need to inform a third party whose personal information is being considered for disclosure, which is another criteria under the Model Law.[79] Additionally, while the Model Law states that a public interest in disclosure of information that outweighs the potential harm caused will override a privacy exemption, some African countries have chosen not to adopt the override,[80] while others have it as a discretionary, rather than absolute, measure.[81]

72. UNESCO, "To Recovery and Beyond: 2021 UNESCO Report on Public Access to Information (SDG 16.10.2)", (UNESCO, 2022) at [7].
73. Afghanistan, Albania, Angola, Antigua and Barbuda, Argentina, Armenia, Australia, Azerbaijan, Bangladesh, Belarus, Belgium, Belize, Benin, Bosnia and Herzegovina, Brazil, Bulgaria, Burkina Faso, Canada, Chile, China, Côte D'Ivoire, Croatia, Czech republic, Denmark, Dominican Republic, El Salvador, Estonia, Ethiopia, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Guatemala, Guyana, Honduras, Hungary, Iceland, India, Indonesia, Iran, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Latvia, Lebanon, Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Malawi, Maldives, Malta, Mexico, Monaco, Mongolia, Montenegro, Morocco, Mozambique, Nepal, The Netherlands, New Zealand, Nicaragua, Niger, Nigeria, North Macedonia, Norway, Pakistan, Palau, Panama, Peru, Philippines, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Russia, Rwanda, Saint Kitts and Nevis, Saint Vincent and the Grenadines, San Marino, Saudi Arabia, Serbia, Seychelles, Sierra Leone, Slovakia, Slovenia, South Africa, South Sudan, Spain, Sri Lanka, Sudan, Sweden, Switzerland, Tajikistan, Thailand, Timor Leste, Togo, Trinidad and Tobago, Tunisia, Turkey, Uganda, Ukraine, The United Kingdom, The United States, Uruguay, Vanuatu, Vietnam, Yemen, Zimbabwe.
74. UN Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990.
75. Ololade Shyllon (ed) The Model Law on Access to Information for Africa and other regional instruments: Soft law and human rights in Africa (Pretoria university Law Press, 2018), at vi.
76. Burkina Faso, Côte d'Ivoire, Kenya, Malawi, Mozambique, Rwanda, Sierra Leone, South Sudan, Sudan and Tanzania.
77. Fola Adeleke "The Impact of the Model Law on Access to Information for Africa" in Shyllon, supra note 75, at 21.
78. Model Law on Access to Information for Africa 2010, s 27(1).
79. Model Law, s 39.
80. See for example Mozambique Law no. 34 /2014 of 31 December.
81. See for example Kenya's Access to Information Act, s 6(4).

The 2010 Organisation of American States' Model Inter-American Law on Access to Public Information and its Implementation Guidelines was another example of a soft law initiative on addressing the interface of ATI and privacy in a regional legal framework. As discussed above, the Organization of American States' General Assembly adopted a new Model Law in 2020 which will help update the ATI and privacy laws of its member states.

The Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted tin 2013 or help harmonise national privacy legislation to "prevent interruptions in international flows" of personal data.[82]

While the EU GDPR mentioned earlier is binding law in all EU member states, it has also been used as a model law in a number of non-EU countries[83] and its principles on personal data can inform law reform in other countries. At the same time, many countries do not have similar privacy protections, which may result in additional complications where for example an app headquartered in one country garners data from users of the app in another jurisdiction.

3.3. Judicial approaches to ATI and privacy

Rulings from courts in various jurisdictions demonstrate the clashes of the right to access to information and the right to privacy. The courts' reasoning and decisions can help inform policy and law making as well as the conduct of information and privacy authorities. Similar to balancing other human rights, international courts have adopted the principle of proportionality when balancing the right to information and privacy. In cases involving the balancing of the right to privacy against other rights, the European Court of Human Rights relies on the three-part test in article 8 of the European Court of Human Rights. The three-part test, already presented, used by the European Court of Human Rights is based on the concepts of lawfulness, legitimacy, and necessity in a democratic society.[84]

In ***Claude Reyes et al. v. Chile***, the Inter-American Court of Human Rights (IACtHR) emphasised the need for an information authority to clearly communicate and justify any withholding of documents that contain information of public interest, to avoid a violation of the RTI.[85] While the case did not involve a privacy exemption, the same dicta regarding clear communication of refusal or redaction grounds can arguably apply to cases of application of privacy exemptions.

