A DANGEROUS SYMBIOSIS: GAPS IN INFORMATION TRANSPARENCY AND SECURITY AMONG HUMAN RIGHTS MECHANISMS

LISA REINSBERG*

ABSTRACT

What obligations do supranational human rights bodies have as guardians of sensitive and vital information and administration of international justice? To keep individuals' private data secure? To proactively publish the decisions that result from their petitions? Advocates, in particular, face significant risks when their communications are intercepted, and their work is frustrated when they cannot obtain necessary information. Cognizant of such concerns, human rights bodies are increasingly requiring States to ensure individuals' rights to data privacy, access to information, and use of encrypted communication channels.

Yet, human rights bodies themselves lack formal policies and consistent practices with regard to receiving, processing, and sharing information. At times, their information management methods imperil advocates and impede access to justice. Advocates and human rights bodies depend on one another for information and impact, but inattention to these risks may perpetuate a dangerous symbiosis.

This article provides a first, comprehensive overview of United Nations and regional human rights bodies' public-facing information management practices.

DOI: https://doi.org/10.15779/Z38CF9J77N

* Executive Director, International Justice Resource Center; Visiting Fellow, Centre for Fundamental Rights at the Hertie School. I am deeply grateful to Eric Stover for his time, guidance, contributions, and good humor while advising me on this project. I thank the participants in the American Society of International Law (ASIL) 2021 Research Forum and the Berkeley Law Human Rights and Social Justice Writing Workshop for their comments and discussion. And, thank you to Carolyn Patty Blum, David Kaye, Alexa Koenig, Paul Schwartz, and Friedhelm Weinberg for helpful suggestions at various stages. Human rights defenders and staff members of human rights mechanisms have my sincere appreciation, including for the information and insights they have shared on this topic. Finally, an enormous thank you to the BJIL team for their thoughtful and valuable edits. Of course, this article reflects my views alone and all errors are my own.

It identifies the gaps between those practices and international human rights norms, and offers recommendations for future policy development.

I. ERIKA'S DILEMMA: INFORMATION FLOWS BETWEEN THE HUMAN RIGHTS ADVOCATES AND ACCOUNTABILITY MECHANISMS

Erika stares past the open door to the dust still floating down onto fresh tire tracks in the sandy earth of the Honduran coast. A few feet out, the tracks fade, along with any clues as to where her colleague Daniel might be. The armed men who dragged him away wore balaclavas.[1] She fears his name will join the ever-growing list of fellow activists killed for opposing land grabs and development projects in the deadliest country in the world for environmental defenders.[2] Erika looks at her mobile phone. If she calls local law enforcement, she could put Daniel in greater danger. Someone could be listening and the authorities may already be complicit. She has heard the Inter-American Commission on Human Rights (IACHR)—all the way in Washington, D.C.—could intervene, but how can she request its help?

Though she is fearful that the government or private actors could be monitoring her online activity, Erika turns to the internet for answers. Her search leads to the IACHR webpage on "precautionary measures."[3] Erika reads that the IACHR can grant precautionary measures "in serious and urgent situations" involving a "risk of irreparable harm to persons."[4] Would Daniel's situation meet these criteria?

It is difficult to tell. The list of previously-granted measures[5] is organized by year and there is no full-text search function, subject matter filter, or country filter. The webpage on human rights defenders[6] lists precautionary measures

---

[1] This account is fictional, but the scenario is familiar for many human rights advocates. *See, e.g.*, Comunidades Garífunas de Triunfo de la Cruz y Punta Piedra v. Honduras, Provisional Measures, Order of the Court, Inter-Am. Ct. H.R. (ser. E) No. 4, ¶ 8 (Sept. 2, 2020), https://www.corteidh.or.cr/docs/medidas/garifuna_se_04.pdf.

[2] GLOBAL WITNESS, HONDURAS: THE DEADLIEST PLACE TO DEFEND THE PLANET (2017) https://www.globalwitness.org/documents/18798/Defenders_Honduras_full_report_single_v5_AH12dtf.pdf.

[3] *About Precautionary Measures*, INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/jsForm/?File=/en/iachr/decisions/about-precautionary.asp (last visited Sept. 4, 2022).

[4] *See id.*

[5] *Inter-American Commission on Human Rights, Precautionary Measures, Grants and Extensions*, INTERNET ARCHIVE, https://web.archive.org/web/20210113035203/http://www.oas.org/en/iachr/decisions/precautionary.asp (Jan. 13, 2021). In a welcome development, in approximately March 2021, the IACHR published a new version of this webpage that does have a search function and country filter. *See Inter-American Commission on Human Rights, Precautionary Measures*, INTER-AM. COMM'N H.R., https://www.oas.org/en/IACHR/decisions/MC/precautionary.asp (last visited Sept. 4, 2022).

[6] *Inter-American Commission on Human Rights, Rapporteurship on Human Rights Defenders and Justice Operators*, INTERNET ARCHIVE, https://web.archive.org/web/20210418221256/https://www.oas.org/en/iachr/defenders/protection/pre

granted to protect advocates, but the most recent are from 2013 and the files are not text-searchable.[7] Reading through each document would take time that Erika does not have. Next, she conducts an internet search for precautionary measures involving her community, the Garifuna people. She finds a link to an IACHR hearing. To her disappointment, the audio and video files are all missing.[8]

Erika hopes someone at the IACHR can give her guidance, but she does not see any way to contact the IACHR via an end-to-end encrypted channel,[9] such as Signal, which would help keep her identity and message confidential.[10] There are no forms or instructions for making information requests on the IACHR website. She finds the portal[11] for requesting precautionary measures, but the website terms refer to the IACHR's "privileges and immunities" while disavowing responsibility for the security of any personal information—including names and addresses—that Erika provides.[12] How can she help secure Daniel's safety while protecting her own?

Erika's conundrum reflects a broader question: how should human rights mechanisms handle the incoming and outgoing information that is their lifeblood? For the people of the Americas, the IACHR represents a chance for justice and accountability; its work promoting and protecting human rights is invaluable and effective. However, for victims and advocates, interacting with the IACHR can be costly and challenging. Individuals often expend significant time and effort to obtain necessary information and may face retaliation from governmental or private actors. If the IACHR does not transparently, consistently, and securely

---

cautionary.asp (Apr. 18, 2021). In another welcome development, the IACHR published a new version of this webpage in April 2021 that includes a text search function, as well as more recent precautionary measures resolutions that are available in searchable PDF format. *See Rapporteurship on Human Rights Defenders, Precautionary Measures*, INTER-AM. COMM'N H.R., https://www.oas.org/en/IACHR/jsForm/?File=/en/IACHR/r/dddh/MC.asp (last visited Sept. 4, 2022).

[7] *See, e.g.*, Iván Hernández Carrillo v. Cuba, Precautionary Measure 245-13, INTER-AM. COMM'N H.R. (Oct. 28, 2013), http://www.oas.org/es/cidh/decisiones/pdf/MC245-13-esp.pdf.

[8] *Audiencias, 124 Período de Sesiones*, INTER-AM. COMM'N H.R., https://www.oas.org/es/cidh/audiencias/Hearings.aspx?Lang=es&Session=19&page=2 (last visited Sept. 4, 2022) (none of the audio, video, or image files are available for any of the hearings on this page).

[9] End-to-end encryption generally requires both the sender and receiver to use personalized keys in order to access a message. *See, e.g.*, *A Deep Dive on End-to-End Encryption: How do Public Key Encryption Systems Work?*, ELECTRONIC FRONTIER FOUNDATION, https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work (last visited Mar. 22, 2022).

[10] *Contact the IACHR*, INTER-AM. COMM'N H.R., https://www.oas.org/en/iachr/about/contactus.asp (last visited Sept. 4, 2022).

[11] *IACHR Individual Petition System Portal*, OAS, https://www.oas.org/ipsp/default.aspx?lang=en (last visited Sept. 4, 2022).

[12] *IACHR Web Site Terms*, INTER-AM. COMM'N H.R., https://www.cidh.oas.org/disclaimer.htm (last visited Sept. 4, 2022). *See also Terms & Conditions*, OAS, https://www.oas.org/en/terms_conditions.asp (last visited Sept. 4, 2022).

manage the information it disseminates and receives online, it risks imperiling individuals' safety and privacy, as well as losing the trust—and input—of the advocates who are essential to its relevance and impact.

The Inter-American Commission is not alone in its inattention to information management. The United Nations and regional intergovernmental organizations, including the African Union, Council of Europe, and Organization of American States, have established dozens of specialized courts, commissions, committees, and other independent expert bodies to monitor human rights conditions in nearly every country of the world. Yet, despite increased communication between these human rights mechanisms[13] and advocates, particularly via the internet, none has shared an information management policy, let alone one adapted to the digital era. This gap has already had profound consequences, exposing advocates to excessive obstacles and risks.

At the same time, human rights mechanisms are defining and enforcing States' obligations under international law to, *inter alia*, ensure access to public information and to justice, promote the work and security of human rights advocates, and protect individuals' privacy and correspondence. These standards arguably bind human rights mechanisms themselves as well, and, at minimum, should guide the development of necessary information management policies.

While the term "information management" covers many topics, including internal case management software and overall cybersecurity, I focus here on three issues of particular concern for human rights advocates: security of communications, protection of personal data processed by human rights mechanisms, and public access to documents and other information human rights mechanisms produce. In Part II, I argue that information management policies are necessary due to the expansion and evolution of human rights oversight in the digital era, and introduce the regional and universal mechanisms covered in this article. Part III focuses on whether intergovernmental organizations, or the human rights mechanisms they have created, have international human rights obligations, and therefore, may have a legal duty to adopt certain information management policies. In Parts IV, V, and VI, I address encryption, data protection, and access to information, respectively, reviewing the human rights mechanisms' corresponding policies and practices. In each of these parts, I also identify relevant human rights treaty provisions and soft law that shape States' obligations in these areas. With regard to individual rights related to data protection and access to

[13] I use the term "human rights mechanisms" to refer to the independent human rights oversight bodies created by the United Nations and regional intergovernmental organizations, which are the focus of this article. *See infra* Part I.A for an overview of these mechanisms. I use the term "advocates" to refer to lawyers and non-lawyers who engage in documentation, reporting, litigation, and advocacy to protect or vindicate human rights, whether in a professional or voluntary capacity.

information, I suggest these norms may have reached customary status. Finally, VII concludes with recommendations for human rights mechanisms' consideration.

II. HUMAN RIGHTS OVERSIGHT IN THE DIGITAL AGE

Twenty-five years ago, human rights protection was a paper world. Human rights mechanisms published their decisions and reports in thick volumes; their corridors were lined with cabinets overstuffed with letters, domestic court records, and photographs. Evidence of the abuses they investigated was hidden, not infrequently, in stacked cardboard boxes.[14] Then, at the very end of the twentieth century, human rights mechanisms began to move online. Their new websites included online complaint forms and became the primary method of disseminating their growing body of caselaw.[15] These developments facilitated the receipt and dissemination of critical information while also deepening dependence on the internet in the field of human rights. And then, time largely stood still. Since those early days of the digital era, human rights secretariats—from Geneva to Banjul—have mostly used the same channels to impart, receive,

[14] *See, e.g.*, Janowiec and Others v. Russia [GC], App. Nos. 55508/07 and 29520/99, 2013-V Eur. Ct. H.R. 203, ¶ 38 (in 1990, the president of the USSR handed documents to the Polish president from a secret archive concerning responsibility for the 1940 Katyn massacre); Ginger Thompson, *Mildewed Police Files May Hold Clues to Atrocities in Guatemala*, N.Y. TIMES (Nov. 21, 2005), https://www.nytimes.com/2005/11/21/world/americas/mildewed-police-files-may-hold-clues-to-atrocities-in.html; Giles Tremlett, *Operation Condor: the Cold War Conspiracy that Terrorised South Americ*a, GUARDIAN, Sept. 3, 2020, https://www.theguardian.com/news/2020/sep/03/operation-condor-the-illegal-state-network-that-terrorised-south-america (relating the 1992 discovery of General Alfredo Stroessner's secret police archive containing "half a million sheets of paper").

[15] Many human rights mechanisms appear to have first created websites between 1997 and 2002. *See, e.g.*, *Office of the High Commissioner for Human Rights*, INTERNET ARCHIVE, https://web.archive.org/web/19970421200705/http://www.unhchr.ch/ (Apr. 21, 1997); *European Court of Human Rights*, INTERNET ARCHIVE, https://web.archive.org/web/19981211234741/http://194.250.50.200/ (Dec. 11, 1998); Afr. Comm'n Hum. & Peoples' Rts., *Fifteenth Annual Activity Report of the African Commission on Human and Peoples' Rights: 2001-2002*, 22 (2002), https://www.achpr.org/public/Document/file/English/achpr30and31_actrep15_20012002_eng.pdf. *See also African Commission on Human & Peoples' Rights*, INTERNET ARCHIVE, https://web.archive.org/web/20020223204742/http://www.achpr.org/html/africancommissiononhuman.html (Feb. 22, 2002).

and manage online communications.[16] Like their practices, their policies have evolved very little, very slowly.[17]

Meanwhile, the broader digital landscape has transformed. Over the past 15 years, the number of people using the internet has quadrupled to more than 4 billion.[18] Human rights advocates now rely on digital technologies, which have expanded and reshaped their methods and reach.[19] States and private actors have also gained technological capabilities, enabling targeted and mass collection of data and communications, for example.[20] Unlawful or arbitrary surveillance of communications "continues without evident constraint" in a climate of secrecy and weak regulation.[21]

Against this backdrop, human rights advocates and the general public are interacting with human rights mechanisms much more than in prior decades. For example, in 2000, the IACHR received 658 individual complaints of human rights violations; that number soared to 3,034 in 2019.[22] The United Nations Special Procedure mandate holders (independent experts appointed to monitor and promote human rights with respect to particular themes or countries) carried out eighty-four country visits in 2019, compared to forty-eight in 2006.[23] At the same

---

[16] For example, the first iteration of the Inter-American Commission on Human Rights' website, apparently published in January 1999, included an online form for submitting petitions (complaints). *See Inter-American Commission on Human Rights: Complaint Form*, INTERNET ARCHIVE, https://web.archive.org/web/19990428003528/http://www.cidh.oas.org/email.htm (Apr. 28, 1999). The original European Court of Human Rights' website included its HUDOC case law database. *See HUDOC INTERnet*, INTERNET ARCHIVE, https://web.archive.org/web/19990202141539/http://194.250.50.200/hudoc/default.htm (Feb. 2, 1999). The early OHCHR website also allowed visitors to search its document databases. *See Office of the High Commissioner for Human Rights*, INTERNET ARCHIVE, https://web.archive.org/web/19970804040956/http://www.unhchr.ch/search.htm (Aug. 4, 1997).

[17] *See* discussion, *infra* Parts I.B (overview), 0 (data protection), and 0 (access to information).

[18] *See* ITU, *Measuring digital developments: Facts and figures 2019*, 1 (2019), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

[19] *See generally* Mallika Dutt & Nadia Rasul, *Raising Digital Consciousness: An Analysis of the Opportunities and Risks Facing Human Rights Activists in a Digital Age*, 20 SUR 427-35 (2014); *Digital Security and Privacy for Human Rights Defenders*, FRONT LINE, https://equalit.ie/esecman/index.html (last visited Sept. 4, 2022); *see also* DIGITAL WITNESS (Sam Dubberley, Alexa Koenig & Daragh Murray eds., 2020); NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE (Molly K. Land & Jay D. Aronson eds., 2018).

[20] *See, e.g.*, Likhita Banerji, *A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work*, AMNESTY INT'L (Aug. 16, 2019), https://www.amnesty.org/en/latest/research/2019/08/a-dangerous-alliance-governments-collaborate-with-surveillance-companies-to-shrink-the-space-for-human-rights-work/ (last visited Sept. 4, 2022).

[21] *See* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Surveillance and Human Rights*, U.N. Doc. A/HRC/41/35 (May 28, 2019), https://www.undocs.org/A/HRC/41/35.

[22] *Statistics by Year, Petitions Received*, INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/multimedia/statistics/statistics.html (last visited Sept. 4, 2022).

[23] *See* U.N. Hum. Rts. Council, *Facts and figures with regard to the special procedures in 2019* 16 (Mar. 10, 2020), https://undocs.org/en/A/HRC/43/64/Add.1; Off. High Comm'r Hum. Rts., *United Nations Special Procedures: Facts and Figures 2006*, 3, https://www.ohchr.org/sites/default/files/Documents/HRBodies/SP/factsfigures2006.pdf. Prior to the

time, States are ratifying more treaties and complaint procedures,[24] while creating new regional and universal oversight bodies, making human rights protections available—at least in theory—to many more people and in many more situations.[25]

Unfortunately, the world is also witnessing a growth in reprisals against human rights advocates. Indeed, States have retaliated against advocates *because of* their purportedly private digital communications with human rights mechanisms.[26] In many countries, this phenomenon has dovetailed with the suppression of domestic civic space. In summarizing the situation in Mexico, for example, the IACHR described "high levels of disappearances and attacks on the lives of human rights defenders and journalists, harassment, threats, surveillance, [and] communication interception, as well as . . . legislation that directly or indirectly criminalizes social protest and the work of human rights defenders."[27] Reports make clear that when advocates contact human rights mechanisms, they often face real harm. In addition to self-censoring as a result of digital surveillance, advocates have reported feeling fear, exhaustion, and depression.[28]

OHCHR's March 2022 website redesign, this document was available at a different link (https://www.ohchr.org/Documents/HRmechanisms/SP/factsfigures2006.pdf), which no longer works.

[24] For example, thirty-two of the forty-two States currently party to the European Social Charter ratified that instrument in the year 2000 or later. *See European Social Charter, Signatures & ratifications*, COE, https://www.coe.int/en/web/european-social-charter/signatures-ratifications (last visited Sept. 4, 2022). The European Committee of Social Rights was authorized to begin accepting collective complaints in 1998. *See Chart of signatures and ratifications of Treaty 158*, COE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/158/signatures?p_auth=F3KSQtYr. Additionally, the individual complaint mechanisms for the Committee on Economic, Social and Cultural Rights and for the Committee on the Rights of the Child became operational in 2013 and 2014, respectively.

[25] The African Committee of Experts on the Rights and Welfare of the Child (ACERWC) was established in 2001. *See ACERWC Secretariat*, AFR. UNION, https://au.int/en/sa/acerwc (last visited Sept. 4, 2022). In 2019, there were fifty-six United Nations Special Procedure mandates, compared to forty-one in 2006. *See* U.N. Hum. Rts. Council, *Facts and figures with regard to the special procedures in 2019* 16, *supra* note 23, at 3; Off. High Comm'r Hum. Rts., *United Nations Special Procedures: Facts and Figures 2006*, *supra* note 23, at 1. Four of the ten United Nations human rights treaty bodies - the Committee on the Rights of Persons with Disabilities (2008), Committee on the Rights of Migrant Workers (2003), Committee on Enforced Disappearances (2010), and Subcommittee on Prevention of Torture (2006) - have come into being since 2003. Their individual complaint mechanisms have also become operational, except in the case of the Committee on the Rights of Migrant Workers, whose envisioned individual complaint mechanism has not yet been accepted by the requisite number of States. *See generally Ch. IV: Human Rights*, U.N. TREATY COLLECTION, https://treaties.un.org/Pages/Treaties.aspx?id=4&subid=A&clang=_en.

[26] *See, e.g.*, Press Release, Human rights: Reported reprisals continue unabated, says UN, Off. High Comm'r Hum. Rts. (Sept. 30, 2020), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26322&LangID=E.

[27] Inter-Am. Comm'n H.R., *Integral Protection Policies for Human Rights Defenders* ¶ 94 (2017), http://www.oas.org/en/iachr/reports/pdfs/Defensores-eng-2017.pdf.

[28] Front Line Defenders, *Living Under Digital Surveillance: Human Rights Defender Perceptions and Experience* (June 23, 2016), https://www.frontlinedefenders.org/en/resource-publication/living-under-digital-surveillance (last visited Sept. 4, 2022).

Moreover, advocates identify gaps in access to documents and other information on human rights mechanisms' activities as significant barriers to their effectiveness as rights defenders.[29] When advocates cannot safely communicate with human rights mechanisms or obtain the information they need, their ability to investigate, document, and report human rights abuses is hampered and may even be foreclosed. Such obstacles, of course, have broader consequences for the protection of human rights worldwide. Human rights mechanisms' impact depends on advocates' capacity to inform them of emerging or ongoing abuses, submit complaints, and advocate for States' implementation.

A. Relevant Mechanisms and Their Mandates

This article focuses on the seventy-six regional and United Nations human rights mechanisms that both regularly receive sensitive information directly from advocates and publish materials that advocates use to assess and promote States' implementation of their human rights commitments.[30] These seventy-six mechanisms comprise eight regional bodies, ten U.N. treaty bodies, and fifty-eight U.N. Special Procedures. Specifically, the eight regional human rights mechanisms included here are the African Commission on Human and Peoples' Rights (ACHPR); African Committee of Experts on the Rights and Welfare of the Child (ACERWC); African Court on Human and Peoples' Rights (AfCHPR); Council of Europe (COE) Commissioner for Human Rights; European Committee of Social Rights (ECSR); European Court of Human Rights (ECtHR); Inter-American Commission on Human Rights (IACHR); and Inter-American Court of Human Rights (IACtHR).[31]

---

[29] *See, e.g.*, INT'L JUST. RES. CTR., CIVIL SOCIETY ACCESS TO INTERNATIONAL OVERSIGHT BODIES: AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS 15, 19 (2018), https://ijrcenter.org/wp-content/uploads/2018/10/Civil-Society-Access-ACHPR-2018.pdf; INT'L JUST. RES. CTR., CIVIL SOCIETY ACCESS TO INTERNATIONAL OVERSIGHT BODIES: INTER-AMERICAN COMMISSION ON HUMAN RIGHTS 33, 43 (2019), https://ijrcenter.org/wp-content/uploads/2019/05/Civil-Society-Access-IACHR-2019.pdf.