The case of ***Gomes Lund v. Brazil*** showcases the intersection of access to personal and family data and ATI in a context where the rights complement each other. In this case, the IACtHR affirmed its previous rulings that the public has a right to know the truth about human rights violations, even if information about such events is exempted from disclosure under secrecy laws. The Court also, for the first time, recognised that the right of relatives of victims of human rights violations to know the truth, is part of the right to seek and receive information.[86] This ruling and its ratio can provide persuasive authority for other courts and tribunals where the application of a privacy exemption, regarding ordinary individuals or public figures, can be ignored in cases of human rights violations.

The case of ***Saket v. Union of India*** brought to light a unique aspect of the interface of ATI and privacy by addressing the privacy rights of individuals making ATI applications for access to information. In 2020, the High Court of Bombay in this case held that the online publication of the personal information of an applicant that had submitted multiple access to information requests was a breach of his right to privacy, as well as a disregard for the purpose of India's Right to Information Act 2005.[87]

82. OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 Preface.
83. For example, Argentina, Brazil, Chile, Japan, Kenya, Mauritius, Republic of Korea, South Africa and Turkey.
84. See for more on this points and decisions of the ECtHR, Guidelines for Judicial Actors on Privacy and Data Protection, supra note 1, at 7.
85. Order of the Inter-American Court of Human Rights, Case of Claude-Reyes et al. v. Chile, Judgment of September 19, 2006.
86. Inter-American Court of Human Rights Case of Gomes Lund Et Al. ("Guerrilha Do Araguaia") V. Brazil, Judgment of November 24, 2010.
87. Bombay High Court, Saket S Gokhale vs The Union of India on 5 November, 2020.

A recent ECtHR decision shows that a failure to strike the right balance between ATI and privacy may lead to a violation of human rights. In its 2020 ruling in *Centre for Democracy and the Rule of Law v. Ukraine*, the Court decided that the education and work history of a number of top Ukrainian politicians included in their official CVs were personal information of public interest and the Government's failure to disclose that information to an NGO constituted a breach of RTI.

4. Information and privacy authorities

In some countries an institution may have a dual mandate which relates to both ATI and privacy rights,[88] while in others there are two separate commissions or authorities in relation to each right.[89] Others yet have designated an existing entity, such as their Human Rights Commission, as the oversight body for RTI.[90]

The ATI law in Australia, like in some other countries,[91] requires the Information Commissioner to publish guidelines for various issues covered in the Freedom of Information (FOI) Act,[92] for example with regards to public interest factors. Information providers or the Minister must in turn "have regard" to any such guidelines.[93] The Australian Information and Privacy Commissioner has issued guidelines on both FOI[94] and privacy.[95] The FOI guidelines, for instance, explain that the fact that the privacy exemption in the FOI Act in Australia is subject to a public interest test signifies that the exemption is "weighted in favour of disclosure".[96] This would arguably be of value to an information officer assessing an application for disclosure of documents containing personal data and potentially leading to an invasion of privacy.

In New Zealand, with an ATI legislation similar to that of Australia's, the Privacy Commissioner has issued guidelines on the right to privacy in the form of "Privacy Codes of Practice"[97] and "Privacy Principles" with the latter mainly relating to collection and use of personal information.[98] Principle 6 states that individuals have a right to ask for access to their own personal information and Principle 11 limits the disclosure of personal information to specific cases, including if doing so is "necessary to uphold or enforce the law". The wording in Principle 11 is in line with a public interest override of a privacy exemption. The Commission also launched the "Privacy is precious" campaign to raise awareness about the changes to the rules about protection of and access to personal data introduced in the new Privacy Act 2020.[99]

Part of UN States' obligations under article 19 of the ICCPR, and in the context of proactive disclosure specifically, is to make available any information that is necessary for the exercise of human rights.[100] Therefore, information and privacy authorities can help States fulfil this obligation by leading the development and distribution of information that is essential to the exercise of both ATI and privacy rights of individuals.