[30] This article does not include the Association of Southeast Asian Nations Intergovernmental Human Rights Commission or Arab Human Rights Committee, which do not generally receive confidential information from advocates. Also excluded are the various, smaller regional human rights mechanisms, such as the European Commission against Racism and Intolerance and the Working Group on the Protocol of San Salvador, as well as mechanisms whose mandate is limited to systemic abuses or general discussion or review of States' human rights practices, such as the Human Rights Council or Commission on the Status of Women. However, a closer look at their information management practices is also called for.

[31] *See generally African Human Rights System*, INT'L JUST. RES. CTR., https://ijrcenter.org/regional/african/ (last visited Sept. 4, 2022); *European Human Rights Bodies*, INT'L JUST. RES. CTR., https://ijrcenter.org/regional/europe/ (last visited Sept. 4, 2022); *Inter-American Human Rights System*, INT'L JUST. RES. CTR., https://ijrcenter.org/regional/inter-american-system/ (last visited Sept. 4, 2022).

The relevant United Nations human rights mechanisms include the ten treaty bodies[32] established to oversee States' implementation of a specific United Nations human rights agreement, and the fifty-eight Special Procedures composed of one or more experts authorized by the United Nations Human Rights Council to monitor human rights according to specific themes or in particular countries.[33] Physically and online, the United Nations Office of the High Commissioner for Human Rights (OHCHR) serves as the home and secretariat for treaty bodies and Special Procedures.[34] As such, the OHCHR is the point of contact for advocates engaging with United Nations human rights mechanisms.

These regional and United Nations mechanisms define States' human rights obligations and hold them to account through processes that are intended to be public and transparent. Their methods of oversight include deciding complaints, undertaking country visits, or regularly reviewing States' implementation of their treaty commitments. These bodies also depend at least as much on civil society input as on State participation, in order to understand and react to human rights conditions across a region or around the world.[35] As such, their information management policies are of particular importance.

B. Sending Up a Flare

Regional and United Nations human rights mechanisms appear to be recognizing some information management gaps and initiating reforms, though incrementally. The ACHPR, for example, has recently adopted a communications strategy (although it is not available online).[36] The IACHR is in the process of

---

[32] These are the Human Rights Committee; Committee on Economic, Social and Cultural Rights; Committee Against Torture; Committee on Enforced Disappearances; Committee on the Elimination of Racial Discrimination; Committee on the Elimination of Discrimination against Women; Committee on the Rights of Persons with Disabilities; and the Committee on the Rights of the Child; Committee on Migrant Workers; and Subcommittee on the Prevention of Torture. *See UN Human Rights Treaty Bodies*, INT'L JUST. RES. CTR., https://ijrcenter.org/un-treaty-bodies/ (last visited Sept. 4, 2022).

[33] *See Special Procedures of the Human Rights Council*, Off. High Comm'r Hum. Rts, https://www.ohchr.org/en/special-procedures-human-rights-council (last visited Sept. 4, 2022) (indicating there are fifty-eight special procedures as of October 2021).

[34] *See* G.A., Res. 48/141, High Commissioner for the Promotion and Protection of All Human Rights (Dec. 20, 1993), https://undocs.org/A/RES/48/141.

[35] *See generally* Off. High Comm'r Hum. Rts., *Procedures and Practices in Respect of Civil Society Engagement with International and Regional Organizations: Report of the United Nations High Commissioner for Human Rights*, ¶ 56, U.N. Doc. A/HRC/38/18 (Apr. 2018), https://undocs.org/a/hrc/38/18 (describing "[t]he effective functioning of international and regional organizations," including their human rights mechanisms, as "inexorably linked to civil society participation"). (The International Justice Resource Center, of which the author is executive director, contributed to the preparation of this report.)

[36] *See* Afr. Comm'n Hum. & Peoples' Rts., *Final Communique of the 65th Ordinary Session of the African Commission on Human and Peoples' Rights* ¶ 35 (2019),

developing a policy on public access to its information, more than a decade after resolving to do so.[37] The United Nations Secretary-General has adopted principles to shape its eventual data protection policy[38] and the African Union (AU) is developing new standards on data protection, cybersecurity, and access to information that would apply to all its organs.[39]

In addition to being slow to take shape, these envisioned developments have progressed incrementally. For example, an AfCHPR representative suggested that a privacy policy would only be necessary if its new website allowed public comments—a suggestion that does not take into consideration the ways in which the AfCHPR already collects information of individuals online, such as through its newsletter subscription form.[40] Separately, the IACHR's new "User Support" section is meant to "[g]uide users in the use of the most suitable means of submission or tools according to their requirements,"[41] but merely directs visitors to use the general IACHR email address for questions.[42] Consider the millions and millions of people entitled to turn to each of these bodies for protection and redress, and the lack of clarity and security around the exchange of information seems woefully inadequate. An appropriate starting point for mapping the necessary reforms may be to identify the legal standards human rights mechanisms must, or should, satisfy in their information management.

III. GOOD GUYS AND THE GOLDEN RULE: DO ACCOUNTABILITY MECHANISMS HAVE HUMAN RIGHTS OBLIGATIONS?

Must human rights mechanisms adhere to external norms? Are they obligated, for example, to respect individuals' rights to information and to

---

https://www.achpr.org/public/Document/file/English/Final%20Communique%2065%20OS.ENG.pdf.

[37] Inter-Am. Comm'n H.R., *Strategic Plan: 2017-2021* 52 (2017), http://www.oas.org/en/iachr/mandate/StrategicPlan2017/docs/StrategicPlan2017-2021.pdf; Inter-Am. Comm'n H.R. Res. 2/09, Documents and Historical Archives of the Inter-American Commission on Human Rights (Nov. 13, 2009), https://www.oas.org/en/iachr/docs/Resolutions/Resolucion.02.09.ENG.pdf.

[38] *See* U.N., *Personal Data Protection and Privacy Principles* (Oct. 11, 2018), https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf.

[39] Email from IT specialist with the AfCHPR, Dec. 12, 2020 (on file with author).

[40] On the AfCHPR's website, the Newsletter page invites visitors to sign up to receive certain announcements via email. *See Newsletter*, AFR. CT. HUM. & PEOPLES' RTS., https://www.african-court.org/wpafc/ (last visited Sept. 4, 2022).

[41] *User Support Section, Areas of Action*, INTER-AM. COMM'N H.R., http://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/usersupport/areasaccion.asp (last visited Sept. 4, 2022).

[42] *User Support Section, Contact Us*, INTER-AM. COMM'N HUM. RTS., http://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/usersupport/contact.asp (last visited Sept. 4, 2022).

privacy? If so, to what extent and under what body of law? These questions are not only significant as a matter of legal principle but also for aligning mechanisms' information management policies with the appropriate standards.

Answers to these questions are still speculative. Intergovernmental organizations (IGOs) undoubtedly have legal personality,[43] making them capable of assuming rights and obligations, in addition to responsibility for the acts of their agents.[44] However, despite their self-described autonomy,[45] it seems clear that most, perhaps all, human rights mechanisms themselves lack independent legal personhood; they are merely organs of the "parent" IGO.[46] While human rights courts enjoy greater autonomy than non-judicial mechanisms, their founding instruments typically do not specify that they have independent legal

---

[43] *See, e.g.*, Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 ICJ REP. 174 (Apr. 11, 1949); Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt, Advisory Opinion, 1980 ICJ REP. 73, 89–90 ¶ 37 (Dec. 20, 1980); Legality of the Use by a State of Nuclear Weapons in Armed Conflict, Advisory Opinion, 1996 ICJ REP. 66, 78, ¶ 25 (July 8, 1996); Int'l Law Comm'n, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries*, arts. 1, 57 (2001), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

[44] *See* Int'l Law Comm'n, *Draft Articles on the Responsibility of International Organizations*, in G.A. Res. 66/100, Responsibility of International Organizations, U.N. Doc. A/RES/66/100, annex (Dec. 9, 2011), https://undocs.org/en/A/RES/66/100; s*ee also* Int'l Law Comm'n, *Draft Articles on the Responsibility of International Organizations, with Commentaries* (2011), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_11_2011.pdf.

[45] *Compare, e.g.*, Organization of American States, American Convention on Human Rights art. 33, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123 *with* Inter-Am. Comm'n H.R., Rules of Procedure of the Inter-American Commission on Human Rights, art. 1 (2013), http://www.oas.org/en/iachr/mandate/Basics/rulesiachr2013.pdf *and* Inter-Am. Comm'n H.R., Statute of the Inter-Am. Ct. H.R., art. 1 (1979), https://www.oas.org/36ag/english/doc_referencia/Estatuto_CIDH.pdf. *See* OAS, Fifth Meeting of Consultation of Ministers of Foreign Affairs, Final Act (1960), Res. VIII, Human Rights, Part II, https://www.oas.org/council/MEETINGS%20OF%20CONSULTATION/Actas/Acta%205.pdf.

[46] *See* Int'l Law Comm'n, *Draft Articles on the Responsibility of International Organizations, with Commentaries*, *supra* note 44, art. 2, p. 52, note 82 (identifying the Charter of the OAS as an example of a constitutive document that lists the IGO's organs, among them the IACHR); s*ee also* American Convention on Human Rights, *supra* note 45, art. 33; Organization of African Unity, African Charter on Human and Peoples' Rights art. 30, Jun. 27, 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982); Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights art. 1, Jun. 10, 1998; African Charter on the Rights and Welfare of the Child art. 32, July 11, 1990, CAB/LEG/24.9/49 (1990); Eur. Ct. H.R., *The European Convention on Human Rights: A Living Instrument* 5 (2020), https://www.echr.coe.int/Documents/Convention_Instrument_ENG.pdf (describing the Court as the "judicial organ of the Council of Europe." Note, however, that the Court's relationship to the COE is not explicitly spelled out in the Convention or the Rules of Court.); Council of Europe Committee of Ministers, Res. (99) 50 on the Council of Europe Commissioner for Human Rights of 7 May 1999, Commissioner for Human Rights, art. 12(1), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e305a (establishing the Office of the Commissioner for Human Rights "within" the General Secretariat of the COE). *Cf.* UN HUMAN RIGHTS TREATY BODIES: LAW AND LEGITIMACY (Helen Keller & Geir Ulfstein eds., 2012); Geneva Academy, *The Secretariat Support to the United Nations Treaty Bodies: What is the High Commissioner for Human Rights' Mandate?: A role in Need of Clarification* 3 (June 2019), https://www.geneva-academy.ch/joomlatools-files/docman-files/The%20Secretariat%20Support%20to%20UN%20TBs.pdf.

personality.[47] The precise contours of human rights mechanisms' obligations, and the extent of their capacity to engage the legal liability of the "parent" IGO, would be a worthy focus of future scholarship. In the meantime, this discussion is focused on the IGOs themselves, which bear responsibility for their organs' actions and are also highly involved in human rights information management. After all, it is the IGOs that often provide the online platforms, communications infrastructure, administrative policies, and budgets that human rights mechanisms employ.

Despite their legal personhood, IGOs have thus far managed to avoid any obligation to ensure access to information or protect individuals' privacy. They, and their representatives, are often immune from liability under domestic law.[48] IGOs have argued that domestic or regional legal requirements do not apply to them.[49] At the international level, IGOs do not have any relevant treaty obligations of their own[50] and have so far opted only to recommend—rather than require—

---

[47] In contrast, for example, the International Criminal Court was explicitly granted independent legal personality. *See* Rome Statute of the International Criminal Court art. 4(1).

[48] IGOs' founding documents and other agreements grant them, and their experts, privileges and immunities. *See, e.g.*, Charter of the United Nations; Convention on the Privileges and Immunities of the United Nations arts. II-VI, (General Agreement) (Feb. 13, 1946), https://www.un.org/en/ethics/assets/pdfs/Convention%20of%20Privileges-Immunities%20of%20the%20UN.pdf; Charter of the OAS, arts. 133-136, https://www.cidh.oas.org/basicos/english/Basic22a.Charter%20OAS.htm; General Convention on the Privileges and Immunities of the Organization of African Unity, https://au.int/sites/default/files/treaties/7760-treaty-0001_-_general_convention_on_the_privileges_and_immunities_of_the_oau_e.pdf; Statute of the Council of Europe art. 40, https://rm.coe.int/1680306052; General Agreement on Privileges and Immunities of the COE, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063729; *see also* Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion, 1999 I.C.J. Reports 62 (Apr. 29), https://www.icj-cij.org/public/files/case-related/100/100-19990429-ADV-01-00-EN.pdf (concluding that a U.N. Special Rapporteur was entitled to the privileges and immunities of a U.N. expert on mission, including immunity from legal process, when acting in his official capacity).

[49] *See, e.g.*, U.N., *Comments of the United Nations Secretariat on behalf of the United Nations System Organizations on the "Guidelines 2/2020 on articles 46(2)(a) and 46(3) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies" adopted by the European Data Protection Board on 18 January 2020* ¶ 16 (May 14, 2020), https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf; Vince Chadwick, *UNICEF data leak reveals personal info of 8,000 online learners*, DEVEX, Sept. 9, 2019 (quoting UNICEF official saying, "U.N. entities are not subject to GDPR."); *see also* U.N., *Personal Data Protection and Privacy Principles*, *supra* note 38. *See also* Broadbent v. Organization of Am. States, 628 F.2d 27 (D.C. Cir. 1980) (in which the Organization of American States, as respondent, argued it was immune from service of process and the United Nations, as amicus curiae, argued that domestic courts lack jurisdiction over disputes relating to IGOs' employment contracts.) *See also* Brief for the United Nations as *Amicus Curiae*, 1980 U.N. Jurid. Y.B. 227, https://legal.un.org/unjuridicalyearbook/pdfs/english/by_volume/1980/chpVIII.pdf.

[50] *Cf., e.g.*, *Multilateral Treaties Deposited with the Secretary General, Participant Search*, U.N. TREATY COLLECTION, https://treaties.un.org/pages/TreatyParticipantSearch.aspx?clang=_en (last visited Sept. 4, 2022) (indicating that the United Nations is party only to the Vienna Convention on the Law of Treaties between States and International Organizations or between International

their own compliance with a limited number of international standards relevant to information management.[51]

Despite this resistance, there is appreciable consensus that IGOs *are* bound by at least some international norms.[52] Legal scholars have proposed that IGOs have human rights obligations, in particular, by virtue of: 1) their charters or other foundational texts, to the extent that they reference the promotion or protection of human rights; 2) their status as subjects of international law, bound by the norms that bind all such subjects; or, 3) the obligations of their Member States.[53] The first theory posits that IGOs are obligated to respect (not violate) human rights because their founding documents give them duties related to the advancement of human rights. Pursuant to this theory, for example, the United Nations Charter's requirement that the U.N. "promote" human rights must be viewed as an evolving obligation, in light of the Charter's purpose and with the understanding that States would not have intended to authorize rights violations by the United Nations itself.[54] The second theory proposes that IGOs, as subjects of international law, are bound by customary or shared norms, no matter their specific treaty obligations.[55] This view enjoys greatest support among scholars.[56] Notably, it is the position featured in the U.N. Audiovisual Library of

---

Organizations); *Chart of signatures and ratifications of Treaty 205, COE Convention on Access to Official Documents*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205/signatures?p_auth=DgWsCboQ (listing no IGO parties as of Sept. 4, 2022).

[51] *See* G.A. Res. 45/95, Guidelines for the regulation of computerized personal data files, U.N. Doc. A/RES/45/95 (Dec. 14, 1990), https://undocs.org/A/RES/45/95 (adopting the guidelines and "request[ing] governmental, intergovernmental and non-governmental organizations to respect" them); U.N. Comm'n Hum. Rts., *Revised version of the guidelines for the regulation of computerized personal data files prepared by Mr. Louis Joinet, Special Rapporteur*, U.N. Doc. E/CN.4/1990/72, Part II.B: Application of the guidelines to personal data files kept by governmental international organizations (Feb. 20, 1990), https://undocs.org/E/CN.4/1990/72.

[52] *See generally* CARLA FERSTMAN, INTERNATIONAL ORGANIZATIONS AND THE FIGHT FOR ACCOUNTABILITY: THE REMEDIES AND REPARATIONS GAP (2017).

[53] *See* Kristina Daugirdas, *How and Why International Law Binds International Organizations*, 57 Harvard Int'l L. J. 2 (2016), 325; Andrew Clapham, *Non-State Actors*, in INTERNATIONAL HUMAN RIGHTS LAW (2016); Mac Darrow & Louise Arbour, *The Pillar of Glass: Human Rights in the Development Operations of the United Nations*, 103 AM. J. INT'L LAW 3, 446-501 (2009); Frédéric Mégret & Florian Hoffmann, *The UN as a Human Rights Violator? Some Reflections on the United Nations Changing Human Rights Responsibilities,* HUM. RTS Q., Vol. 25, No. 2, at 317-18 (May 2003).

[54] Mégret & Hoffmann, *supra* note 53, at 317-18. *See also* Int'l Law Comm'n, *Draft Articles on the Responsibility of International Organizations, with Commentaries*, *supra* note 44, at 63 ("the international obligation 'may be established by a customary rule of international law, by a treaty or by a general principle applicable within the international legal order'").

[55] *See* Mégret & Hoffmann, *supra* note 53.

[56] *See, e.g.*, Noëlle Quénivet, *Binding the United Nations to Customary (Human Rights) Law*, 17 INT'L ORGS. L. REV. 2 (2020), https://uwe-repository.worktribe.com/output/852692/binding-the-united-nations-to-customary-human-rights-law; Daugirdas, *supra* note 53.

International Law in a lecture by Kristina Daugirdas.[57] Finally, the third theory argues that IGOs are "bound 'transitively' by international human rights standards as a result and to the extent that [their] members are bound" because States should not be able to avoid their own obligations by creating an intergovernmental organization that can violate them.[58]

Depending on which of these three theories hold, an IGO's human rights obligations are those 1) recognized in the human rights treaties adopted under its auspices and entered into by its Member States, or 2) that form part of "general international law." General international law includes customary international law (principles established by the consistent practice of States acting out of a sense of legal obligation),[59] *jus cogens* norms (peremptory norms from which no derogation is allowed, such as the prohibition on torture),[60] and general principles of law (a fuzzy concept referring to principles generally recognized in national legal systems).[61] For purposes of this Article the most relevant bodies of law are international human rights treaties and customary international norms relating to information management, to the extent that they exist.

To identify the substance of these norms, and how current practices align with them, let us begin with the initial digital contact between an advocate and a human rights mechanism. What are the vulnerabilities in existing communication channels? Can international standards help us understand what human rights mechanisms can be doing to mitigate them?

IV. SNIFFING, SPOOFING, AND OTHER RISKS TO DIGITAL COMMUNICATIONS

Information passed between advocates and human rights mechanisms may be exposed or exploited when it is intercepted in transit, which leads to risks for advocates. Governments and private actors have used various methods to monitor or interfere with advocates' digital communications. These methods include packet sniffers, through which others can view and capture data sent over

---

[57] *International Organizations: How and Why International Law Binds International Organizations*, AUDIOVISUAL LIBRARY OF INTERNATIONAL LAW, https://legal.un.org/avl/ls/Daugirdas_IO.html (last visited Sept. 4, 2022).
[58] *See* Mégret & Hoffmann, *supra* note 53, at 318.
[59] *See, e.g.*, *Customary International Law*, ENCYCLOPEDIA OF HUMAN RIGHTS (David P. Forsythe ed., 2009); s*ee also* Int'l Law Comm'n, *Draft Conclusions on Identification of Customary International Law with commentaries* (2018), https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.
[60] *See, e.g.*, *Jus Cogens*, ENCYCLOPEDIA OF HUMAN RIGHTS (David P. Forsythe ed., 2009).
[61] *See* Int'l Law Comm'n, *First Report on General Principles of Law by Marcelo Vázquez-Bermúdez, Special Rapporteur*, U.N. Doc. A/CN.4/732 (Apr. 5, 2019), https://undocs.org/en/A/CN.4/732; *see also* GIORGIO GAJA, *General Principles of Law*, MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW (Apr. 2020).

a particular computer or wireless network.[62] Another technique utilizes spoofing, which allows a third party to mimic an email or website in an attempt to collect information from targets.[63] Malware installed on cloned apps on mobile devices can give third parties access to an individual's contacts, camera, or communications.[64] Governmental mass surveillance programs have used fiber-optic splitters to copy digital data as well.[65] In the absence of strong encryption and other security measures, advocates' purportedly confidential communications may be compromised.

Human rights mechanisms have signaled their awareness of these vulnerabilities and their consequences. For example, in 2015, Michel Forst, then-UN Special Rapporteur on the situation of human rights defenders, wrote: "Fear of reprisals perpetrated by non-State or governmental actors deters some defenders from cooperating with the United Nations and regional mechanisms [in view of] surveillance exercised over them."[66] Such surveillance, the OHCHR noted a year earlier, "has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings."[67]

A. Relevant International Standards and Recommendations

International standards provide a relevant and useful measure of advocates' rights (vis-a-vis States) and expectations with regard to online security and confidentiality. These norms are particularly important in light of ongoing efforts by States to prohibit or limit some encryption tools.[68] While human rights mechanisms have not offered comprehensive guidance regarding the existence, or scope, of positive obligations related to online encryption and anonymity, they

---

[62] *See, e.g.*, Andy O'Donnell, *What Are Packet Sniffers and How Do They Work?*, LIFEWIRE, https://www.lifewire.com/what-is-a-packet-sniffer-2487312 (June 25, 2021); Chet Hosmer, *Python Forensics: A Workbench for Inventing and Sharing Digital Forensic Technology* 238 (2014), https://doi.org/10.1016/B978-0-12-418676-7.09991-6.

[63] *See, e.g.*, *The Motherboard e-Glossary of Cyber Terms and Hacking Lingo*, VICE, July 26, 2016, https://www.vice.com/en/article/mg79v4/hacking-glossary.

[64] *See, e.g.*, ACCESS NOW, HOW JOURNALISTS AND HUMAN RIGHTS DEFENDERS ARE TARGETED ONLINE: A DETAILED REPORT ON THE MIDDLE EAST AND NORTH AFRICA (2019), https://www.accessnow.org/cms/assets/uploads/2019/06/MENA-report.pdf.

[65] *See, e.g.*, *NSA Spying, How It Works*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/nsa-spying/how-it-works (last visited Sept. 4, 2022).

[66] Michel Forst (Special Rapporteur on the Situation of Human Rights Defenders), *Situation of Human Rights Defenders: Report of the Special Rapporteur on the situation of human rights defenders* ¶ 89, U.N. Doc. A/70/217 (July 30, 2015), https://undocs.org/A/70/217.

[67] Off. High Comm'r Hum. Rts., *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/27/37 (Jun. 30, 2014), https://undocs.org/A/HRC/27/37.

[68] *See, e.g.*, Press Release, U.S. Dep't of Justice, *International Statement: End-to-End Encryption and Public Safety* (Oct. 11, 2020), https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

have identified some minimum requirements.[69] These nascent norms are rooted in the rights to freedom of expression and privacy, as well as in soft law standards concerning protection of human rights advocates and their work. Communication between advocates and human rights mechanisms is an area of focus in this growing body of guidance.

1. The Right to Communicate Freely, Anonymously and Privately

Numerous human rights instruments protect the rights to freedom of expression and privacy.[70] The right to freedom of expression includes the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers" through any medium.[71] Similarly, the right to privacy protects individuals from interference with their privacy and correspondence.[72] Both rights apply online and offline.[73] States may interfere with individuals' enjoyment of these rights only insofar as any restriction is provided by law, serves a legitimate interest such as public health, and is necessary to further that interest.[74]

With regard to digital communications, human rights experts have urged States not to limit anonymous and confidential speech by restricting technologies such as end-to-end encryption. In the words of former Inter-American Special

---

[69] *But see* Danaja Fabčič Povše, *Protecting Human Rights Through a Global Encryption Provision*, *in* SECURITY AND LAW (2019), https://fentec.eu/sites/default/files/fentec/public/content-files/article/202001-%20Protecting%20Human%20Rights%20through%20a%20Global%20Encryption%20Provision.pdf (analyzing whether international law recognizes a State obligation to mandate encryption in order to protect data security and privacy).

[70] For example, as of September 4, 2022, 173 of 193 United Nations Member States have ratified the International Covenant on Civil and Political Rights (ICCPR). *See* U.N. Treaty Collection, Chapter IV: Human Rights, 4. International Covenant on Civil and Political Rights, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (last visited Sept. 4, 2022). Some of the States that are not party to the ICCPR have ratified other instruments that recognize these rights. For example, Comoros and South Sudan have ratified the African Charter on Human and Peoples' Rights. *See* Afr. Union, *List of Countries Which Have Signed, Ratified/Acceded to the African Charter on Human and Peoples' Rights* (June 15, 2017), https://au.int/sites/default/files/treaties/36390-sl-african_charter_on_human_and_peoples_rights_2.pdf.

[71] *See, e.g.*, International Covenant on Civil and Political Rights art. 19(2), December 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

[72] *See, e.g.*, *id*. at art. 17.

[73] *See, e.g.*, U.N. Hum. Rts. Comm., General Comment No. 34, Article 19: Freedoms of opinion and expression ¶ 12, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011), https://undocs.org/CCPR/C/GC/34; Off. High Comm'r Hum. Rts., *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/39/29, ¶ 11 (Aug. 3, 2018), https://undocs.org/A/HRC/39/29.

[74] *See, e.g.*, ICCPR, *supra* note 71, at art. 19(3). *See also* U.N. Special Rapporteur on Freedom of Opinion and Expression et al., *Joint Declaration on Freedom of Expression and Responses to Conflict Situations* (2015), ¶ 2(c), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=987&lID=1.

Rapporteur for Freedom of Expression Catalina Botero, "[t]he protection of the right to private life involves at least two specific policies related to the exercise of the right to freedom of thought and expression: the protection of anonymous speech and the protection of personal data."[75] In this regard, the Declaration of Principles on Freedom of Expression and Access to Information in Africa asserts that everyone has the right "to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies."[76] The IACHR has described end-to-end encrypted messaging systems as "essential to protect privacy—and consequently, freedom—of citizens' communications." Therefore, they must not be inappropriately limited by States.[77]

According to human rights mechanisms, States must do more than "[r]efrain from arbitrary or unlawful restrictions on the use of encryption and anonymity technologies." They must also actively protect and promote the use of these technologies, including as part of the State obligation to "create enabling environments for freedom of expression."[78] For example, the Declaration of Principles on Freedom of Expression and Access to Information in Africa directs States not to "condone acts of indiscriminate or untargeted collection . . . of a person's communications" by third parties.[79] Regional human rights experts, in particular, have identified a *positive* obligation "to take appropriate steps to protect digital communications systems against cyber-attacks and to bolster digital safety and security for those who are at risk of such attacks for exercising their right to freedom of expression."[80] This entails "enabling the anonymous use of digital technologies."[81] The COE, for example, has urged its Member States to

---

[75] Inter-Am. Comm'n H.R., *Freedom of Expression and the Internet* ¶ 133 (2013), http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.
[76] Afr. Comm'n Hum. & Peoples' Rts., *Declaration of Principles on Freedom of Expression and Access to Information in Africa* (2019), Principles 40(2), 41(1), https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf.
[77] Inter-Am. Comm'n H.R. & OAS, *Guide to Guarantee Freedom of Expression Regarding Deliberate Disinformation in Electoral Contexts* 25 (2019), https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf. *See also* U.N. Special Rapporteur on Freedom of Opinion and Expression et al., *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*, *supra* note 74, at ¶ 8(e).
[78] *See, e.g.*, Inter-Am. Comm'n H.R., *Twentieth Anniversary of the Joint Declaration: Challenges to Freedom of Expression in the Next Decade* (2019), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&lID=1.
[79] Afr. Comm'n Hum. & Peoples' Rts., *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, *supra* note 76, Principles 40(2), 41(1).
[80] U.N. Special Rapporteur on Freedom of Opinion and Expression et al., *Joint Declaration on Media Independence and Diversity in the Digital Age* (2018), Principle 5(d), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1100&lID=1.
[81] *Id*., Principle 1(a)(iii), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1100&lID=1.

"ensure that search engine providers apply the most appropriate security measures to protect personal data against unlawful access . . . includ[ing] 'end-to-end' encryption of the communication between the user and the search engine provider."[82] Former Special Rapporteur David Kaye likewise recommended that States "adopt laws and policies that provide comprehensive protection for and support the use of encryption [and anonymity] tools."[83]

In summary, human rights mechanisms have encouraged States to protect and not unduly restrict encryption, and in some instances, to ensure its use by third parties. However, they have not yet identified State obligations to either guarantee the general availability of encrypted communication channels or to make such channels available to individuals in their correspondence with governmental entities.

2. Specific Rights of Human Rights Advocates

In contrast, various soft law instruments, governments, and human rights mechanisms have declared that human rights advocates are entitled to communicate securely and confidentially with international human rights mechanisms.[84] The Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms ("Declaration on Human Rights Defenders") states that "everyone has the right, individually and in association with others, to unhindered access to and communication with international human rights bodies with general or special competence to receive and consider communications on matters of human rights and fundamental freedoms."[85] The

---

[82] Council of Europe Comm. of Ministers, Appendix to Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the protection of human rights with regard to search engines *(Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies)*, ¶ 10, https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2012)3.

[83] Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Encryption and Anonymity follow-up report* (Jun. 2018), ¶ 47, https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.

[84] *See, e.g.*, G.A., Res. 53/144, Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, U.N. Doc. A/RES/53/144 (Mar. 8, 1999), https://undocs.org/A/RES/53/144 [hereinafter "Declaration on Human Rights Defenders"]. *See generally* Inter-Am. Comm'n H.R., *Integral Protection Policies for Human Rights Defenders* (2017), http://www.oas.org/en/iachr/reports/pdfs/Defensores-eng-2017.pdf.

[85] Declaration on Human Rights Defenders, *supra* note 84, at art. 9(4). While the Declaration does not use the term "human rights defenders" and instead applies to "everyone," its adoption was motivated in part by repression of human rights defenders and States and human rights mechanisms have used it to define protections for this group. *See* Petter Wille and Janika Spannagel, *The History of the UN Declaration on Human Rights Defenders: Its Genesis, Drafting and Adoption*, UNIVERSAL RIGHTS GROUP (Mar. 11, 2019), https://www.universal-rights.org/blog/the-un-declaration-on-

ACHPR's Guidelines on Freedom of Association and Assembly in Africa state: "Associations shall be able to comment publicly and privately on reports submitted by States to national human rights institutions and regional and international human rights bodies, including prior to the submission of the reports in question."[86] Relatedly, the guidelines require "States [to] protect associations, including their principal and most visible members, from threats, harassment, interference, intimidation or reprisals by third parties and non-State actors."[87]

Various entities of the United Nations have recommended that intergovernmental organizations and organs themselves take steps to protect advocates' online security, in order to ensure their ability to seek international justice or protection. In 2015, former U.N. Special Rapporteur on freedom of opinion and expression David Kaye "urgently call[ed] upon entities of the United Nations system, especially those involved in human rights and humanitarian protection, to support the use of communication security tools in order to ensure that those who interact with them may do so securely."[88] Michel Forst expanded that call, urging regional intergovernmental organizations to address advocates' "digital security" and "facilitate the internalization of security awareness individually and collectively."[89] The Office of the High Commissioner for Human Rights (OHCHR) urged regional and universal intergovernmental organizations to "ensur[e] secure information channels" and to "[e]nsure the safety and security

---

human-rights-defenders-its-history-and-drafting-process/.

[86] Afr. Comm'n Hum. & Peoples' Rts., *Guidelines on Freedom of Association and Assembly in Africa* ¶ 27 (2017), https://www.achpr.org/public/Document/file/English/guidelines_on_freedom_of_association_and_assembly_in_africa_eng.pdf (emphasis added).

[87] *See id*., ¶ 30. *See also* Afr. Comm'n Hum. & Peoples' Rts.*, supra* note 76, Principle 20(2) (indicating that the Declaration applies to human rights defenders); U.N. Special Rapporteur on Freedom of Opinion and Expression et al., *Joint Declaration on Protecting and Supporting Civil Society At-Risk* (2021), https://www.osce.org/representative-on-freedom-of-media/501697 (calling on international and regional bodies to facilitate access to human rights complaint mechanisms and ensure civil society's full participation with human rights bodies). (Note, the OHCHR, IACHR, and ACHPR all announced this joint declaration by sharing the link on the OHCHR website: https://www.ohchr.org/Documents/Issues/FAssociation/newpage_jointdeclaration_9dec2021_en.pdf. *See, e.g.*, Press Release, Inter-Am. Comm'n H.R., Human Rights Experts Urge States to Protect at-Risk Civil Society Actors (Dec. 10, 2021), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1221&lID=1. When the OHCHR redesigned its website in March 2022, this link ceased to work.)

[88] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, U.N. Doc. A/HRC/29/32 (May 22, 2015), https://www.undocs.org/A/HRC/29/32. *See also* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*), Encryption and Anonymity Follow-up Report*, U.N. Doc. A/HRC/38/35/Add.5 (July 13, 2018), https://undocs.org/A/HRC/38/35/Add.5.

[89] Michel Forst (Special Rapporteur on the Situation of Human Rights Defenders), *Report of the Special Rapporteur on the situation of human rights defenders* ¶ 115(b), U.N. Doc. A/HRC/31/55 (Feb. 1, 2016), https://undocs.org/A/HRC/31/55.

of persons seeking to engage with [them], including online" in a 2018 report.[90] Separately, the United Nations Educational, Scientific and Cultural Organization recommends that all stakeholders, including international organizations, "[u]se and promote the use of open-source encryption technologies such as HTTPS Everywhere,[91] so as to facilitate more secure channels" of communication.[92]

With respect to their own role, some human rights mechanisms have explicitly recommended internal measures to help protect advocates' right to communicate confidentially with them. For example, the United Nations human rights treaty bodies have emphasized "[t]he need to respect the 'do-no-harm' principle, participation, confidentiality, safety, security, and free and informed consent" in their own efforts to protect individuals from reprisals for engaging with the treaty bodies.[93] Accordingly, the treaty bodies suggested preventive measures that "could include permitting requests from individuals or groups to provide information . . . in a confidential manner."[94] Together, these non-binding regional and United Nations statements support the argument that advocates have a right to use secure and confidential channels of communication when contacting human rights mechanisms and that States or international bodies themselves have a corresponding obligation to provide—or ensure the availability of—those channels.

Have human rights mechanisms heeded these calls to establish and protect secure communication channels for advocates? The following subsections review human rights mechanisms' various digital communication channels, and assess the vulnerabilities of each.

B. Methods and Vulnerabilities of Communication

In many of their interactions with human rights mechanisms, advocates expect that the existence and content of their communications will remain confidential. Specifically, advocates may reasonably have an expectation of confidentiality with regard to: 1) bilateral communication or meetings with a

---

[90] Off. High Comm'r Hum. Rts., *Procedures and Practices in Respect of Civil Society Engagement with International and Regional Organizations: Report of the United Nations High Commissioner for Human Rights*, *supra* note 35, at ¶¶ 61(e)-(f).

[91] HTTPS Everywhere is a browser extension created by the Electronic Frontier Foundation and The Tor Project to encrypt users' communications via HTTPS. *See* HTTPS Everywhere, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/https-everywhere.

[92] UNESCO, *Building Digital Safety for Journalism: A Survey of Selected Issues* (2015), 52, https://unesdoc.unesco.org/ark:/48223/pf0000232358.

[93] Chairs of the Human Rights Treaty Bodies, *Guidelines against Intimidation or Reprisals ("San José Guidelines")*, U.N. Doc. HRI/MC/2015/6, ¶ 5(e) (July 30, 2015), https://undocs.org/HRI/MC/2015/6.

[94] *See id*. at ¶ 18.

human rights body's members or staff; 2) submissions and correspondence related to a complaint or request for interim measures that has not yet been communicated to the State (which may not happen for years, if ever);[95] 3) submission of background or general information not explicitly intended, or requested, for dissemination; and 4) arrangements related to attending or participating in a hearing, session, or country visit.[96] Additionally, even in complaint filings that will be disclosed or referred to in published decisions, advocates may request anonymity for themselves vis-a-vis the State and public or request anonymity for the victim vis-a-vis the public.[97]

However, each human rights body uses a unique combination of tools to receive communications from advocates—including websites, email, call and messaging apps, and video conferencing software—and each type of tool has its own weaknesses. Some are more susceptible to interception and may not satisfy advocates' privacy expectations.

1. Websites

All of the regional human rights mechanisms and the OHCHR have websites through which they primarily share information with the public. Some of these are hosted on the "parent" IGO domain and others are not.[98] While the security of most of these websites has improved in recent years, some vulnerabilities remain.

Beginning in 2017, human rights mechanisms implemented hypertext transfer protocol (HTTPS) on their websites.[99] The AfCHPR and IACHR were

---

[95] The IACHR, for example, typically rejects more than 75 percent of petitions before they are communicated to the State. In 2019, it decided to open only 733 petitions while declining to open 2,460. *See Statistics by Year*, INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/multimedia/statistics/statistics.html (last visited Sept. 4, 2022).

[96] *See* discussion, *infra* Part **Error! Reference source not found.** for an explanation of human rights bodies' practices and policies regarding protection of individuals' personal information.

[97] *See, e.g.*, Afr. Ct. Hum. & Peoples' Rts., Rules of Court, Rule 41(5)-(8) (2020), https://www.african-court.org/en/images/Basic%20Documents/Rules_of_Court_-_25_September_2020.pdf; Afr. Comm'n Hum. & Peoples' Rts., Rules of Procedure of the African Commission on Human and Peoples' Rights, Rule 115(2)(b) (2020), https://www.achpr.org/public/Document/file/English/Rules%20of%20Procedure%202020_ENG.pdf ; Inter-Am. Comm'n H.R., Rules of Procedure of the Inter-American Commission on Human Rights, *supra* note 45, art. 28(2); Eur. Ct. H.R., Rules of Court, Rule 47(4) (2022), https://www.echr.coe.int/documents/rules_court_eng.pdf.

[98] *See* INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/default.asp; EUR. CT. H.R., https://echr.coe.int/Pages/home.aspx?p=home; EUR. COMM. SOCIAL RTS., https://www.coe.int/en/web/european-social-charter/home; COE COMM'R HUM. RTS., https://www.coe.int/en/web/commissioner.

[99] Many mechanisms implemented Secure Sockets Layer (SSL), technology that secure the connection between a website and a user through encryption, between mid 2017 and mid 2019. The OHCHR implemented SSL in June 2018. *See Office of the High Commissioner for Human Rights*, INTERNET ARCHIVE, https://web.archive.org/web/20180101000000*/https://www.ohchr.org/ (Jan. 1, 2018). The COE implemented SSL in approximately September 2017. *Compare Council of Europe*,

the last mechanisms to implement HTTPS in December 2020 and April 2021, respectively.[100] HTTPS provides users some protection from attacks and surveillance by encrypting each website's connection. HTTPS also conceals the content of communications or information shared via a website, but does not prevent the monitoring or collection of data concerning an individual's internet history or location.[101] In the words of Amnesty International, "[w]hen websites use HTTPS, it ensures that, even if data is intercepted by an unauthorised party while transiting the internet, it is more secure against being read than if you were using an unencrypted connection (over plain HTTP)."[102] However, even secure websites have vulnerabilities. For example, in March 2021, the ACHPR website was hit with a malware attack that filled most of the webpage on the State Parties to the African Charter with explicit text.[103]

A separate concern is the proliferation of external or personal websites, which often do not use HTTPS. United Nations Special Procedure mandate

---

INTERNET ARCHIVE, https://web.archive.org/web/20170902051840/http://www.coe.int/en/web/portal/home (Sept. 2, 2017) *with Council of Europe*, INTERNET ARCHIVE https://web.archive.org/web/20171019061020/https://www.coe.int/en/web/portal/home (Oct. 19, 2017).
The ACHPR implemented SSL in approximately July 2019. *Compare African Commission on Human and Peoples' Rights,* INTERNET ARCHIVE, https://web.archive.org/web/20190627101338/http://www.achpr.org/ (Jun. 27, 2019) *with African Commission on Human and Peoples' Rights,* INTERNET ARCHIVE, https://web.archive.org/web/20190708194045/https://www.achpr.org/ (July 8, 2019). The ACERWC implemented SSL upon launching its new website, at a new URL, in 2019. *Compare African Committee of Experts on the Rights and Welfare of the Child,* INTERNET ARCHIVE, https://web.archive.org/web/*/http://acerwc.org/ *with African Committee of Experts on the Rights and Welfare of the Child*, INTERNET ARCHIVE, https://web.archive.org/web/*/https://acerwc.africa. *See also* ACERWC, Facebook post on January 28, 2019, https://www.facebook.com/acerwc/posts/1192561330918912.

[100] As of October 2020, the websites of the IACHR and AfCHPR were not HTTPS. *See Inter-American Commission on Human Rights*, INTERNET ARCHIVE, https://web.archive.org/web/20201021101312/www.oas.org/en/iachr/ (Oct. 21, 2020); *African Court on Human and Peoples' Rights*, INTERNET ARCHIVE, https://web.archive.org/web/20201020130015/http://www.african-court.org/en/ (Oct. 20, 2020). The AfCHPR implemented https with its new website and URL in December 2020. *See* AFR. CT. H.P.R., https://www.african-court.org/wpafc/. The IACHR implemented HTTPS in April 2021, but some pages remain HTTP.

[101] *See generally HTTPS*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/https (last visited Sept. 4, 2022). *See also* Kaveh Waddell, *Encryption Won't Stop Your Internet Provider from Spying on You*, ATLANTIC, Mar. 29, 2017, https://www.theatlantic.com/technology/archive/2017/03/encryption-wont-stop-your-internet-provider-from-spying-on-you/521208/.

[102] AMNESTY INT'L, ENCRYPTION: A MATTER OF HUMAN RIGHTS 7 (2016), https://www.amnestyusa.org/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

[103] *State Parties to the African Charter*, AFR. COMM'N HUM. & PEOPLES' RTS., https://www.achpr.org/statepartiestotheafricancharter. On March 22, 2021, this webpage included a new section titled "I'm glad I now signed up" that was filled with explicit terms and links. Screenshot on file with author.

holders have indicated that there are logistical barriers and time delays in updating their official OHCHR webpages.[104] As such, many have turned to websites that they can directly control.[105] These websites are not hosted by the OHCHR, are often unsecure (not HTTPS), and would not be subject to any security measures implemented by the OHCHR.[106]

2. Email

All human rights mechanisms, except the European Court of Human Rights, invite email correspondence from the public.[107] Most mechanisms' email accounts use the same domain as the body's website, but some are distinct. For example, the ACHPR lists two institutional email addresses[108] hosted by the AU and Yahoo. In addition, human rights mechanisms' members or mandate holders often use external or personal email addresses in their work-related communications.[109] This appears to be particularly true for mechanisms whose

---

[104] Based on private conversations.

[105] *See, e.g.*, EXTREME POVERTY AND HUMAN RIGHTS, https://srpoverty.org/; HUMAN RIGHTS & TOXICS, http://www.srtoxics.org/; FREE ASSEMBLY, http://freeassembly.net/; U.N. SPECIAL RAPPORTEUR ON THE RIGHT TO HOUSING, http://unhousingrapp.org/; U.N. SPECIAL RAPPORTEUR ON HUMAN RIGHTS AND THE ENVIRONMENT, http://www.srenvironment.org/; UNITED NATIONS SPECIAL RAPPORTEUR ON THE INDEPENDENCE OF JUDGES AND LAWYERS, https://independence-judges-lawyers.org/; RIGHT TO FOOD, http://www.righttofood.org/; JAMES ANAYA, https://unsr.jamesanaya.org/; ANTI-TORTURE INITIATIVE, http://antitorture.org/; U.N. SPECIAL RAPPORTEUR ON RACISM, RACIAL DISCRIMINATION, XENOPHOBIA AND RELATED INTOLERANCE, https://antiracismsr.org/.

[106] *See, e.g.*, UNITED NATIONS SPECIAL RAPPORTEUR ON THE SITUATION OF HUMAN RIGHTS DEFENDERS, http://www.protecting-defenders.org/en (Google cautions would-be visitors to the site that their "connection is not private" and "[a]ttackers might be trying to steal your information" from the site.)