88. For example, the New Zealand Privacy Commissioner (working together with the Ombudsman) is the oversight authority for both rights.
89. For example, in Chile, the Transparency Council (Del Consejo para la Transparencia) was established under s 31 of the Transparency of public office and access to the information of the State Administration law 2008 with regards to RTI; and the Data Privacy Authority was established under the Bill No. 11144-07 which amends Laws 19.628 and regulates the processing and protection of personal data.
90. Malawi Access to Information Act 2016, s 7.
91. See for example Bahamas Freedom of Information Act 2017.
92. Freedom of Information Act 1982, s 93A(1).
93. S 11B(5).
94. FOI Guidelines, Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982.
95. Australian Privacy Principles Guidelines, Privacy Act 1988, https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf, accessed 2 August 2022.
96. FOI Guidelines, at [1.14].
97. Under the Privacy Act 2020, the codes of practice become part of law in New Zealand. The Commissioner has currently issued 6 codes of practice relating to issues such as credit reporting privacy and health information privacy. https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/.
98. https://www.privacy.org.nz/privacy-act-2020/privacy-principles/.
99. https://www.privacy.org.nz/privacy-act-2020/campaign/.
100. Annual Report of The Inter-American Commission on Human Rights, Report of the Office of the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II.134 (25 February 2009), at [147] and [161].

Conclusion and recommendations

This brief overview of the current intersection of the right to access to information and right to privacy highlights a number of both long existing and emerging challenges. The main themes at the intersection of the two rights relate to the protection of and access to personal data, privacy exemptions to RTI, and the balancing of public interest against privacy interests of individuals in their personal data. Based on the above observations, the below recommendations are made:

1. States should provide a definition of key concepts such as privacy, personal data, personal information, information authority, etc., in their existing ATI and/or privacy legislation to help guide implementation. These definitions must be in line with international human rights standards on ATI and the right to privacy. This should also be done with due consideration given to the interface of the right to information and privacy as they mutually shape one another. In countries without ATI and/or privacy legislation, the significance of definitions in light of the interconnectedness of the two rights should be paramount when adopting laws and policies.

2. States should provide for specific habeas data provisions in their ATI and/or privacy legislation that allow individuals to find out if and what personal information about them is held by public and private entities. This should also include the individual's ability to request that incorrect or incomplete information is rectified, or that certain data is removed from the entity's databases if the purpose for the initial collection and/or holding of the data no longer applies. This would ensure that any such legislative provisions adhere to the principles of transparency, quality, accuracy, and access in relation to personal data protection.

3. States should include a comprehensive and sufficiently precise and accessible framework for balancing the restriction of ATI on the basis of protection of privacy interests and the role of the public interest in that balance in regard to ATI and/or privacy legislation. This should take account of existing international human rights standards, particularly the three-part test related to two both rights and the principle of proportionality. Such a framework must include multiple components:

    a. Provision of a privacy exemption that limits the right to access to information when disclosure of information would breach an individual's right to privacy;
    b. Provision of a "public interest override" of the privacy exemption generally which is subject to a proportionality test that weighs up harms to the two rights and enables the least intrusive option;
    c. Provision of a specific limit on the privacy exemption in relation to information about public authorities or figures which relates to their public functions and is of public importance; and,
    d. Provision of a specific limit on the privacy exemption in relation to information about violations of human rights, crimes against humanity, war crimes, genocide, environmental and climate change related offenses, and similar matters.

4. In cases of a decision to disclose otherwise exempted private information and personal data on the ground of public interest or by a ruling of a court or similar authority, States should require the relevant information authority, for example the information and/or privacy commissioner, to attempt to notify the individual whose non-anonymised personal data is subject to disclosure and give that person the opportunity to challenge the disclosure.

5. As part of a well-balanced normative framework on ATI and the right to privacy, States should provide for independent oversight, review, appeal, and remedy mechanisms in relation to both rights, either separately or jointly. As the ATI and data protection increasingly overlap, any such framework should take into account the need for an interconnected and inclusive protection of both rights. This means that appeal and oversight mechanisms should actively consider and balance the interface of ATI and personal data protection.

6. In addition to the adoption of a national legislative framework, States should ensure that the norms balancing the two rights are properly enforced. Effective enforcement would require the dedication of sufficient resources and provision of appropriate training for administrative and judicial authorities to ensure that they strike the right balance when manoeuvring the overlap of ATI and right to privacy.

7. States should make relevant information publicly available about access to public information generally, access to personal data specifically, and the available legal and other measures for the protection of individuals' privacy. This will let the public know what information and data are available, including elements that may ultimately be drawn from users themselves.

8. States could consider reviewing ATI laws, as balanced with the right to privacy, in relation to their applicability to personal and other data that is collected and used by private actors.

9. In applying the relevant laws, information and privacy commissioners and judicial actors must ensure that any restrictions on ATI and freedom of the press due to privacy concerns are proportionate and necessary. This is because they play a fundamental role in ensuring that privacy exemptions are not abused and that the right balance is struck between the protection of privacy and the public interest.