[107] *See Contact Information*, EUR. CT. H.R., https://echr.coe.int/Pages/home.aspx?p=contact&c= (last visited Sept. 4, 2022) (noting, "We would draw your attention to the fact that applications to the Court and all documents relating to the application must be sent by post, even if they have been faxed beforehand. Please bear in mind that any documents or questions relating to applications must also be sent to the Court by post."); *Contact the Court*, EUR. CT. H.R., https://app.echr.coe.int/Contact/EchrContactForm/English/22 (last visited Sept. 4, 2022). Note, however, that States and applicants may file subsequent pleadings electronically, at the Court's discretion, after the complaint has been communicated to the State. *See* EUR. CT. H.R, *Practice Directions: Written Pleadings*, https://www.echr.coe.int/Documents/PD_written_pleadings_ENG.pdf.

[108] While the URL africa-union.org is not functional, it is the domain used for AU email addresses, including those of the ACHPR staff. Separately, the AU website is: https://au.int/.

[109] For example, I have corresponded with U.N. Special Procedure mandate holders and elected members of the IACHR and AfCHPR, in matters related to their mandates, using their email addresses provided by Gmail, Yahoo, Hotmail, or their institution of regular employment.

members are elected to part-time positions,[110] which is the case for all except the ECtHR and the COE Commissioner for Human Rights.[111]

Email is notoriously vulnerable to surveillance and has long been a security concern for human rights advocates.[112] In 2005, Frontline Defenders wrote, "[i]t is imperative for human rights workers to use encryption to protect themselves and the people they are trying to help" "[s]ince unencrypted emails can be accessed and read by almost anyone."[113] Some email providers use secure sockets layer (SSL) or transport layer security (TLS) to encrypt emails. TLS protects the contents of an email, particularly if the sender and recipient use this technology.[114] Still, the use of encryption, particularly as a default, is not universal among email providers.[115]

Human rights mechanisms generally use technology that supports SSL/TLS encryption for the duration of the email's journey from sender to receiver, at least for their official email addresses. According to the STARTTLS Everywhere site, the TLS-related security of the email domains of the ACHPR, ECtHR, and other COE mechanisms is "great"[116] but the IACtHR's is "not great."[117] With regard to the IACtHR, the site warns, "This means that when you

---

[110] As just one example, former U.N. Special Rapporteur David Kaye invited correspondence to his University of California, Irvine email address while fulfilling his six-year mandate. *See Freedex.org*, INTERNET ARCHIVE (Oct. 3, 2018), https://web.archive.org/web/20181003133040/https://freedex.org/contact-us/.

[111] *See* Council of Europe, European Convention on Human Rights art. 21(3), Nov. 4, 1950, E.T.S. 5; Council of Europe Committee of Ministers, Res. (99) 50 on the COE Commissioner for Human Rights, May 7, 1999, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e305a.

[112] *See, e.g.*, FRONT LINE DEFENDERS, PROTECTION MANUAL FOR HUMAN RIGHTS DEFENDERS 100 (2005), https://www.frontlinedefenders.org/sites/default/files/protection_manual_-_english.pdf; Sydney Li & Jeremy Gillula, *Announcing STARTTLS Everywhere: Securing Hop-to-Hop Email Delivery*, ELECTRONIC FRONTIER FOUNDATION (Jun. 24, 2018), https://www.eff.org/deeplinks/2018/06/announcing-starttls-everywhere-securing-hop-hop-email-delivery; Nate Lord, *What Is Email Encryption? Definition, Best Practices & More*, DIGITAL GUARDIAN (Jan. 3, 2019), https://digitalguardian.com/blog/what-email-encryption.

[113] FRONT LINE DEFENDERS, *supra* note 112, at 100.

[114] *See, e.g., Google Workspace Admin Help, Require Mail to be Transmitted via a Secure (TLS) Connection*, GOOGLE, https://support.google.com/a/answer/2520500?hl=en (last visited Sept. 4, 2022) (explaining, "a secure TLS connection requires that both the sender and recipient must use TLS.").

[115] *See, e.g., Google Transparency Report, Email encryption in transit*, GOOGLE, https://transparencyreport.google.com/safer-email/overview; *Gmail Help, Email encryption in transit*, GOOGLE, https://support.google.com/mail/answer/6330403?hl=en (last visited Sept. 4, 2022) (explaining how to set up encryption in transit); Justinas Mazūra, *How to Encrypt Emails?*, CYBERNEWS, https://cybernews.com/secure-email-providers/how-to-encrypt-email/ (last visited Sept. 4, 2022).

[116] *See STARTTLS Everywhere, africa-union.org results*, ELECTRONIC FRONTIER FOUNDATION, https://starttls-everywhere.org/results/?africa-union.org (last visited November 7, 2020) (indicating that africa-union.org supports the use of TLS, uses a secure version of TLS, and presents a valid certificate.

[117] *See STARTTLS Everywhere, corteidh.or.cr results*, ELECTRONIC FRONTIER FOUNDATION, https://starttls-everywhere.org/results/?corteidh.or.cr (last visited Nov. 7, 2020) (indicating that the

send e-mail to this domain, anyone listening in on your network, your recipient's network, or on corteidh.or.cr networks can read your e-mails, and some can even alter them!"[118]

Even when human rights mechanisms encrypt emails in transit, however, risks to confidentiality and security persist. When using SSL/TLS, the contents of a message in transit may be accessible to the email service provider[119] or read by governmental authorities who get court-approved access through the email service provider or via mass surveillance.[120] The email metadata, including the sender, recipient, time, subject text, and the presence of any attachments,[121] would also be visible to such eavesdroppers.[122] Other threats to the security and confidentiality of email include phishing[123] and malware[124] attacks, which rely on users opening fraudulent emails. For example, human rights advocates who use Microsoft Outlook—which is used by the ACHPR[125] —have been the target of phishing scams.[126] Different email providers implement distinct protections against these kinds of attacks.[127] Only when both the sender and receiver are using

---

corteidh.or.cr domain does not present a valid certificate).

[118] *See id*.

[119] *See, e.g., Surveillance Self-Defense, Communicating with Others*, ELECTRONIC FRONTIER FOUNDATION (Jun. 9, 2020), https://ssd.eff.org/en/module/communicating-others (noting that "your messaging service provider - or the website you are browsing, or the app you are using - can see unencrypted copies of your messages" when they are encrypted with TLS, and not end-to-end encryption).

[120] 18 U.S.C. §2516, Authorization for interception of wire, oral, or electronic communications. *See also, e.g.,* Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (Jun. 27, 2014), https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data; *Data Law, About our practices and your data*, MICROSOFT, https://blogs.microsoft.com/datalaw/our-practices (last visited Sept. 4, 2022).

[121] *See, e.g.*, TACTICAL TECHNOLOGY COLLECTIVE, HOLISTIC SECURITY: A STRATEGY MANUAL FOR HUMAN RIGHTS DEFENDERS 78, https://holistic-security.tacticaltech.org/media/sections/chapterpdfs/original/HS_Complete_HiRes.pdf.

[122] *See What Should I Know About Encryption*, ELECTRONIC FRONTIER FOUNDATION, https://ssd.eff.org/en/module/what-should-i-know-about-encryption (last visited Sept. 4, 2022); *Protect the Privacy of Your Online Communication*, SECURITY IN-A-BOX (Sept. 15, 2021), https://securityinabox.org/en/communication/private-communication/ (last visited Sept. 4, 2022).

[123] For an explanation of phishing attacks and their use against human rights defenders, see Amnesty Int'l, *Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa* (Aug. 16, 2019), https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/.

[124] For an overview of malware, including how it may be introduced to a computer or smartphone by email, see Security in-a-box, *Protect Against Malware* (June 17, 2021), https://securityinabox.org/en/phones-and-computers/malware/ (last visited Sept. 4, 2022).

[125] A recent email from an ACHPR staff member read, "Get Outlook for iOs" at the bottom of the email.

[126] *See Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa*, AMNESTY INT'L (Aug. 16, 2019), https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/.

[127] *See, e.g.*, Whitson Gordon, *Switch from Your Internet Provider's Email to Something Better*, N.Y. TIMES, Jan. 24, 2020, https://www.nytimes.com/article/how-to-change-email-address.html.

an email application with end-to-end encryption are messages secure from phishing and malware attacks.[128]

In response to specific requests for information, the human rights mechanism staff members that I connected with did not know which, if any, security measures protected their email correspondence. These staff members also did not know if their institutions did, or would, accept communications through end-to-end encrypted channels such as Signal.[129] This lack of awareness regarding encryption among human rights mechanisms' staff members, as well as the absence of any relevant information (such as public keys for receiving encrypted communications)[130] on human rights mechanisms' websites and email correspondence, seems to indicate that mechanisms do not routinely or formally use end-to-end encryption[131] programs when sending messages and documents. Consequently, any advocate seeking to understand their security risks in communicating with a human rights body or seeking to use an encryption program for correspondence would need to first contact the body using its regular, less secure channels.

3. Calls and Messaging

Formally, all human rights mechanisms use traditional landlines for receiving telephone calls. They do not publicly provide mobile phone numbers or details for use on voice over internet protocol (VOIP) or messaging technology. Informally, however, staff members often use personal cell phones, Skype, and WhatsApp to communicate with advocates, who are also using those same tools.[132]

---

[128] *See, e.g.*, Dave Johnson, *A Guide to End-to-End Encryption, the System that Keeps Your Transmitted Data and Communication Secure*, BUSINESS INSIDER (May 14, 2021), https://www.businessinsider.com/end-to-end-encryption; Kate O'Flaherty, *How Private Is Your Gmail, and Should You Switch?*, GUARDIAN, May 9, 2021, https://www.theguardian.com/technology/2021/may/09/how-private-is-your-gmail-and-should-you-switch; *Proton Mail Encryption Explained*, PROTON, https://proton.me/support/proton-mail-encryption-explained (last visited Sept. 4, 2022).

[129] I requested information on digital security policies and practices from the OHCHR, ECtHR, IACHR, IACtHR, ACHPR, and AfCHPR. To date, the IACHR, AfCHPR, and ACHPR have responded substantively. The IACHR's User Support Section indicated they could not provide an answer as this information was outside their purview; the AfCHPR's IT specialist indicated that policies are under development on each of these questions; the ACHPR – via the African Union – provided a copy of the ACHPR's new Media Relations and External Communication Strategy, which does not mention encryption or security.

[130] *See A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?*, ELECTRONIC FRONTIER FOUNDATION, *supra* note 9.

[131] In correspondence with each of the human rights mechanisms, I have never had to use a key to send or receive an email.

[132] Based on personal experience.

These communication channels have varying degrees of security and have been subject to governmental surveillance and third-party hacking.[133] Some States have a long and expansive history of listening in on phone calls or collecting phone call metadata from advocates and international bodies.[134] Skype users have been targeted with malware attacks and governmental hacking.[135] Microsoft, Skype's parent company, has reportedly voluntarily shared user information with third parties and helped authorities to monitor communications.[136] WhatsApp has also been compromised by spyware attacks aimed at human rights advocates, although it has since taken steps to address its vulnerabilities.[137] As with other tools, the specific security weaknesses depend on which programs advocates and human rights mechanisms use and how they use them, as well as on the surveillance practices of the countries where they are located.[138]

---

[133] *See, e.g.*, *Surveillance Self-Defense, The Problem with Mobile Phones*, ELECTRONIC FRONTIER FOUNDATION (Oct. 30, 2018), https://ssd.eff.org/en/module/problem-mobile-phones (last visited Sept. 4, 2022); Paul Blake, *How an Attempt to Hack a Top Human Rights Activist Exposed Unprecedented iPhone Vulnerabilities*, ABC NEWS (Aug. 27, 2016), https://abcnews.go.com/Technology/attempt-hack-top-human-rights-activist-exposed-unprecedented/story?id=41671098.

[134] *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, Jun. 6, 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *ACLU History: Wiretapping: A New Kind of 'Search and Seizure,'* AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/other/aclu-history-wiretapping-new-kind-search-and-seizure (last visited Sept. 4, 2022); Tess McClure, *Why Were Police Tapping the Phones of NZ Human Rights Activists?*, VICE, Oct. 9, 2017, https://www.vice.com/en/article/59d85d/why-were-police-tapping-the-phones-of-nz-human-rights-activists; *US Plan to Bug Security Council: The Text*, GUARDIAN, Mar. 2, 2003, https://www.theguardian.com/world/2003/mar/02/iraq.unitednations1; Off. High Comm'r Hum. Rts., *Human Rights Defenders: Protecting the Right to Defend Human Rights*, Fact Sheet No. 29, 12 (2004), https://www.ohchr.org/sites/default/files/Documents/Publications/FactSheet29en.pdf ("[h]uman rights defenders are kept under surveillance and have their telephone lines cut or tapped").

[135] *See, e.g.*, Scott Shane Matthew Rosenberg & Andrew W. Lehren, *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES, Mar. 7, 2017, https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html; Kim Zetter, *Leaked Documents Show German Police Attempting to Hack Skype*, WIRED, Jan. 29, 2008, https://www.wired.com/2008/01/leaked-document/.

[136] Ryan Gallagher, *Did Skype Give a Private Company Data on Teen WikiLeaks Supporter Without a Warrant?*, SLATE, Nov. 9, 2012, https://slate.com/technology/2012/11/skype-gave-data-on-a-teen-wikileaks-supporter-to-a-private-company-without-a-warrant-report.html; Craig Timberg & Ellen Nakashima, *Skype Makes Chats and User Data More Available to Police*, WASH. POST, July 25, 2012, https://www.washingtonpost.com/business/economy/skype-makes-chats-and-user-data-more-available-to-police/2012/07/25/gJQAobI39W_story.html; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, Jun. 7, 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[137] Samuel Gibbs, *WhatsApp Hack: Have I Been Affected and What Should I Do?*, GUARDIAN, May 14, 2019, https://www.theguardian.com/technology/2019/may/14/whatsapp-hack-have-i-been-affected-and-what-should-i-do.

[138] *See, e.g.*, *Surveillance Self-Defense, How to: Use WhatsApp on Android*, ELECTRONIC FRONTIER

4. Online Forms

Several human rights mechanisms regularly use online forms to solicit information or receive communications from advocates and others. These include forms that are built into the mechanism's website (and self-hosted),[139] as well as forms that are built or hosted by third parties like Google.[140] Whether the information submitted via these forms may be intercepted depends on both the security of the connection and the security practices of the receiving entity. For example, the IACHR hosts its petition portal on an HTTPS site, which it asserts is "secure."[141] However, the petition portal's terms of use state that "any message or information you send to the Portal may be read or intercepted by others, even if there is a special notice that a particular transmission . . . is encrypted."[142] This disclaimer is necessary because even encrypted web traffic may be monitored through "man-in-the-middle" attacks, in which a third party intercepts connections to a website by impersonating the site.[143] Similarly, some tools provide varying levels of security depending on the user's account and practices and may be subject to governmental data requests.[144]

FOUNDATION, https://ssd.eff.org/en/module/how-use-whatsapp-android (last visited Sept. 4, 2022).

[139] For example, the IACHR's Individual Petition System Portal allows individuals to submit petitions and check on their status through a platform hosted on the OAS domain. *See IACHR Individual Petition System Portal*, OAS, https://www.oas.org/ipsp/default.aspx?lang=en (last visited Sept. 4, 2022).

[140] For example, the ACHPR has asked individuals to register for events using Google Forms. *See* Afr. Comm'n Hum. & Peoples' Rts., Register Questions and Request to Take the Floor, https://www.achpr.org/announcement/detail?id=99 (linking to a Google Form at https://docs.google.com/forms/d/e/1FAIpQLSdxD5iHGZLSb-AR7QfaV5CO_JBNLC2_ML6Dm5ZzgtPwRpN1xQ/viewform). The OHCHR has used other third-party service providers to conduct surveys. *See, e.g.*, *OHCHR, Survey on Good Practices in the Protection of Human Rights Defenders*, INTERNET ARCHIVE, https://web.archive.org/web/20200919165530/https://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Survey.aspx (Sept. 19, 2020) (linking to Qualtrics form https://york.qualtrics.com/jfe/form/SV_cGPcviVNX3BI6z3?Q_JFE=qdg). After the OHCHR redesigned its website in March 2022, this link led to a page stating, "Sorry, we couldn't find that page." *See Sorry, we couldn't find that page*, OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Survey.aspx.

[141] *IACHR Individual Petition System Portal*, OAS, *supra* note 139 (indicating, "This Portal offers several advantages: It is a secure site.")

[142] *IACHR Individual Petition System Portal: Terms and Conditions of Use*, INTER-AM. COMM'N H.R. & OAS, https://www.oas.org/ipsp/help/Terms_EN.htm (last visited Sept. 4, 2022).

[143] Elie Bursztein, *Understanding the Prevalence of Web Traffic Interception*, CLOUDFLARE BLOG (Sept. 12, 2017), https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/; David Meyer, *Nokia: Yes, We Decrypt Your HTTPS Data, but Don't Worry about It*, GIGAOM (Jan. 10, 2013), https://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/; Josh Harkinson, *Report: NSA Mimics Google to Monitor "Target" Web Users*, MOTHER JONES, Sept. 12, 2013, https://www.motherjones.com/politics/2013/09/flying-pig-nsa-impersonates-google/.

[144] *See* J.D. Biersdorfer, *Keeping Your Files Safe in Google's Cloud*, N.Y. TIMES, Sept. 6, 2017,

5. Video Conferencing

Many human rights mechanisms, particularly during the COVID-19 pandemic, have relied on video conferencing software to conduct their activities and consult with advocates, giving rise to additional security concerns.[145] For most of 2020 and 2021, the ACHPR and IACHR, in particular, conducted their public sessions via Zoom and invited advocates to register and participate via that platform.[146] In 2020, the prevalence of "Zoombombing" helped expose security weaknesses on Zoom, including the lack of the end-to-end encryption the company had claimed was in place.[147] Advocates and journalists also reported that Zoom blocked activists' accounts pursuant to Chinese authorities' requests, meaning those advocates could not participate in any convening held via Zoom.[148] Previously, some mechanisms used Skype or other tools to allow (limited) remote participation by advocates in meetings and hearings.[149] As mentioned above, data stored by Skype and communications conducted over the service may be subject to interception. Internal videoconferencing systems also have vulnerabilities, as evidenced by the US National Security Agency's successful attempt in 2012 to break the encryption on the UN's conferencing system.[150] Whether human rights

---

https://www.nytimes.com/2017/09/06/technology/personaltech/security-google-cloud.html; Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA, Jun. 27, 2014, https://www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data.

[145] *See, e.g.*, Citlalli Ochoa & Lisa Reinsberg, *Cancelled, postponed, virtual: COVID-19's impact on human rights oversight*, OPENGLOBALRIGHTS (July 17, 2020), https://www.openglobalrights.org/cancelled-postponed-virtual-covid-19-impact-on-human-rights-oversight/.

[146] *See, e.g.*, *Upcoming Session, 67th Ordinary Session of the African Commission on Human and Peoples' Rights,* AFR. COMM'N HUM. & PEOPLES' RTS. (Oct. 5, 2020), https://www.achpr.org/sessions/info?id=337; *IACHR Announces Calendar of Public Hearings for 178th Period of Sessions*, INTER-AM. COMM'N H.R. (Nov. 20, 2020), http://www.oas.org/en/iachr/media_center/PReleases/2020/279.asp (linking to calendar with Zoom registration links: http://www.oas.org/en/iachr/sessions/docs/CalendarioAudiencias_178PS_en.pdf).

[147] Kari Paul, *'Zoom is Malware': Why Experts Worry about the Video Conferencing Platform*, GUARDIAN, Apr. 2, 2020, https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing.

[148] Paul Mozur, *Zoom Blocks Activist in U.S. After China Objects to Tiananmen Vigil*, N.Y. TIMES, Jun. 11, 2020, https://www.nytimes.com/2020/06/11/technology/zoom-china-tiananmen-square.html; Lily Kuo & Helen Davidson, *Zoom Shuts Accounts of Activists Holding Tiananmen Square and Hong Kong Events*, GUARDIAN, Jun. 11, 2020, https://www.theguardian.com/technology/2020/jun/11/zoom-shuts-account-of-us-based-rights-group-after-tiananmen-anniversary-meeting.

[149] *See, e.g.*, INT'L JUST. RES. CTR., CIVIL SOCIETY ACCESS TO INTERNATIONAL OVERSIGHT BODIES: INTER-AMERICAN COMMISSION ON HUMAN RIGHTS, *supra* note 29, at 4; Amnesty Int'l, et al., *Position Paper on Strengthening the Human Rights Treaty Bodies in 2020 and Beyond* (2019), https://www.amnesty.org/download/Documents/IOR4012182019ENGLISH.pdf.

[150] *US Intelligence Wiretapped United Nations Headquarters*, DER SPIEGEL, Aug. 25, 2013, https://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-

bodies use external platforms or their own systems for video calls, risks of interception or introduction of malware exist.

C. Assessment of Vulnerabilities

If advocates have a right to communicate with human rights mechanisms privately and without fear of reprisals, as discussed in Part IV.A.2, confidential and secure channels of communication must be available for this purpose. This requires action on the part of mechanisms because precautions taken by advocates alone will be insufficient to fully protect their communications. The security vulnerabilities of the channels currently used by human rights mechanisms will continue to expose advocates to risk. If human rights mechanisms send unencrypted emails or if they solicit advocates' information via unsecured websites, human rights advocates' identities and the content of their communications may be revealed. While many mechanisms have made important improvements in recent years, such as increased use of encryption for their websites and email, significant gaps in technology, policies, and transparency remain.

Many channels used by human rights mechanisms have been or could be compromised by hacks or surveillance, creating risks that advocates would not necessarily perceive. Though no communication channel can provide absolute privacy and security, some are less secure than others, as reviewed above. It is exceedingly difficult for a member of the public to determine how vulnerable their own web use or digital communications might be to monitoring or interceptions. Individuals typically have little knowledge of what metadata or content a human rights mechanism or third-party service provider has access to, where and how it is stored, and whether that information might be disclosed to authorities either voluntarily or by court order. As such, advocates may have little insight into the potential risks of sharing information with human rights mechanisms using common digital channels. Moreover, human rights mechanisms do not offer accessible guidance to help advocates mitigate the risks.

If we follow advocates' communications further along their path, what other risks arise? Are human rights mechanisms responsibly and securely managing individuals' data once it is in their possession?

V. THE ADMINISTRATOR SHALL NOT BE LIABLE: PROTECTION OF INDIVIDUAL'S DATA

918421.html.

In 2019, the United Nations Under-Secretary for Global Communications tweeted a photograph of a Syrian child refugee holding up a document that revealed her last name, location, and family phone number. The Office of the United Nations High Commissioner for Refugees retweeted the image to its 2.3 million followers.[151] Based on the information divulged in that photograph, the girl and her family could have been identified and located. In light of the documented human rights abuses taking place in Syria at that time, the ongoing nature of the conflict in the country, and the precarity of many refugees' existence, exposing these details created serious risks for this refugee family and any relatives still in Syria.[152] The "astonishing" lapse exemplified an extreme version of some human rights mechanisms' routine practice of posting photographs and videos of advocates and victims to their social media channels, without ensuring those posts will not create or exacerbate safety risks for these individuals.[153]

In 2019 the United Nations also experienced an "unprecedented number" of cybersecurity threats aimed at accessing its systems or information in its possession, including 1.8 billion malicious emails, more than 20,000 "highly sophisticated attacks," and 200 compromised email accounts.[154] The United Nations OHCHR, which was among the agencies targeted in 2019, did not notify affected individuals of the breach of its system until a news outlet reported it six months later.[155] Separately, and perhaps most disturbingly, a whistleblower

---

[151] *See* Karen McVeigh, *UN communications chief under fire for tweeting refugee's details*, GUARDIAN, Sept. 3, 2019, https://www.theguardian.com/global-development/2019/sep/03/un-communications-chief-under-fire-for-tweeting-refugees-details.

[152] *See, e.g.*, Commission of Inquiry on the Syrian Arab Republic, *Report of the Independent International Commission of Inquiry on the Syrian Arab Republic*, U.N. Doc. A/HRC/49/77 (Feb. 8, 2022), https://undocs.org/A/HRC/49/77.

[153] The IACHR and ACHPR, for example, publish videos and photographs of participants and observers during their sessions and country visits. *See, e.g.*, Inter-Am. Comm'n H.R., FLICKR, https://www.flickr.com/photos/cidh/albums; Afr. Comm'n Hum. & Peoples' Rts., YOUTUBE, https://www.youtube.com/channel/UCgwJmiMTr59J0jYZJJtfzuw/videos. The U.N. human rights treaty bodies broadcast the public portions of their sessions on UN Web TV, where advocates who attend may also be visible. *See Human Rights Treaty Bodies*, UN WEB TV, https://media.un.org/en/search/categories/meetings-events/human-rights-treaty-bodies (last visited Sept. 4, 2022). To my knowledge, no human rights mechanism has a consistent practice for allowing participants or observers to decline to be photographed or recorded.

[154] G.A., Proposed programme budget for 2021, Part VIII: Common support services, § 29C: Office of Information and Communications Technology 1 (Apr. 28, 2020), https://undocs.org/A/75/6(Sect.29C). Relatedly, the Board of Auditors for the IT strategy has repeatedly flagged weaknesses in the U.N.'s digital security. *See, e.g.*, G.A., Third annual progress report of the Board of Auditors on the implementation of the information and communications technology strategy, U.N. Doc. A/74/177 (July 16, 2019), https://undocs.org/A/74/177.

[155] Press Release, Off. High Comm'r Hum. Rts., Clarification of circumstances surrounding hacking of OHCHR systems (Jan. 29, 2020), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25509&LangID=E; Ben Parker, *Exclusive: The cyber attack the UN tried to keep under wraps*, NEW HUMANITARIAN (Jan.

accused the OHCHR of sending Chinese authorities information on Uyghur dissidents and other advocates who had registered to participate in United Nations activities.[156] These incidents illustrate the urgent need for international organizations like the U.N. to adopt comprehensive data protection standards.

I focus here on data protection within the United Nations for purposes of a clear assessment and comparison with relevant international standards. However, it must also be noted that the African and Inter-American human rights mechanisms (and their parent IGOs) lack data protection policies, while the COE and its human rights mechanisms have adopted policies that fall short of regional standards.[157] Part A of this section identifies international human rights standards relevant to data protection and analyzes whether these standards have crystallized into a customary norm. Part B reviews the development of data protection standards at the regional level and among other IGOs, in comparison with the United Nations. Finally, part C details the status of internal United Nations data privacy norms.

A. International Human Rights Standards on Data Protection

Assuming that the United Nations has international human rights obligations, as discussed in Part II, to what extent would it be required to protect individuals' data? The answer depends on whether the United Nations is transitively bound by United Nations human rights treaties or, rather, by customary law.

1. International Human Rights Instruments

The human right to privacy is at the core of data protection and is enshrined in numerous instruments. The Universal Declaration of Human Rights

---

29, 2020), https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack.

[156] *See, e.g.*, Letter from David Kaye, U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Ref. OL OTH 17/2017 (Aug. 9, 2017), https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=23269; *Former UN Official Calls for Probe of Rights Body Confirming Dissident Testimonies to China*, RADIO FREE ASIA, Nov. 6, 2020, https://www.rfa.org/english/news/uyghur/testimonies-11062020164710.html; Press Release, Off. High Comm'r Hum. Rts., UN rights office categorically rejects claims it endangered NGOs (Feb. 2, 2017), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21139&LangID=E.

[157] *Compare Disclaimer*, COUNCIL OF EUROPE, https://www.coe.int/en/web/portal/disclaimer *and Privacy Statement*, EUR. CT. H.R., https://www.echr.coe.int/Pages/home.aspx?p=privacy&c= *with* Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Treaty No. 223, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

and the International Covenant on Civil and Political Rights, among other United Nations and regional standards, recognize privacy as a fundamental right.[158] Each of these agreements explicitly recognizes the right to be free from unlawful or arbitrary interference with one's privacy, family, home, and correspondence. Each agreement also includes an entitlement to legal protection of the right to privacy. Arbitrary interference with this right includes invasions of privacy that are not necessary to further a legitimate governmental purpose or to protect others' rights.[159]

IGOs and human rights accountability mechanisms have repeatedly interpreted the right to privacy to apply to personal information that is digitally processed or stored, including via new technologies.[160] Recently, for example, the United Nations General Assembly adopted a resolution recognizing data protection as a component of the right to privacy, "[e]mphasizing that . . . the unlawful or arbitrary collection of personal data . . . as highly intrusive acts, violate[s] the right to privacy."[161] The resolution urges States "[t]o consider adopting or maintaining data protection legislation, regulation and policies, including on digital communication data, that comply with their international human rights obligations."[162] It further calls on companies to share their data management policies and to respect key data protection principles, including lawful processing, data minimization, legitimate purpose, accuracy, confidentiality, access, and correction.[163]

While the law will undoubtedly continue to evolve, human rights mechanisms agree that the right to privacy requires States to ensure that governmental entities and private actors only collect personal data lawfully, fairly, and transparently; for a legitimate purpose; and, in a manner that respects the data

---

[158] G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948); International Covenant on Civil and Political Rights, *supra* note 71, art. 17; Convention on the Rights of the Child art. 16, Nov. 20, 1989, 1577 U.N.T.S. 3; International Convention on the Protection of All Migrant Workers and Members of Their Families art. 14, Dec. 18, 1990, 2220 U.N.T.S. 3; European Convention on Human Rights art. 8, *supra* note 111; American Convention on Human Rights, *supra* note 45, art. 11; African Charter on the Rights and Welfare of the Child, *supra* note 46, art. 10.

[159] These requirements are specific to Article 8 of the European Convention on Human Rights, but have also been read into the other treaties. *See, e.g.*, U.N. Hum. Rts. Comm., General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.9 (Vol.I) 191 (Apr. 8, 1988), https://undocs.org/HRI/GEN/1/Rev.9(Vol.I).

[160] *See, e.g., id*., ¶ 10. *Cf.* Inter-Am. Comm'n H.R., Declaration of Principles on Freedom of Expression, Principle 3, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26 (identifying the rights of access and correction as part of freedom of expression).

[161] G.A., Res. 75/176, The right to privacy in the digital age, U.N. Doc. A/RES/75/176, Preamble (Dec. 28, 2020), https://undocs.org/A/RES/75/176.

[162] *Id*., ¶ 7(h).

[163] *Id*., ¶ 8.

subject's rights of access and correction.[164] These core protections are considered integral and fundamental to the human right to privacy under United Nations human rights treaties.[165] At the regional level, human rights mechanisms have also urged States to adopt legislation respecting those core data protection principles.[166]

The OHCHR's 2018 report on privacy in the digital age provides the most comprehensive guidance to date, recommending that all States adopt legislation that incorporates a broad range of data protection principles.[167] It urges States to ensure that data processing is: 1) fair, lawful, and transparent; 2) based on consent or another lawful, legitimate basis; 3) necessary and proportionate to a specific, legitimate purpose; 4) limited in amount, type, and duration; 5) accurate; 6) minimized via anonymization and pseudonymization techniques, whenever possible; 7) protected by adequate security measures; and 8) subject to accountability.[168] Moreover, it asserts that individuals "have a right to know that personal data has been retained and processed, to have access to the data stored, to rectify data that is inaccurate or outdated and to delete or rectify data unlawfully or unnecessarily stored."[169] The report refers to these as "minimum standards that should govern the processing of personal data by States"[170] and describes them as

---

[164] *See, e.g.*, U.N. Hum. Rts. Comm., General Comment No. 16: Article 17 (Right to Privacy), *supra* note 159, ¶ 10; Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Right to Privacy: Report of the Special Rapporteur of the Human Rights Council on the right to privacy*, U.N. Doc. A/72/540, ¶¶ 71–75 (Oct. 19, 2017), https://undocs.org/A/72/540. –

[165] *See, e.g.*, U.N. Hum. Rts. Comm., General Comment No. 16: Article 17 (Right to Privacy), *supra* note 159, ¶ 10; Inter-Am. Comm'n H.R., *Standards for a Free, Open, and Inclusive Internet* (2016), ¶¶ 204–08, http://www.oas.org/en/iachr/expression/docs/publications/internet_2016_eng.pdf; Eur. Ct. H.R., *Factsheet: Personal Data Protection* (Oct. 2020), https://www.echr.coe.int/Documents/FS_Data_ENG.pdf. *See also* Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Right to Privacy: Report of the Special Rapporteur on the right to privacy*, U.N. Doc. A/74/277 (Aug. 5, 2019), https://undocs.org/A/74/277.

[166] *See, e.g.*, S. and Marper v. United Kingdom [GC], 2008-V Eur. Ct. H.R. 167, ¶ 103; Afr. Comm'n Hum. & Peoples' Rts., *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, *supra* note 76, Principle 42. *See generally* Eur. Ct. H.R., *Factsheet: Personal Data Protection* (Oct. 2020), *supra* note 165; Carlos Affonso Souza, Caio César de Oliveira, Christian Perrone & Giovana Carneiro, *From privacy to data protection: the road ahead for the Inter-American System of human rights*, INT'L J. HUM. RTS. (2020), https://doi.org/10.1080/13642987.2020.1789108.

[167] Off. High Comm'r Hum. Rts., *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, *supra* note 73. More recently, in her July 2022 report, the United Nations Special Rapporteur on privacy identified and compared the "common elements" of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimization, quality, responsibility, and security among regional and universal data protection standards. *See* Ana Brian Nougrères (Special Rapporteur on the Right to Privacy), *Principles Underpinning Privacy and the Protection of Personal Data*, U.N. Doc. A/77/196, 2 (Jul. 20, 2022), https://undocs.org/A/77/196.

[168] Off. High Comm'r Hum. Rts., *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, *supra* note 73, ¶ 29.

[169] *Id.* at ¶ 30.

[170] *Id.* at ¶ 28.

"the key privacy principles."[171] The OHCHR recommends States ensure adequate protection of personal data transferred internationally and establish data protection oversight bodies.[172]

International standards on data protection continue to develop, and not all human rights mechanisms have comprehensively defined States' relevant obligations under specific universal or regional treaties. At a minimum, though, it is clear that human rights mechanisms *recommend* the adoption of legislation implementing the principles of lawfulness, legitimate purpose, transparency, and individual access and correction.

2. Customary International Law

Separate from any specific human rights treaty requirements, legal scholars, the International Law Commission, and others have increasingly pointed to the possible emergence of a customary right to data protection, although a significant portion of this discussion has focused on the context of mass surveillance.[173] Customary norms bind all States and crystallize when States generally recognize the norm through their actions (State practice) and subjectively believe that their practice is required by law (*opinio juris*).[174] The tentative conclusion that data protection obligations have reached customary status is based in part on the fact that at least 126 of 193 United Nations Member States have enacted data privacy laws, and others have drafted relevant legislation.[175]

The most well-known example is the European Union's General Data Protection Regulation (GDPR).[176] Generally, the GDPR requires that public and private entities collect and store as little personally identifiable information

---

[171] *Id*. at ¶ 62(c).
[172] *Id*. at ¶¶ 32, 33.
[173] *See, e.g.*, Laurence R. Helfer & Ingrid B. Wuerth, *Customary International Law: An Instrument Choice Perspective*, 37 MICH. J. INT'L L. 563, 592–94 (2016), https://repository.law.umich.edu/mjil/vol37/iss4/1; Monika Zalnieriute, *An international constitutional moment for data privacy in the times of mass-surveillance*, INT'L J. L. & INFO. TECH., Volume 23, Issue 2, Summer 2015, pp. 99–133, https://doi.org/10.1093/ijlit/eav005.
[174] *See, e.g.*, G.A., Res. 73/203, Identification of Customary Law, U.N. Doc. A/RES/73/203, Annex, Conclusion 2 (Dec. 20, 2018), https://undocs.org/A/RES/73/203.
[175] *See, e.g.*, Graham Greenleaf & Bertil Cottier, *2020 Ends a Decade of 62 New Data Privacy Laws*, 163 PRIVACY LAWS & BUSINESS INT'L REPORT (2020) 24–26, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611 (indicating that, as of December 2019, 142 countries and territories, including 16 that are not Members of the United Nations, had enacted data privacy laws). *See also* Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611.
[176] 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) 2016 OJ (L 119) 1 [hereinafter GDPR].

(PII)[177] as is necessary for specific, legitimate purposes, using appropriate security measures; and that they process PII in lawful, fair, and transparent ways. The GDPR specifies that compliance with these standards is subject to governmental oversight.[178]

Such protection measures, even in the digital world, are not particularly new. For example, in 1980 and 1981, respectively, both the Organization for Economic Cooperation and Development (OECD) and the COE adopted guidelines and a treaty to protect the privacy of personal data.[179] They focused on "automatic processing" and included principles and language that are very similar to those of the GDPR. These standards have also inspired many national data protection laws, increasing safeguards for people around the world.[180] Intergovernmental organizations and agencies have implemented their own internal data protection policies as well.[181] Most relevantly, the COE has long had an internal data protection policy in place.[182]

Legal scholar Graham Greenleaf and others note that national data protection laws vary in their requirements and stringency, but also that they are generally "comprehensive" in covering all private and public entities.[183] Many countries share common minimum standards for data protection, and a number of

---

[177] Personally identifiable information, or "personal data," is defined in GDPR Article 4(1) to mean "any information relating to an identified or identifiable natural person, including the person's name, identification number, location data, online identifier, or by factor(s) specific to the person's "physical, physiological, genetic, mental, economic, cultural or social identity."

[178] *See* GDPR, *supra* note 176 art. 5.

[179] *See* OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[180] *See* Paul M. Schwartz, *Global Data Privacy Law: the EU Way*, 94 N.Y.U. L. REV. 771 (2019), 777–78, https://www.nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-euway/ (citing a 2017 study finding 120 countries had adopted national data privacy laws in the style of the GDPR). *See also* DLA Piper, *Data Protection Laws of the World: Full Handbook*, https://www.dlapiperdataprotection.com/index.html?t=world-map (as downloaded Oct. 16, 2020).

[181] Regulation (EU) 2018/1725 of the European Parliament and of the Council (Oct. 23, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1725.

[182] *See, e.g.*, *Privacy Statement*, EUR. CT. H.R., https://www.echr.coe.int/Pages/home.aspx?p=privacy&c= (last visited Sept. 4, 2022); COE, Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680684608.

[183] *See* Graham Greenleaf & Bertil Cottier, *Comparing African Data Privacy Laws: International, African and Regional Commitments* (Apr. 22, 2020), University of New South Wales Law Research Series, https://ssrn.com/abstract=3582478; David Banisar, *National Comprehensive Data Protection/Privacy Laws and Bills 2019* (Nov. 30, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

countries have adopted data protection laws closely modeled on the OECD Guidelines, the EU Data Protection Directive, or, more recently, the GDPR.[184]

Based on its review of international instruments, national legislation, and judicial decisions, in 2006 the International Law Commission identified "a number of core principles, including: (a) lawful and fair data collection and processing; (b) accuracy; (c) purpose specification and limitation; (d) proportionality; (d) transparency; (f) individual participation and in particular the right to access; (g) non-discrimination; (h) responsibility; (i) supervision and legal sanction; (j) data equivalency in the case of transborder flow of personal data; and (k) the principle of derogability."[185] These principles incorporate the concepts of minimization, necessity, legitimacy, correction, and accountability. For example, the International Law Commission specifies that the principle of lawful and fair collection "presupposes that the collection of personal data would be restricted to a necessary minimum."[186] The principle of purpose specification and limitation includes a requirement of individual consent or knowledge or legal authorization for the collection of data.

In subsequent years, new agreements and principles have further recognized the international consensus on data protection. For example, in 2014 the African Union adopted its Convention on Cyber Security and Personal Data Protection.[187] Among other bodies, the Department of International Law of the Organization of American States (OAS) endorsed shared principles similar to those identified by the International Law Commission as "the basis for data protection legislation worldwide."[188] The OHCHR's 2018 report draws similar conclusions, pointing to "a growing global consensus on minimum standards."[189]

In addition to widespread State practice, there is ample evidence that States believe they are required to respect individuals' data privacy. The many national and regional standards that expressly cite the human right to privacy as a core motivation for their enactment are relevant to this *opinio juris* requirement.

---

[184] *See* Daniel J. Solove & Paul M. Schwartz, *International Privacy Law*, *in* PRIVACY LAW FUNDAMENTALS 2019 (2019); Int'l Law Comm'n, *Annex IV: Protection of Personal Data in Transborder Flow of Information*, *in* YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 2006, Volume II, Part Two 219–20 (2006), https://legal.un.org/ilc/reports/2006/english/annexes.pdf#page=27.

[185] *See* Int'l Law Comm'n, *Annex IV: Protection of Personal Data in Transborder Flow of Information*, *supra* note 184, ¶ 11.

[186] *See id*. ¶ 23.

[187] *See* African Union Convention on Cyber Security and Personal Data Protection (not yet in force), https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[188] OAS, *Preliminary Principles and Recommendations on Data Protection*, OEA/Ser.G/CP/CAJP-2921/10/rev.1/corr.1 (Oct. 17, 2011), http://www.oas.org/dil/CP-CAJP-2921-10_rev1_corr1_eng.pdf. *See also* OAS *Principles on Privacy and Personal Data Protection with Annotations*, http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf.

[189] *See* Off. High Comm'r Hum. Rts., *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, *supra* note 73, ¶¶ 28–33.

For example, the European Union Data Protection Directive of 1995 repeatedly references the individual "right to privacy" as a foundational principle and legal obligation driving its adoption.[190] The preface to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data lists the various European countries that had already adopted laws "to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data."[191] The Economic Community of West African States (ECOWAS) referred to the African Charter on Human and Peoples' Rights in its Supplementary Act on data protection and described the "urgen[t] need to ensure that national laws protect privacy and freedom of information in the online space."[192] Similarly, the Mexican data protection law states that its overarching purpose is to "guarantee privacy and the right to informational self-determination" of individuals.[193]

The numerous national laws and regional agreements on data protection, together with apparent State acceptance that the right to privacy includes data protection, provide strong support for a customary international norm obligating States to adopt legislation in keeping with the "core principles" of data protection. As such, if the United Nations is bound by customary international law,[194] it may be required to implement data protection policies in line with those core principles.

B. Evolving Status of Data Protection at the UN

To date, the United Nations remains a step behind many of its Member States and peer intergovernmental organizations because of its continuing failure

---

[190] Directive 95/46/EC of the European Parliament and of the Council, Preamble ¶ 10 (Oct. 24, 1995), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. *See also* EU Regulation 2018/1725, Preamble (Oct. 23, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1725.

[191] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *supra* note 179. *See also* OECD, *Recommendation of the Council concerning the Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, *in* THE OECD PRIVACY FRAMEWORK 11 (2013) ("recognising that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information").

[192] ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (Feb. 16, 2010), http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf. *See also* Greenleaf & Cottier, *2020 Ends a Decade of 62 New Data Privacy Laws*, *supra* note 175.

[193] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF 05-07-2010, Cap I, art. 1, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (translation is the author's).

[194] *See* discussion *supra* Part **Error! Reference source not found.**.

to adopt binding internal data protection requirements. In 2018, the United Nations adopted its internal Personal Data Protection and Privacy Principles, a non-binding, brief list of recommended standards.[195] The two-page document sets out ten principles intended to apply to all personal data processed by, or on behalf of, United Nations entities "in carrying out their mandated activities."[196] The Principles indicate that United Nations entities "should" adhere to the following principles: 1) fair and legitimate processing; 2) purpose specification; 3) proportionality and necessity; 4) retention for minimum length of time; 5) accuracy; 6) confidentiality; 7) security; 8) transparency; 9) transfers only with appropriate protection; and, 10) accountability via "policies and mechanisms" for adherence. While the Principles broadly align with the GDPR's themes, they offer radically simplified, less rigorous, and optional standards. To date, the United Nations has not yet put them into practice by creating internal rules, technological changes, staff positions, or oversight procedures.

Pending the adoption of a comprehensive policy, online visitors have few clues about what data the United Nations collects through its websites, how that data is managed, and whether they can access or correct it. The United Nations has a limited privacy notice on its website, which the OHCHR links to from its separate domain. The United Nations notice indicates that any PII collected via forms "will be used only for statistical purposes," but that the United Nations "assumes no responsibility for the security of this information."[197] The related "Terms and Conditions of Use of United Nations Websites" state repeatedly that the United Nations is not liable for any negative consequence to users of United Nations websites.[198] The OHCHR links to this notice from its main site, and several of its databases contain specific terms of use with similar language disclaiming liability.[199]

Considering the volume and sensitivity of the data the United Nations collects, and the fact that the United Nations may also share that information with other agencies, these notices are inadequate to ensure data protection.[200] Every day, the OHCHR receives emails and online form submissions from advocates

---

[195] *See* U.N., *Personal Data Protection and Privacy Principles*, *supra* note 38.
[196] *Id*.
[197] *Privacy Notice*, U.N., https://www.un.org/en/sections/about-website/privacy-notice/ (last visited Sept. 4, 2022).
[198] *Terms of Use*, U.N., https://www.un.org/en/sections/about-website/terms-use/index.html (last visited Sept. 4, 2022).
[199] *See* OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/en/ohchr_homepage (last visited Sept. 4, 2022) (linking to the U.N. terms of use at the bottom of the page); *Communication Report and Search, Terms of Use*, OFF. HIGH COMM'R HUM. RTS., https://spcommreports.ohchr.org/About/TermOfUse (last visited Sept. 4, 2022), *Jurisprudence Database, Terms of use*, OFF. HIGH COMM'R HUM. RTS., https://juris.ohchr.org/About/TermOfUse (last visited Sept. 4, 2022).
[200] *See Indico*, U.N. GENEVA, https://indico.un.org/ (last visited Sept. 4, 2022).

and victims of human rights abuses that contain complaints, reports, requests for accreditation to attend meetings, and queries.[201] These submissions regularly contain PII.[202] Additionally, people from around the world regularly visit the OHCHR website for informational purposes, including to sign up for email communications.[203] Yet these individuals, including human rights advocates, have almost no control over or insight into what PII the United Nations collects, stores, or shares.

C. A Hole to Be Filled

Data protection policies are urgently needed to safeguard the privacy and security of the advocates and victims who rely on the United Nations to promote and protect human rights worldwide. Thus far, the United Nations and OHCHR have declined to adopt mandatory data protection standards, provide individuals clear channels for access or correction, or publicly share any safeguards or policies already in place. The principles and plans endorsed to date are voluntary in both their adoption and their implementation.[204] Furthermore, their primary goals often include improving organizational functioning and impact,[205] rather than protecting individuals' privacy and security. For example, the Secretary-

---

[201] For an indication of the volume of communications, note that in 2019, the human rights treaty bodies reviewed 133 States (a process that involves written and in-person interventions from as many civil society organizations as want to participate); registered 640 new individual complaints and 248 "urgent actions;" and received 27,771 emails to the OHCHR email address for complaints. *See* Off. High Comm'r Hum. Rts., *UN Human Rights Report 2019* 420-21 (2020), https://web.prod.ohchr.un-icc.cloud/en/publications/annual-report/ohchr-report-2019.

[202] For example, registering to participate in-person in a session of the U.N. Committee Against Torture requires providing one's name, date of birth, email address, organizational affiliation, permanent address, telephone number, occupation, photograph, gender, passport details, and temporary address in Geneva via an online system for managing event participation, called Indico (https://indico.un.org/). Staff at the OHCHR review these applications and communicate via email (from the cat@ohchr.org address) with those seeking accreditation to confirm receipt of the Indico request and, separately, confirm approval.

[203] While the OHCHR does not report publicly on its website traffic, SimilarWeb indicates ohchr.org received 2,500,000 visits in August 2022. *See OHCHR.org*, SIMILARWEB, https://www.similarweb.com/website/ohchr.org/ (last visited Sept. 4, 2022).

[204] *See* U.N., *Personal Data Protection and Privacy Principles*, *supra* note 38. The Principles cite no legal obligation on the part of the U.N. to protect personal data, and "encourage" U.N. entities to adhere to them, including in their development of more detailed policies and guidelines.

[205] *See, e.g.*, U.N. Development Group, *Data Privacy, Ethics and Protection: Guidance Note on Big Data for the Achievement of the 2030 Agenda* (2017), https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf (noting that the guidance is "not a legal document" and identifying three objectives: 1) establishing common principles to support the operational use of big data for achievement of the Sustainable Development Goals; 2) providing a risk-management tool; and, 3) setting principles with regard to data obtained from the private sector); U.N. Secretary-General, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity: 2020-22*, https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf (setting out goals and principles for using data to maximize impact and improve decision making).

General's data strategy describes the goal of improving United Nations data protection and privacy practices to retain partners' trust, avoid fragmentation, and maximize the use of data for public good.[206] This makes it appear less likely that a formal policy, once adopted, will address advocates' concerns and meet increasingly global data protection standards.

The existence of a human right to data protection under international human rights treaty law or customary law potentially bestows legal obligations on the U.N. and should guide its development of obligatory internal standards. While the United Nations Personal Data Protection and Privacy Principles largely recognize certain core rights and obligations to protect data, translating these affirmations into mandatory requirements grounded in specific legal standards would increase the security and confidence of advocates seeking to engage with United Nations human rights mechanisms. Doing so would also increase both predictability and transparency. Importantly, conforming to international standards would add oversight and redress mechanisms that are currently lacking but essential to effective data protection at the United Nations.

Having examined the policies and standards on encryption of communications and the collection and storage of personal data, this article turns to freedom of information in the subsequent section. When advocates seek information from human rights accountability mechanisms, what can they expect to find? What rights do they have to obtain the information they seek?

VI. ACCESS TO INFORMATION: OF 404S, FORMATS, AND FAQS

While regional and United Nations human rights mechanisms publish a plethora of information, they do not hold themselves to any particular accessibility standard. As shown in Table 1 at the end of subsection B, no human rights body has publicly adopted a comprehensive policy on accessibility of information.[207] Only two relevant IGOs—the OAS[208] and COE[209]—have access-to-information policies, but such policies largely exempt regional human rights mechanisms. For

---

[206] *See* U.N. Secretary-General, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity: 2020-22*, *supra* note 205, at 60.

[207] Other intergovernmental organizations and agencies have adopted relevant policies, in contrast. *See, e.g.*, World Bank, *Bank Policy: Access to Information* (2015), https://policies.worldbank.org/en/policies/all/ppfdetail/3693. As discussed *infra* Part VI.A.0, many States have also adopted access-to-information legislation. *See also, e.g.*, Freedom of Information Act, 5 U.S.C. § 552.

[208] General Secretariat of the OAS, *Access to Information Policy* (2012), http://www.oas.org/legal/english/gensec/EXOR1202.DOC.

[209] *See generally Documents, Records and Archives*, COUNCIL OF EUROPE, https://www.coe.int/en/web/documents-records-archives-information; Council of Europe, *Council of Europe Records and Archives Policy*, DGA/DIT (2018) 1, https://rm.coe.int/council-of-europe-records-and-archives-policy/168090759d.

example, the OAS policy states that the OAS will not disclose "any document relating to the Inter-American Commission on Human Rights and its Executive Secretariat."[210] The situation has not changed since 2017, when David Kaye, then-Special Rapporteur on freedom of expression, described the lack of such policies at the United Nations and other international organizations as "intolerable."[211] Moreover, as discussed in subsection C and shown in Table 2, human rights mechanisms have inconsistent practices in their publication, translation, and dissemination of case decisions, details on their own internal composition, and other critical information.

A. Relevant International Standards and Recommendations

What rights do individuals have to access information, generally? What obligations do public entities have to provide—or facilitate—access to their documents, and what exceptions, procedural rights, and oversight are allowed or required? This section reviews the current state of treaty and customary law on the individual's right of access to information.

1. International Human Rights Instruments

Two years before adopting the Universal Declaration of Human Rights, which enshrines the right to "seek, receive and impart information and ideas through any media and regardless of frontiers,"[212] the United Nations General Assembly resolved: "Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated."[213] Regional and United Nations human rights treaties drafted in the following decades similarly guarantee a right to receive—and, sometimes, to seek—"information and ideas without interference by public authority."[214] While these initial statements were more of a rejection of censorship than an endorsement of any governmental obligation of transparency,[215] a specific right

---

[210] General Secretariat of the OAS, *Access to Information Policy*, *supra* note 207, § IV(1)l.
[211] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/72/350, 2 (Aug. 18, 2017), https://undocs.org/A/72/350.
[212] Universal Declaration of Human Rights, *supra* note 158, art. 19.
[213] G.A., Res. 59(1), *Calling of an International Conference on Freedom of Information*, U.N. Doc. A/RES/59(I) (Dec. 14, 1946), https://undocs.org/en/A/RES/59(I).
[214] European Convention on Human Rights, *supra* note 111, art. 10(1). *See also* African Charter on Human and Peoples' Rights, *supra* note 46 art. 9(1); ICCPR, *supra* note 71, art. 19(2); American Convention on Human Rights, *supra* note 45, art. 13(1).
[215] This is clear from the following sentence of Resolution 59(1), which states, "Freedom of information implies the right to gather, transmit and publish news anywhere and everywhere without

of "access to information" held by governmental entities began to take shape in subsequent years.

Recognition of the right to access public information first appeared in national legislation[216] and then in international developments including a 1981 COE Committee of Ministers recommendation.[217] In the 1990s, States emphasized the importance of access to information when they created a United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[218] and an OAS Special Rapporteur for Freedom of Expression,[219] and adopted the United Nations Declaration on Human Rights Defenders.[220] Pursuant to these views, governments have a positive obligation to make information available to the public via formalized processes and as a default, subject only to narrow limits established in law.[221]

---

fetters." *See* G.A., Res. 59(1), *supra* note 213, Preamble. *See also, e.g.*, Toby Mendel, *Freedom of Information: A Comparative Legal Survey* 8 (2d ed. 2008), https://law.yale.edu/sites/default/files/documents/pdf/Intellectual_Life/CL-OGI_Toby_Mendel_book_%28Eng%29.pdf.

[216] By 1980, five U.N. Member States had enacted national legislation establishing a right of access to information. *See Right2Info*, INTERNET ARCHIVE, https://web.archive.org/web/20200918101415/https://www.right2info.org/resources/publications/countries-with-ati-laws-1/view (Sept. 18, 2020) (housing the Open Society Justice Initiative factsheet entitled *States that Guarantee a Right of Access to Information (RTI) in National/Federal Laws or Decrees + Dates of Adoption & Significant Amendments: 127 (out of 193) UN member states + 2 non-member states, as of May 2019*).

[217] Council of Europe Committee of Ministers, *Recommendation No. R (81) 19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities* (Nov. 25, 1981), https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-81-19-of-the-committee-of-ministers-to-member-states-on-the-access-to-information-held-by-public-authorities.

[218] *See* U.N. Comm'n Hum. Rts., *Right to freedom of opinion and expression*, U.N. Doc. E/CN.4/1993/L.48, ¶ 11 (Mar. 4, 1993), https://undocs.org/E/CN.4/1993/L.48.

[219] *See Special Rapporteurship for Freedom of Expression, History*, INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/expression/showarticle.asp?artID=52&lID=1 (last visited Sept. 4, 2022) (describing the creation of the Office of the Special Rapporteur for Freedom of Expression, in 1997).

[220] Declaration on Human Rights Defenders, *supra* note 84.

[221] *See, e.g.*, Inter-Am. Comm'n H.R. Declaration of Principles on Freedom of Expression, Principle 4 (Oct. 2000), http://www.oas.org/en/iachr/mandate/Basics/declaration-principles-freedom-expression.pdf; Abid Hussain (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. Abid Hussain, submitted in accordance with Commission resolution 1999/36*, U.N. Doc. E/CN.4/2000/63, ¶¶ 42-44 (Jan. 18, 2000), https://undocs.org/en/E/CN.4/2000/63 (endorsing the Article 19 principles entitled "The Public's Right to Know: Principles on Freedom of Information Legislation" and identifying key considerations for the adoption of national freedom of information legislation); Abid Hussain (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1997/26*, U.N. Doc. E/CN.4/1998/40, ¶¶ 11–12 (Jan. 28, 1998), https://undocs.org/E/CN.4/1998/40.

Subsequent case law and soft law[222] have clarified the core components of the right of access to information.[223] According to these outputs from United Nations, Inter-American, and African human rights mechanisms, the core components include a State obligation of maximum disclosure of information, subject only to limited exceptions, and a duty to proactively publish information of public interest. Governmental entities must also establish simple, quick, and free or low-cost processes for requesting information. Denials must be reasoned and appealable.

The OHCHR recently endorsed these core principles in its 2022 report, requested by the Human Rights Council, on good practices for the protection of the right of access to information.[224] The report indicates "in accordance with international human rights law, the normative framework [governing access to information] should be recognized by law, based on a principle of maximum disclosure, provide for proactive publication, incorporate procedures that facilitate access and include independent oversight and review." The report reiterates that the right of access to information belongs to "everyone" and "covers

---

[222] *See* Inter-Am. Comm'n H.R., Declaration of Principles on Freedom of Expression, *supra* note 221; Claude Reyes et al. v. Chile. Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R., (ser. C) No. 151 (Sept. 19, 2006), https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_ing.pdf; U.N. Hum. Rts. Comm., General Comment No. 34, *supra* note 73; Afr. Comm'n Hum. & Peoples' Rts., *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, *supra* note 76. *See also* Inter-Am. Comm'n H.R., *The Inter-American Legal Framework Regarding the Right to Access to Information* (2d ed. 2012), http://www.oas.org/en/iachr/expression/docs/publications/2013%2005%2020%20NATIONAL%20JURISPRUDENCE%20ON%20FREEDOM%20OF%20EXPRESSION.pdf; Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/68/362 (Sept. 4, 2013), https://undocs.org/A/68/362; Inter-Am. Comm'n H.R., *Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression* (2004), http://www.oas.org/en/iachr/expression/basic_documents/declarations.asp; Afr. Comm'n Hum. & Peoples' Rts., Model Law on Access to Information for Africa (2013), https://www.achpr.org/presspublic/publication?id=82; OAS, Model Inter-American Law on Access to Public Information and its Implementation Guidelines (2012), http://www.oas.org/en/sla/dil/docs/Access_Model_Law_Book_English.pdf. *See also* UNESCO, Brisbane Declaration, Freedom of Information: The Right to Know (2010), http://www.unesco.org/new/en/unesco/events/prizes-and-celebrations/celebrations/international-days/world-press-freedom-day/previous-celebrations/2010/brisbane-declaration/.

[223] *See* Sandra Coliver, *The Right of Access to Information Held by Public Authorities: Emergence as a Global Norm*, *in* REGARDLESS OF FRONTIERS 57, 69–70 (Lee C. Bollinger & Agnes Callamard eds., 2021). *See also* Off. High Comm'r Hum. RTS., *Factsheet: Access to Information* (2013), https://www.ohchr.org/Documents/Issues/Expression/Factsheet_5.pdf; David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Disease pandemics and freedom of opinion and expression*, U.N. Doc. A/HRC/44/49, ¶ 20 (Apr. 23, 2020), https://undocs.org/a/hrc/44/49.

[224] Off. High Comm'r Hum. Rts., *Freedom of Opinion and Expression: Report of the Office of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/49/38 (Jan. 10, 2022), https://undocs.org/A/HRC/49/38.

information held by public authorities" across "all branches of government," "irrespective of the content of the information and the manner in which it is stored."[225]

The ECtHR is an outlier in its more restrictive views.[226] In 2016, the Grand Chamber of the European Court of Human Rights confirmed the Court's understanding that a right of access to information only arises in certain circumstances. Specifically, such a right exists when ordered by a court or when the requestor serves a "watchdog" function by seeking to publicize information related to the public interest that is "ready and available" for the government.[227] While the new COE Convention on Access to Official Documents[228] changes this calculus with respect to its States parties,[229] the treaty still falls short of the UN, Inter-American, and African standards in its description of a more limited universe of public information that must be accessible.[230]

Separately, some human rights instruments and mechanisms have directly addressed freedom of information for persons with disabilities. Broader treaties that include a right of access to information prohibit States from discriminating against persons with disabilities.[231] More specifically, the 185 States party[232] to the United Nations Convention on the Rights of Persons with Disabilities must "take all appropriate measures to ensure that persons with disabilities can exercise the right to freedom of expression and opinion, including the freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice." This

---

[225] *Id*. at ¶ 4.

[226] *See* Magyar Helsinki Bizottság v. Hungary [GC], App. No. 18030/11 (Nov. 8, 2016), http://hudoc.echr.coe.int/eng?i=001-167828. *See generally* Eur. Ct. H.R., *Guide on Article 10 of the European Convention on Human Rights: Freedom of Expression* 71 (Aug. 31, 2020), https://www.echr.coe.int/Documents/Guide_Art_10_ENG.pdf; Council of Europe, *Explanatory Report to the COE Convention on Access to Official Documents*, ¶¶ 2, 17, 71–73, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3836.

[227] *See Magyar Helsinki Bizottság v. Hungary* [GC], App. No. 18030/11, ¶¶ 158–70.

[228] Council of Europe, Convention on Access to Official Documents ("Tromsø Convention"), June 18, 2009, CETS No. 205.

[229] *See* Council of Europe, Chart of signatures and ratifications of Treaty 205, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205/signatures (last visited Sept. 4, 2022).

[230] *See* Tromsø Convention, *supra* note 228, art. 1(2)(a)(2) (limiting the Convention's application to legislative and judicial bodies only "insofar as they perform administrative functions according to national law").

[231] *See, e.g.*, ICCPR, *supra* note 71, at arts. 2, 26; American Convention on Human Rights, *supra* note 45, at arts. 1(1), 24; African Charter on Human and Peoples' Rights, *supra* note 46, at arts. 2, 3; European Convention on Human Rights, *supra* note 111, at art. 14; Protocol No. 12 to the European Convention on Human Rights, Nov. 4, 2000, CETS No. 177; Tromsø Convention, *supra* note 228, at art. 2(1).

[232] *See* U.N. Treaty Collection, Ch. IV: Human Rights, 15. Convention on the Rights of Persons with Disabilities, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-15&chapter=4&clang=_en (last visited Sept. 4, 2022).

obligation entails specific services and accommodations, including the provision of information in accessible formats.[233] A limited collection of treaties and soft law statements supports these obligations at the regional level.[234]

In summary, universal and regional human rights treaties recognize a right to receive and share information which has been increasingly interpreted as requiring governments to provide access to information. Except for the ECtHR, all human rights mechanisms agree that this right imposes on States an obligation of maximum disclosure of information, subject to limited and defined exceptions. Per this obligation, the public must be able to request information via processes that are straightforward and not overly burdensome, either financially or otherwise. The public also has the right to appeal denials of those requests. Additionally, States have a duty to publish certain information even in the absence of a specific request, particularly when the information relates to matters of public interest. However, outside of some mechanisms' specific rule provisions, which are discussed below, human rights standards do not impose additional requirements for online publication, formatting, searchability, or translation. Moreover, beyond the direct application of the Convention on the Rights of Persons with Disabilities, human rights mechanisms have not mandated access-to-information requirements for persons with disabilities.

2. Customary International Law

---

[233] Convention on the Rights of Persons with Disabilities art. 21, Dec. 13, 2006, 2515 U.N.T.S. 3.

[234] *See* Afr. Comm'n Hum. & Peoples' Rts., *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, *supra* note 76, at Principles 7, 31(3); Organization of American States, Inter-American Convention on the Elimination of All Forms of Discrimination Against Persons with Disabilities, 7 June 1999, AG/RES. 1608 (XXIX-O/99); Afr. Comm'n Hum. & Peoples' Rts., Protocol to the African Charter on Human and Peoples' Rights on the Rights of Persons with Disabilities in Africa, Jan. 29, 2018, arts. 15, 23, 24 (as of March 28, 2022, the Protocol has been ratified by three States and has not yet entered into force. *See* Afr. Union, *List of Countries Which Have Signed, Ratified/Acceded to the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Persons with Disabilities in Africa* (Mar. 28, 2022), https://au.int/sites/default/files/treaties/36440-sl-PROTOCOL%20TO%20THE%20AFRICAN%20CHARTER%20ON%20HUMAN%20AND%20PEOPLES%E2%80%99%20RIGHTS%20ON%20THE%20RIGHTS%20OF%20PERSONS%20WITH%20DISABILITIES%20IN%20AFRICA.pdf. *See also* Council of Europe Committee of Ministers, Rec. CM/Rec(2009)8 of the Committee of Ministers to Member States on Achieving Full Participation through Universal Design (Oct. 21, 2009), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d0459. *See also* Catalina Devandas Aguilar (Special Rapporteur on the Rights of Persons with Disabilities), *Report of the Special Rapporteur on the rights of persons with disabilities*, U.N. Doc. A/HRC/31/62 (Jan. 12, 2016), https://undocs.org/en/A/HRC/31/62. *Cf.* U.N. Hum. Rts. Comm., General Comment No. 34, *supra* note 73 (containing no references to the needs of persons with disabilities, aside from a statement, in para. 12, that sign language is a form of expression protected by the ICCPR). For more on this topic, *see* Eliza Varney, *Convention on the Rights of Persons with Disabilities: ensuring full and equal access to information*, in THE UNITED NATIONS AND FREEDOM OF EXPRESSION AND INFORMATION: CRITICAL PERSPECTIVES 171 (Tarlach McGonagle & Yvonne Donders eds., 2015).

Both legislation and scholarly consensus support the conclusion that the right to access to information has become a rule of customary international law. In 2021, freedom of information lawyer and advocate Sandra Coliver argued, "it may be concluded that the right of access to information ripened into a [customary-international-law] right by 2011, if not earlier" based on the proliferation of national freedom of information legislation and human rights mechanisms' authoritative interpretations of human rights instruments.[235] It was in 2011 that the Human Rights Committee issued General Comment No. 34, describing "a right of access to information held by public bodies" and urging States to, *inter alia*, enact freedom of information legislation.[236]

As of 2020, between 118 and 126 United Nations Member States had adopted national legislation ensuring a right of access to information held by public authorities.[237] Coliver notes that such legislation is in place in countries "representing 90 percent of the world's population, and that it is taking hold in all regions, with only minor regional variations."[238] Other human rights mechanisms have recognized the proliferation of such legislation as evidence of consensus on the existence of such a right.[239] In its 2006 judgment in *Claude Reyes v. Chile*, citing OAS General Assembly resolutions and other regional documents, the IACtHR "emphasize[d] that there is regional consensus among the [OAS Member States] about the importance of access to public information and the need to protect it."[240] Similarly, in *Magyar Helsinki Bizottság v. Hungary*, the Grand Chamber of the ECtHR noted, "there exists a broad consensus, in Europe (and beyond) on the need to recognise an individual right of access to State-held information in order to assist the public in forming an opinion on matters of general interest."[241] In its 2022 report on access to information, the OHCHR described the recognition of this right as "universal."[242] Several scholars have also

---

[235] Coliver, *supra* note 223 at 68.
[236] U.N. Hum. Rts. Comm., General Comment No. 34, *supra* note 73, at 18, 19.
[237] *See* Coliver, *supra* note 223, at 62 (Figure 2.1, listing 126 U.N. Member States with such legislation as of June 2020); UNESCO, *Powering Sustainable Development with Access to Information: Highlights from the 2019 UNESCO Monitoring and Reporting of SDG Indicator 16.10.2 - Access to Information* 4 (2019), https://unesdoc.unesco.org/ark:/48223/pf0000369160 (identifying 125 countries with such legislation, as of February 2019); *By Country*, GLOBAL RIGHT TO INFORMATION RATING, http://www.rti-rating.org/country-data/ (listing 126 U.N. Member States and two non-Member States with relevant legislation) (last visited Sept. 4, 2022).
[238] *See* Coliver, *supra* note 223, at 74.
[239] *See, e.g.*, David Kaye, *Report of the Special Rapporteur of the Human Rights Council on the promotion and protection of the right to freedom of opinion and expression*, *supra* note 211, ¶ 58 (referring to the "broad global acceptance that the right of access to information held by public authorities is rooted in international law").
[240] *Claude Reyes v. Chile*, Merits, Reparations and Costs, ¶¶ 78–80.
[241] *Magyar Helsinki Bizottság v. Hungary* [GC], ¶ 148.
[242] *See* U.N. Hum. Rts. Council, *Freedom of Opinion and Expression: Report of the Office of the United Nations High Commissioner for Human Rights*, *supra* note 224, ¶ 53.

documented the widespread recognition of a right of access to information, both at the national and international levels.[243]

The timing of international legislation recognizing the right to access information, as well as the timing of States' actions and statements in support of such legislation, suggests that States have enacted their access-to-information legislation out of a sense of legal obligation, or *opinio juris*. By 2002, most States were already party to one or more relevant human rights treaties,[244] and the United Nations, African, European, and Inter-American systems had all expressly recognized a human right of access to information.[245] Since then, at least seventy-eight countries have enacted access-to-information legislation, constituting nearly two-thirds of States with ATI laws.[246]

Numerous access-to-information laws adopted since 2002 specifically reference human rights standards. The language in these laws refers to a need to "recognize" or "guarantee" an existing "fundamental" or "indispensable" right of access to information, or cites directly to international human rights instruments. Examples can be found across the globe, including in Guatemala, South Sudan, Afghanistan, Montenegro, Uruguay, Tunisia, Luxembourg, and the Philippines.[247]

---

[243] *See, e.g.*, Coliver, *supra* note 208; Mendel, *supra* note 215, at 7 (noting "there is very widespread support for [the] contention" that "the right to information ha[s] been internationally recognised as a fundamental human right"); Maeve McDonagh, *The Right to Information in International Human Rights Law*, 13 HUM. RTS L. REV. 1, 22-55 (2013).

[244] *See* U.N. Treaty Collection, Chapter IV: Human Rights, 4. International Covenant on Civil and Political Rights, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (status as at: 25-03-2021) (143 of 173 States ratified the ICCPR prior to 2000). All States party to the American Convention on Human Rights ratified it prior to 1994. *See* OAS, Multilateral Treaties, American Convention on Human Rights "Pact of San Jose, Costa Rica" (B-32), https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights_sign.htm (last visited Sept. 4, 2022). Fifty-four of fifty-five African Union Member States ratified the African Charter prior to 2000. *See* Afr. Union, *List of Countries Which Have Signed, Ratified/Acceded to the African Charter on Human and Peoples' Rights*, *supra* note 70. Forty-two of forty-seven COE Member States ratified the European Convention on Human Rights prior to 2000. *See Chart of signatures and ratifications of Treaty 205: Convention for the Protection of Human Rights and Fundamental Freedoms (Status as of 04/09/2022)*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=005 (last visited Sept. 4, 2022).

[245] *See* Afr. Comm'n Hum. & Peoples' Rts., *Declaration of Principles on Freedom of Expression in Africa, Preamble*, Part IV, *supra* note 76 (recognizing "the right of access to information held by public bodies and companies" and detailing this right in Part IV); IACHR Declaration of Principles on Freedom of Expression, Principle 4 (Oct. 2000), http://www.oas.org/en/iachr/mandate/Basics/declaration-principles-freedom-expression.pdf; Abid Hussain, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. Abid Hussain, submitted in accordance with Commission resolution 1999/36*, U.N. Doc. E/CN.4/2000/63, *supra* note 221, ¶ 43; Council of Europe Committee of Ministers, Rec. No. R (81) 19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities (Nov. 25, 1981).

[246] *See Country Data*, GLOBAL RIGHT TO INFORMATION RATING, http://www.rti-rating.org/country-data/ (last visited Sept. 4, 2022).

[247] *See, e.g.*, Congreso de la República de Guatemala, Decreto Número 57-2008, http://www.rti-rating.org/wp-content/uploads/Guatemala.pdf; Right of Access to Information Act (2013), Act. No. 65, Laws of South Sudan, ¶ 4(2), https://www.rti-rating.org/wp-content/uploads/2018/09/South-

Additionally, as members of intergovernmental organizations' political organs, States themselves recognized a right of access to public documents in, for example, the Declaration on Human Rights Defenders,[248] the European Union Charter of Fundamental Rights,[249] and resolutions and recommendations on access to public information.[250] Similarly, in the context of the Universal Periodic Review, States have on many occasions recommended that their peers ensure access to public information in their national legislation.[251] Governments have framed these statements, principles, and recommendations in relation to human rights standards, meaning that they identify an obligation grounded in international human rights law to adopt access-to-information legislation. In 2004, for example, the OAS General Assembly encouraged Member States to "provide the citizenry with broad access to public information" through their laws or regulations, and directed the OAS Special Rapporteur for Freedom of Expression to assist interested States in developing such laws.[252] The resolution references human rights instruments[253] and "reiterate[s] that states are obliged to

---

Sudan.RTI_.2013.pdf; Islamic Republic of Afghanistan, Access to Information Law (2019), https://www.rti-rating.org/wp-content/uploads/2020/01/Afghan.RTI_.Decree.May18.Amend_.Oct19.pdf (unofficial translation); Law on Free Access to Information (Montenegro), http://www.rti-rating.org/wp-content/uploads/Montenegro.pdf; Ley No. 18.381, Derecho de Acceso a la Información Pública (Uruguay), art. 1, http://www.rti-rating.org/wp-content/uploads/Uruguay.pdf; Loi organique no. 2016-22 du 24 mars 2016, relative au droit d'accès à l'information (Tunisia), http://www.rti-rating.org/wp-content/uploads/Tunisia.pdf; Accessibilite des documents, Droit d'acces (Luxembourg), art. 1 (2018), https://www.rti-rating.org/wp-content/uploads/2019/09/Luxembourg.RTI_.Sep18.pdf; Law of the Republic of Armenia on Freedom of Information, art. 6 (Sept. 23, 2003), http://www.rti-rating.org/wp-content/uploads/Armenia.pdf; Senate Bill No. 3308, Fourteenth Congress of the Republic of the Philippines (3 June 2009), https://legacy.senate.gov.ph/lis/bill_res.aspx?congress=14&q=SBN-3308. *See also* Ley de Transparencia y Acceso a la Información Pública, Decreto No. 170-2006 (Honduras), http://www.rti-rating.org/wp-content/uploads/Honduras.pdf.

[248] *See* Declaration on Human Rights Defenders, *supra* note 84, art. 6 (adopted in 1998).

[249] Charter of Fundamental Rights of the European Union arts. 11, 42, Dec. 18, 2000, 2000 O.J. (C364).

[250] *See, e.g.*, OAS G.A., AG/RES. 1932 (XXXIII-O/03), Access to Public Information: Strengthening Democracy (Jun. 10, 2003), http://www.oas.org/en/sla/dil/docs/AG-RES_1932_XXXIII-O-03_eng.pdf; Council of Europe Committee of Ministers, Rec.(2002)2 of the Committee of Ministers to Member States on access to official documents (Feb. 21, 2002), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804c6fcc. While adopted in 2002 and 2003, these documents had been in development for years.

[251] *See, e.g.*, U.N. Hum. Rts. Council, *Report of the Working Group on the Universal Periodic Review: Marshall Islands*, U.N. Doc. A/HRC/46/14, Rec. 106.60 (Dec. 22, 2020) (recommendation by the Dominican Republic that the Marshall Islands "[t]ake the necessary measures to ensure freedom of access to public information and consider adopting relevant legislation). For additional recommendations, search the Universal Human Rights Index, https://uhri.ohchr.org/.

[252] OAS G.A., AG/RES. 2057 (XXXIV-O/04), Access to Public Information: Strengthening Democracy (Jun. 8, 2004), ¶¶ 1–3, 6, http://www.oas.org/en/sla/dil/docs/AG-RES_2057_XXXIV-O-04_eng.pdf.

[253] Inter-American Press Association, Declaration of Chapultepec, https://media.sipiapa.org/adjuntos/185/documentos/001/795/0001795833.pdf. The Declaration

respect and promote respect for everyone's access to public information and to promote the adoption of any necessary legislative or other types of provisions to ensure its recognition and effective application."[254] The African model law on access to information similarly refers to human rights standards.[255]

Taken together, the broad coverage of human rights treaties guaranteeing a general right of access to public information, the many intergovernmental statements recognizing and promoting this right, and the proliferation of national legislation provide strong evidence for the existence of a customary international norm.

Considering those standards, what are human rights mechanisms' policies and practices regarding access to information? The following sub-section examines the status quo among the relevant bodies, as compared to international norms, while also raising additional accessibility and transparency considerations that may go beyond the formal requirements of freedom of information standards.

B. Formal Rules on Information Accessibility

While only the OAS and COE have (limited) access-to-information policies, all the relevant IGOs and human rights mechanisms have instituted some rules and policies governing information transparency. These include standards regarding which documents are considered public or confidential, what information must be published, when translation is required, and what degree of accessibility is required for persons with disabilities.

1. Confidentiality and Classification

All human rights mechanisms keep their internal and deliberative documents confidential, and some also limit the publication of submissions or decisions.[256] For example, "[a]ll documents prepared by the deliberations of the

states, in Principle 3, "The authorities must be compelled by law to make available in a timely and reasonable manner the information generated by the public sector."

[254] OAS G.A., AG/RES. 2057 (XXXIV-O/04), *supra* note 252, ¶ 2.

[255] *See* Afr. Comm'n Hum. & Peoples' Rts., Model Law on Access to Information for Africa, Preamble (2013), https://www.achpr.org/public/Document/file/English/Model%20Law%20on%20Access%20to%20Information%20for%20Africa%202013_ENG.pdf.

[256] *See, e.g.*, ACERWC, Revised Rules of Procedure of the African Committee of Experts on the Rights and Welfare of the Child, Rule 32 (2018), https://www.acerwc.africa/wp-content/uploads/2018/04/Revised-rules-of-procedures-final.pdf; Inter-Am. Ct. H.R., Rules of Procedure of the Inter-American Court of Human Rights, art. 15(2) (2009), https://www.corteidh.or.cr/reglamento.cfm?lang=en. *Cf.* Eur. Ct. H.R., Rules of Court, *supra* note 97, Rule 22 (2022).

[European Committee of Social Rights] . . . shall never be made public."[257] The Committee Against Torture, for instance, "may consider, at its discretion, that information, documentation and written statements received [regarding State implementation of the Convention] are confidential and decide not to make them public."[258]

Additionally, some mechanisms reserve the right to request that an individual or State keep a submission, complaint, or decision confidential.[259] In fact, the ACHPR has interpreted its founding treaty as prohibiting complainants from publishing their submissions or the ACHPR's decisions regarding a complaint until the African Union Assembly of Heads of State and Government approves the publication of the ACHPR's activity report announcing the final resolution of that complaint. The AU Executive Council has also directed the ACHPR to remove references to certain decisions from its activity reports, thereby precluding their publication.[260] This runs counter to the ACHPR's communications strategy, which identifies access to information as a core value and expresses an intent to "ensure that all decisions and actions of the ACHPR are accessible to the public, in order to fully comply with international standards on freedom of expression."[261]

---

[257] Eur. Comm. Social Rts., Rules of Procedure, Rule 38 (2022), https://www.coe.int/en/web/european-social-charter/rules. *See also* Inter-Am. Comm'n H.R., Rules of Procedure of the Inter-American Commission on Human Rights, *supra* note 45, arts. 14(3), 20(1), 43(2) (2013). *See also* Eur. Ct. H.R., Access to case files (undated), https://www.echr.coe.int/Documents/Practical_arrangements_ENG.pdf.

[258] Committee Against Torture, Rules of Procedure, Rule 63(4), U.N. Doc. CAT/C/3/Rev.6 (Sept. 1. 2014), https://undocs.org/CAT/C/3/Rev.6.

[259] *See, e.g.*, U.N. Hum. Rts. Comm., Rules of Procedure of the Human Rights Committee, Rule 111(4), U.N. Doc. CCPR/C/3/Rev.12 (Jan. 4, 2021), https://undocs.org/CCPR/C/3/Rev.12; U.N. Comm. Rts. Persons with Disabilities, Rules of Procedure, Rule 76(4), U.N. Doc. CRPD/C/1/Rev.1 (Oct. 10, 2016), https://undocs.org/CRPD/C/1/Rev.1; Afr. Comm'n Hum. & Peoples' Rts., Rules of Procedure of the African Commission on Human and Peoples' Rights, *supra* note 97, Rule 118(4). *See also* Inter-Am. Ct. H.R., Rules of Procedure of the Inter-American Court of Human Rights, *supra* note 257, art. 58(c).

[260] *See* African Charter on Human and Peoples' Rights, *supra* note 46, art. 59; Afr. Comm'n Hum. & Peoples' Rts., Rules of Procedure of the African Commission on Human and Peoples' Rights, *supra* note 97, Rule 118(4). For a discussion of the consequences of this requirement, *see* Dr. Ruth Nekura & Sibongile Ndashe, *Confidentiality or Secrecy? Interpretation of Article 59, and Implications for Advocacy on Pending Communications before the African Commission in* Equality Now, LITIGATING THE MAPUTO PROTOCOL: A COMPENDIUM OF STRATEGIES AND APPROACHES FOR DEFENDING THE RIGHTS OF WOMEN AND GIRLS IN AFRICA (K. Kanyali Mwikya, Carole Osero-Ageng'o & Esther Waweru eds., 2021), https://live-equality-now.pantheonsite.io/wp-content/uploads/2021/11/Compendium_of_Papers_on_the_Maputo_Protocol_Equality_Now_2020_Final.pdf. *See also Status of Communication 383/10, Al-Asad v. Djibouti, Before the African Commission on Human and Peoples' Rights*, CTR. HUM. RTS. & GLOBAL JUST. (July 6, 2020), https://chrgj.org/2020/07/06/status-of-communication-383-10-al-asad-v-djibouti-before-the-african-commission-on-human-and-peoples-rights/.

[261] Afr. Comm'n Hum. & Peoples' Rts., *Media Relations and External Communication Strategy for the African Commission on Human and Peoples' Rights* (2019) (on file with author). The ACHPR formally adopted the strategy at its 65th Ordinary Session in October – November 2019. *See* Afr.

2. Publication

Few specific rules govern the publication of different categories of documents, and there are few standards on timing or format. Critically, most bodies' rules do not mandate that public documents be made available online. The ECSR and ACHPR are exceptions, given that they require online publication of non-confidential documents.[262]

Regarding complaints, most human rights mechanisms require admissibility decisions and judgments to be made public, while keeping friendly settlement negotiations and initial review or screening decisions confidential.[263] For example, the AfCHPR's new Rules of Court generally require publication of pilot judgments, decisions, and requests for advisory opinions.[264] Some mechanisms do not disclose parties' submissions.[265]

Mechanisms' rules typically do not require logistical information to be published. An exception is the ACERWC, whose session agendas and related documents must be published "in the public domain at least [twenty-one] days before the opening of an Ordinary Session."[266]

3. Languages

IGOs and human rights mechanisms have official languages and working languages, but often do not clearly explain how these designations affect the availability of documents in those languages.[267] Some human rights mechanisms

---

Comm'n Hum. & Peoples' Rts., *Final Communiqué of the 65th Ordinary Session of the African Commission on Human and Peoples' Rights* ¶ 35(v) (Nov. 10, 2019), https://www.achpr.org/sessions/info?id=317.

[262] *See, e.g.*, Eur. Comm. Social Rts., Rules of Procedure, *supra* note 257, Rule 35(5); Afr. Comm'n Hum. & Peoples' Rts., Rules of Procedure, *supra* note 97, Rule 21(d), (i).

[263] *See, e.g.*, Eur. Ct. H.R., Rules of Court, *supra* note 97, Rule 104A (providing that "[a]ll judgments, all decisions and all advisory opinions shall be published" except, *inter alia*, single-judge decisions); Inter-Am. Comm'n H.R. Rules of Procedure of the Inter-American Commission on Human Rights, *supra* note 45, Rule 40(5) (publication of friendly settlements) and Rule 44 (publication of merits decisions).

[264] Afr. Ct. Hum. & Peoples' Rts., Rules of Court, *supra* note 97, Rules 21(2)(q), 66(5), 76(1), 83(2).

[265] *Compare* Afr. Comm'n Hum. & Peoples' Rts., Rules of Procedure, *supra* note 97, Rule 24(1) (mandating confidentiality of case files) *with* Inter-Am. Ct. H.R. Rules of Procedure, *supra* note 256, art. 32(1)(b) (requiring the Court to make public the "documents from the case file, except those considered unsuitable for publication").

[266] ACERWC, Revised Rules of Procedure of the African Committee of Experts on the Rights and Welfare of the Child, *supra* note 256, Rule 35(2). *See also* Inter-Am. Comm'n H.R. Rules of Procedure, *supra* note 45, arts. 64(4), 66(5).

[267] *Cf. Minimum standards for multilingualism of United Nations websites*, U.N., https://www.un.org/en/sections/web-governance/minimum-standards-multilingualism-united-nations-websites/index.html (last visited Sept. 4, 2022).

formally require translation of certain documents into all official languages,[268] though they may not always comply with this requirement in practice. Others leave the public guessing as to which languages they will use, as is the case at the IACtHR and ACERWC, which retain the option of choosing one or more unspecified working languages.

4. Accessibility for Persons with Disabilities

Most human rights mechanisms have not formally addressed accessibility to their documents or information for persons with disabilities, with several key exceptions.[269] The United Nations Human Rights Council instructed the Special Rapporteur on the rights of persons with disabilities to produce reports "in accessible formats, including Braille and easy-to-read reports, and international sign language interpretation and closed captioning during the presentation of the reports."[270] Some treaty bodies specify that their public records should be made available in "accessible formats."[271] The Committee on the Rights of Persons with Disabilities, in particular, has in place requirements to increase the accessibility of its activities and information.[272]

---

[268] *See, e.g.*, Afr. Ct. Hum. Peoples' Rts., Rules of Court, *supra* note 97, Rule 76.
[269] *Cf.* G.A., Res. 61/106: Convention on the Rights of Persons with Disabilities, U.N. Doc. A/RES/61/106, ¶ 4 (Dec. 13, 2006), https://undocs.org/A/RES/61/106; *Accessibility Guidelines for UN Websites*, U.N., https://www.un.org/en/webaccessibility/ (last visited Sept. 4, 2022).
[270] *See* U.N. Hum. Rts. Council, Res. 44/10, *Special Rapporteur on the rights of persons with disabilities*, U.N. Doc. A/HRC/RES/44/10 (July 16, 2020), https://undocs.org/A/HRC/RES/44/10.
[271] *See, e.g.*, U.N. Comm. Rts. Persons with Disabilities, Rules of Procedure, *supra* note 259, Rule 27(4).
[272] *Id.*, Rules 7, 24, 25.

Public Availability of Written Rules or Policies, as of April 2021:

Entity	Access to Information	Data Protection	Encryption	Confidentiality /Classification	Website Privacy	Translation△	Publication △	Timing of Publication △	Info Request Procedure	Unlimited Classification Discretion	Requesting Confidentiality of Others	Accessibility	Availability of Recordings
UN	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗
OHCHR	✗	✗	✗	✓	✗	✗	✗	✗	✓◆	✗	✗	✗	✗
CAT	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗
CED	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗
CEDAW	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗
CERD	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗
CESCR	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗
CMW	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✗
CRC	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	✓
CRPD	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗
HRC	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗
SPs	✗	✗	✗	✗	✗	✗	✗✢	✗	✗	✗	✗	✗*	✗
AU	✗	✗	✗	✗	✗				✗			✗	✗
ACERWC	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓		✗	✗
ACHPR	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗
AfCHPR	✗	✗	✗	✗	✗	✓	✓	✓	✗			✗	✗
OAS	✓	✗	✗		✗		✗	✗	✓	✗	✗	✗	✗
IACHR	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗
IACtHR	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗
COE	✓	✓	✗	✓	✓				✓	✗	✗	✓	✗
Comm'r	✗	✓○	✗	✗	✓○	✗	✗	✗	✗	✗	✗	✓○	✗
ECSR	✗	✓○	✗	✗	✓○	✗	✓	✗	✗	✓	✗	✓○	✗
ECtHR	✗	✓	✗	✓□	✓	✓	✓	✗	✓	✗	✗	✗	✗

△ Of certain documents.

○ Policy adopted by the "parent" intergovernmental organization.

□ Policy exists, but is not made publicly available.

◆ Policy is limited to classified records.

* The Special Rapporteur on the rights of persons with disabilities is an exception.

✢ The Working Group on Arbitrary Detention is an exception.

C. Availability of Necessary Information in Practice

In scope or implementation, the few existing rules on information accessibility are of limited value to advocates for three primary reasons. First, human rights mechanisms routinely fail to abide by some of their own rules, especially rules governing translation. Second, advocates depend on information and documents, such as treaty ratifications, session dates, or staff contacts, that are not covered by the rules and are unevenly available. Third, the relevant rules do not address formatting, organization, or presentation of information, which all have significant consequences for accessibility. Table 2 compares human rights mechanisms' online publication of certain documents and information, as well as their translation and searchability. The following subsections review these practical concerns, provide examples, and identify common gaps.

1. Publication of Critical Information

Human rights mechanisms publish a great deal of information on their websites. This information includes the texts of their treaties, rules and other basic documents, ratification information, judgments and decisions, opportunities for input and participation, recordings, and institutional information and contacts. Inconsistency, inaccuracy, untimeliness, and incompleteness in publishing practices cause the key gaps in the accessibility of this information.

Inconsistencies arise within and across human rights mechanisms. The ECtHR, for example, issues press releases announcing judgments in some cases, but not all.[273] The ACERWC posts some of its session videos to YouTube[274] and others to Facebook,[275] but none on its own website. In an example of disparate practices, the IACtHR and ECSR publish incoming complaints or related briefs while other bodies do not, even when those documents are not classified as confidential.[276]

---

[273] *See, e.g.*, Press Release, Eur. Ct. of H.R., Judgments of 16.03.2021 (Mar. 16, 2021), http://hudoc.echr.coe.int/eng-press?i=003-6965141-9374633 (announcing four judgments and identifying individual press releases on four other judgments announced the same day). The decision to issue a case-specific press release does not entirely correspond to the scale used to identify the "importance level" of judgments.

[274] *See* ACERWC, YOUTUBE, https://www.youtube.com/channel/UC06SYs77p7tTLK1rL_3XyYg/videos (last visited Sept. 4, 2022).

[275] ACERWC, FACEBOOK, https://www.facebook.com/pg/acerwc/videos/?ref=page_internal (last visited Sept. 4, 2022).

[276] *See, e.g.*, *Escritos principales de Casos con Sentencia*, INTER-AM. CT. OF H.R., https://corteidh.or.cr/listado_escritos_principales.cfm (last visited Sept. 4, 2022); *Pending complaints*, EUR. COMM. SOCIAL RTS., https://www.coe.int/en/web/european-social-charter/pending-complaints (last visited Sept. 4, 2022); *Processed complaints*, EUR. COMM. SOCIAL RTS.,

Inaccuracies also plague human rights mechanisms' online information. For example, the ACHPR's map of the continent does not portray South Sudan[277] and the list of ratifications[278] indicates that the State never deposited an instrument of ratification of the African Charter on Human and Peoples' Rights. In reality, South Sudan ratified the Charter in 2013 and deposited its instrument of ratification in 2016.[279] Someone relying on the ACHPR's information would erroneously believe that South Sudan does not have any regional human rights obligations and, moreover, is not subject to the jurisdiction of the ACHPR.

Publication lag time varies across human rights mechanisms, but is particularly detrimental to civil society participation. For example, the ACHPR often announces its country visits on its website only a few days in advance.[280] Even when advocates are aware of an opportunity and request to participate in a country visit, they may only have a week's notice that they will be allowed to participate.[281] Considering that human rights mechanisms have vast geographic jurisdiction, such short notice may be inadequate for many advocates to prepare for in-person participation. In two studies carried out between 2017 and 2019, advocates recommended that the Inter-American and African human rights commissions provide greater advance notice of upcoming sessions and other activities, increase the accessibility of such notices, and clarify the requirements and modes of participation.[282]

Finally, incomplete or missing information hampers advocates' engagement and the public's familiarity with human rights mechanisms.[283] Information on personnel[284] and on elected members' term dates and election

---

https://www.coe.int/en/web/european-social-charter/processed-complaints (last visited Sept. 4, 2022).

[277] *African Charter on Human and Peoples' Rights*, AFR. COMM'N HUM. & PEOPLES' RTS.; https://www.achpr.org/legalinstruments/detail?id=49 (last visited Sept. 4, 2022) (showing a unified Sudan).

[278] *Ratification Table: African Charter on Human and Peoples' Rights*, AFR. COMM'N HUM. & PEOPLES' RTS., https://www.achpr.org/ratificationtable?id=49 (last visited Sept. 4, 2022).

[279] Afr. Union, *List of Countries Which Have Signed, Ratified/Acceded to the African Charter on Human and People's Rights*, *supra* note 70.

[280] *See* INT'L JUST. RES. CTR., CIVIL SOCIETY ACCESS TO INTERNATIONAL OVERSIGHT BODIES: AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS, *supra* note 29, at 30.

[281] *See, e.g.*, INT'L JUST. RES. CTR., CIVIL SOCIETY ACCESS TO INTERNATIONAL OVERSIGHT BODIES: INTER-AMERICAN COMMISSION ON HUMAN RIGHTS, *supra* note 29, at 24, 41.

[282] *See id.*

[283] Recognition of this challenge can also be inferred from, *inter alia*, the IACHR's joint "roadmap" on coordination with the U.N. Committee on Enforced Disappearances, which commits both mechanisms to "[i]nstitutionalized information sharing" with regard to their outputs, secretariat staff, contacts, session dates, and other details. *See* Inter-Am. Comm'n H.R. & U.N. Human Rights Treaty Bodies, *Roadmap on the Coordination between the United Nations Committee on Enforced Disappearances and the Inter-American Commission on Human Rights* 4 (Dec. 16, 2021), https://www.oas.org/en/iachr/media_center/preleases/2021/Roadmap_CED_IACHR_ENG.pdf.

[284] *Compare The Secretariat*, ACERWC, https://www.acerwc.africa/the-secretariat/ (last visited Sept. 4, 2022) (listing personnel); *Commissioner for Human Rights, Who Is Who*, COUNCIL OF

cycles is often limited, particularly among regional mechanisms.[285] The ECtHR, for instance, indicates when each judge's term began, but not when it will end.[286] No human rights mechanism provides, or links to, information on upcoming member elections. For example, one needs to know to look for the African Union Executive Council's draft session agenda[287] to see whether it will elect ACHPR or AfCHPR members.

2. Website Organization and Functionality

The organization of human rights mechanisms' websites poses its own challenges. No two human rights body websites are alike, and many are not intuitive. For example, the date of ACHPR sessions that are more than a few weeks in the future can be found only in the "final communiqué" from the Commission's most recent session, and not in the text of its "Sessions" webpage.[288] The ACERWC's "Legal Instruments" webpage is blank, but its general comments can be found, in random order, under the tab "Our Work."[289] The United Nations Human Rights Committee and other treaty bodies share their most recent decisions on complaints at the bottom of the webpage for the session during which those decisions were adopted, and not in their "Jurisprudence

---

EUROPE, https://www.coe.int/en/web/commissioner/who-is-who (last visited Sept. 4, 2022) (listing personnel); *Staff*, INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/mandate/staff.asp (last visited Sept. 4, 2022) (listing personnel); *and Human Resources*, INTER-AM. CT. H.R., https://corteidh.or.cr/recursos_humanos.cfm (last visited Sept. 4, 2022) (not listing personnel); *with Structure*, AFR. COMM'N HUM. & PEOPLES' RTS., https://www.achpr.org/structure (last visited Sept. 4, 2022) (indicating that the ACHPR has a Secretary and Secretariat, but not identifying those individuals or other personnel). *See also Registrars & Deputy Registrars of the ECHR*, EUR. CT. H.R., https://www.echr.coe.int/Pages/home.aspx?p=court/registrars&c= (last visited Sept. 4, 2022) (identifying Registrar and Deputy Registrar, but no other personnel).

[285] *Cf. Elections of Treaty Body Members*, OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/EN/HRBodies/Pages/ElectionsofTreatyBodiesMembers.aspx (last visited Sept. 4, 2022); *Nomination, Selection and Appointment of Mandate Holders*, OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/EN/HRBodies/HRC/SP/Pages/Nominations.aspx (last visited Mar. 19, 2021) (providing detailed information and schedules on elections and composition).

[286] *See Composition of the Court*, EUR. CT. H.R., https://www.echr.coe.int/Pages/home.aspx?p=court/judges&c= (last visited Sept. 4, 2022) (this page does link to or provide additional information on the election process, generally).

[287] *See, e.g.*, Afr. Union, Executive Council, Draft Agenda: Thirty-Eight Ordinary Session, Feb. 3-4, 2021, https://au.int/sites/default/files/documents/39915-doc-ex_cl_draft_1_xxxviii_e.pdf.

[288] *See, e.g.*, Afr. Comm'n Hum. & Peoples' Rts., *Final Communiqué of the 69th Ordinary Session of the African Commission on Human and Peoples' Rights* ¶ 51 (Dec. 5, 2021) (identifying the dates and format for the Commission's next session, the 70th Ordinary Session), https://www.achpr.org/sessions/info?id=377.

[289] *Resources, Legal Instruments*, ACERWC, https://www.acerwc.africa/legal-instruments/ (last visited Sept. 4, 2022); *Our Work, General Comments*, ACERWC, https://www.acerwc.africa/general-comments/ (last visited Sept. 4, 2022).

database" or list of "Recent jurisprudence."[290] Such practices reduce the visibility and accessibility of the mechanisms' work.

3. Searchability

Most human rights mechanisms' websites have limited search tools, but they are an improvement over what existed a decade ago.[291] At one end of the spectrum are the COE's HUDOC databases, including for the ECtHR[292] and ECSR,[293] which are highly searchable and filterable and contain most official outputs. On the other end of the spectrum is the IACHR's website,[294] which until recently only included a general search bar and did not allow users to filter results. The IACHR website now allows users to "search" its decisions,[295] but—like the ACHPR's website—this function returns results based only on the names of cases and petitions, rather than the full textual content.

4. Document Formats and Linking

A separate but related concern is the formatting and searchability of individual documents. For instance, the AfCHPR, for many years, published scanned images of its judgments that were not machine-readable.[296] This means,

---

[290] For example, the views on complaints adopted by the Human Rights Committee at its October-November 2020 session, as of September 2022, were only listed on the 130 Session webpage (https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/SessionDetails1.aspx?SessionID=1375&Lang=en) but did not appear in the Jurisprudence Database (https://juris.ohchr.org/en/Search/Documents), which listed decisions from July 2020 and earlier.

[291] Users can conduct an advanced search of the ECtHR website, using full-text, title, or date fields, and filtering by type of document, webpage, State, and other criteria. *See Search*, EUR. CT. H.R., https://www.echr.coe.int/sites/search_eng/pages/search.aspx (last visited Sept. 4, 2022).

[292] *Eur. Ct. H.R.*, HUDOC, https://hudoc.echr.coe.int/eng# (last visited Sept. 4, 2022) (database of all published content, searchable in full-text and filterable by multiple criteria, including State involved, keyword, and judge).

[293] *European Social Charter*, HUDOC, https://hudoc.esc.coe.int/ (last visited Sept. 4, 2022) (including all complaints, decisions, and conclusions on State reports, as well as follow-up).

[294] *See* INTER-AM. COMM'N H.R., https://www.oas.org/en/iachr/default.asp (last visited Sept. 4, 2022) (see the search bar in the top right corner).

[295] Additionally, while in 2021 the IACHR announced, and linked to, a new searchable database of its decisions created and maintained by the Rule of Law Program for Latin America of the Konrad Adenauer Stiftung, the database is available in Spanish only and the scope of its contents are not clearly identified. *See* IUSLAT, https://www.iuslat.com/#search-advanced/content_type:2/* (last visited Sept. 4, 2022).

[296] *Compare* Mohamed Selemani Marwa v. Tanzania, App. No. 014/2016 (Afr. Ct. Hum. & Peoples' Rts. Dec. 2, 2021), https://www.african-court.org/cpmt/storage/app/uploads/public/61b/73f/214/61b73f214df12497608780.pdf (machine readable) *with* Michelot Yogogombaye v. Senegal, App. No. 001/2008 (Afr. Ct. Hum. & Peoples' Rts. Dec. 15, 2009), https://www.african-court.org/cpmt/storage/app/uploads/public/62a/c6b/570/62ac6b57004ca870862237.pdf (not machine readable).

among other consequences, that a reader cannot use the "Control+F" function to search through text. Other mechanisms upload some documents only in Word format,[297] meaning that any link directly downloads the document rather than displaying it in a browser window. Automatic downloads may make individuals uneasy because of the possibility that the document might be infected with a virus. Downloaded Word documents are also more cumbersome to access and share than links because the formatting may change (or be altered) and because they can only be disseminated via email or a file sharing tool. These additional steps in accessing or sharing a document also introduce opportunities for viruses or malware to spread.[298]

More broadly, few mechanisms hyperlink to materials referenced in their decisions and other outputs. A merits decision, for example, typically will not include a hyperlink to the preceding admissibility decision or to any of the precedents cited.[299] The lack of connectivity between documents can make it difficult or labor intensive to locate related decisions, particularly if the case name changes or the citation to a prior decision is incomplete.

5. Link Rot and Website Changes

As with all online content, human rights mechanisms' websites suffer from instances of link rot—when hyperlinks stop leading to the intended file or webpage because the content has been moved or taken down. Though sometimes a link to an external site stops working,[300] link rot is more often attributable to human rights mechanisms' practices. For example, in 2013, the OHCHR completed a new website but failed to ensure that links to its prior site would redirect to this new site. Instead, visitors to some prior pages are greeted with a

---

[297] For example, the IACHR's merits decisions from 2010 to 2013 download directly as Word documents, only, with no option to open the document in a web browser or download a PDF. *See generally Merits Reports*, INTER-AM. COMM'N H.R., http://www.oas.org/en/iachr/decisions/merits.asp (last visited Sept. 4, 2022).

[298] *See, e.g.*, *Protect yourself from macro viruses*, MICROSOFT, https://support.microsoft.com/en-us/office/protect-yourself-from-macro-viruses-a3f3576a-bfef-4d25-84dc-70d18bde5903 (last visited Sept. 4, 2022).

[299] *See, e.g.*, *Virgilio Maldonado Rodriguez v. United States of America*, Inter-Am. Comm'n H.R., Report No. 333/21, OEA/Ser.L/V/II, doc. 343 (2020), https://www.oas.org/en/iachr/decisions/2021/USPU12871EN.pdf.

[300] *See, e.g.*, *Human Rights Committee*, OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/en/treaty-bodies/ccpr (last visited Sept. 4, 2022) (see the External Links section in the right sidebar, featuring a link to "Amnesty International" that no longer works (http://web.amnesty.org/pages/treaty-countries-ai-eng)). *See also supra* note 8 (IACHR videos hosted by OAS no longer work).

404 message reading "File or directory not found"[301] or a 403 message saying "Forbidden: Access is denied."[302] Readers of the OHCHR brochure on United Nations human rights treaty bodies, which is still featured on the OHCHR website, receive a 404 message if they click on the links for more information.[303] While most links continue to work following the OHCHR's March 2022 website redesign, many files are no longer accessible, some pages no longer exist, and some links lead to error messages.[304] Regional mechanisms have also broken many links when launching new websites, leading to additional link rot.[305]

Other digital detritus includes abandoned social media accounts, like the OHCHR's former official Twitter handle @UNrightswire,[306] and channels that human rights mechanisms use inconsistently. For example, the IACtHR website links to its videos on both YouTube and Vimeo, but the former channel includes more recent videos than the latter.[307]

6. Erasure of History and Historical Documents

---

[301] The old site's address for Human Rights Council annual reports (https://www2.ohchr.org/english/bodies/hrcouncil/annual_reports.htm) leads to a 404 message. It should redirect here https://www.ohchr.org/EN/HRBodies/HRC/Pages/Documents.aspx.

[302] The old address for the Human Rights Council (http://www2.ohchr.org/english/bodies/hrcouncil/) leads to a 403 message.

[303] *See* Off. High Comm'r Hum. Rts., *The United Nations Human Rights Treaty System: Fact Sheet No. 30 (Rev. 1)* (2012), https://digitallibrary.un.org/record/735527?ln=en, p. 46 (linking to http://www2.ohchr.org/english/bodies/treaty/newsletter_treaty_bodies.htm). Following the March 2022 redesign of the OHCHR website, the former link to the Fact Sheet itself (https://www.ohchr.org/documents/publications/factsheet30rev1.pdf), which appears in the Google Search results for the publication name, also no longer works, leading instead to a page that says "The requested page could not be found."

[304] For example, as of September 2022, the prior link for the OHCHR webpage on the Human Rights Council (https://www.ohchr.org/EN/HRBodies/HRC/Pages/HRCIndex.aspx) now leads to a blank page with the words "Default title" and the page can be found at a different URL (https://www.ohchr.org/en/hrbodies/hrc/home). *See also* discussion *supra* notes 23, 87, and 140 (referring to links broken in the OHCHR's March 2022 website redesign).

[305] For example, the prior link to the advisory opinions page on the AfCHPR's website (http://www.african-court.org/en/index.php/cases/2016-10-17-16-19-35) now redirects to the new homepage (https://www.african-court.org/wpafc/). Additionally, the prior link to the host agreement between Tanzania and the AfCHPR (https://en.african-court.org/images/Protocol-Host%20Agrtmt/agreement-Tanzania%20and%20AU.pdf) is broken and returns an "Internal Server Error" message.

[306] *U.N. Human Rights, Twitter*, INTERNET ARCHIVE, https://web.archive.org/web/20130314210702/https://twitter.com/UNrightswire (Mar. 14, 2013). *See also* AfricanCommissionHPR, TWITTER, https://twitter.com/ACHPR (last used in December 2012; replaced by https://twitter.com/achpr_cadhp); IACHR, TWITTER, https://twitter.com/IACHumanRights (last used in December 2019); U.N. Human Rights LIVE, TWITTER, https://twitter.com/UNrightsLIVE (last used in November 2015).

[307] *Compare* Corte Interamericana de Derechos Humanos, YOUTUBE, https://www.youtube.com/channel/UCD1E1io4eeR0tk9k4r5CI9w/featured (showing hearings from the August 2022 session and other videos) *with* Corte IDH, VIMEO, https://vimeo.com/corteidh (most recent video is from June 2021).

In addition to failing to redirect or update online content, some human rights mechanisms have a tendency to post content in temporary, ephemeral ways, thus erasing their own history, complicating research, and obscuring practical details that are useful to advocates. This happens when mechanisms delete content or links, such as when the AfCHPR issued new Rules of Court and removed links to the old Rules, leaving litigants in the dark as to what the prior rules said.[308]

The OHCHR, in particular, does this with time-specific information, such as the logistics of country visits and sessions. For example, prior to her visit to Canada in 2018, the United Nations Special Rapporteur on violence against women issued a call for inputs[309] in which she identified her key areas of focus. Such calls are not linked to any webpage or publication,[310] and they are undated, not given United Nations document numbers, and excluded from the online archives, so they are only discoverable by those who already have the link or know to look for them.[311]

7. Accessibility for Persons with disabilities

While some intergovernmental organizations have implemented design criteria[312] to facilitate use of their websites by persons with disabilities, most human rights mechanisms have not.[313] In 2016, the United Nations Special

---

[308] *Basic Documents*, AFR. CT. HUM. PEOPLES' RTS., https://www.african-court.org/wpafc/documents/ (last visited Sept. 4, 2022) (listing only the 2020 Rules and not the prior version).

[309] *Call for submission – Visit to Canada, April 2018*, INTERNET ARCHIVE, https://web.archive.org/web/20180514021850/http://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/VisitCanada.aspx (May 14, 2018). Following the March 2022 redesign of the OHCHR website, the link to this call (https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/VisitCanada.aspx) no longer works.

[310] *Cf.* Press Release, Off. High Comm'r Hum. Rts., *UN Expert on Violence against Women to Visit Canada* (Apr. 9, 2018), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22929&LangID=E; *SR Women, Country Visits*, OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/en/special-procedures/sr-violence-against-women/country-visits.

[311] *See Official Document System, Help*, U.N., https://documents.un.org/prod/ods.nsf/xpHelp.xsp (last visited Sept. 4, 2022) (explaining that the Official Document System does not include "unsymbolled documents").

[312] *See Accessibility Guidelines for UN Websites*, U.N., https://www.un.org/en/webaccessibility/index.shtml (last visited Sept. 4, 2022); *Accessibility*, Council of Europe, https://juris.ohchr.org/en/About/accessibility/ (last visited Sept. 4, 2022).

[313] The OHCHR Jurisprudence Database includes a link marked "accessibility" which leads to a page noting that "this website was developed and is maintained using World Wide Web Consortium (W3C) guidelines for accessibility" and invites users to contact OHCHR for more information or assistance. *Jurisprudence: Accessibility*, OFF. HIGH COMM'R HUM. RTS., https://juris.ohchr.org/en/About/accessibility/ (last visited Sept. 4, 2021). For an explanation of website accessibility and relevant standards, *see* Catherine Eastern, *Revisiting the Law on Website Accessibility in Light of the UK's Equality Act 2010 and the United Nations Convention on the Rights of Persons with Disabilities*, 20 INT. J. L. & TECH. 1 (2012), 19-47.

Rapporteur on the rights of persons with disabilities noted the widespread failure to make information accessible in practice: "Generally, decision-making bodies and mechanisms neither produce nor disseminate information in accessible formats (such as easy-to-read), nor do they ensure the availability of sign language interpretation, guide interpreters for deafblind persons, or captioning during public debates."[314] The Special Rapporteur also noted that the participation of persons with disabilities depends on "the availability of procedures and information in accessible formats" and accordingly urged the United Nations and regional bodies to "increase efforts in this regard."[315] So far, unfortunately, no human rights mechanism appears to have heeded her call.

8. Translations

Regardless of their language policies, all mechanisms favor a language and that language is almost always English.[316] For example, among United Nations human rights treaty bodies, recent documentation is often available only in English.[317] Additionally, the IACHR, which operates primarily in Spanish, typically translates into Portuguese only its decisions regarding Brazil.[318] Similarly, the AfCHPR only rarely publishes Portuguese or Arabic versions of its judgments.[319] In some instances, human rights mechanisms have ordered States to translate human rights decisions into Indigenous or minority languages, but then do not publish those translations on their own websites.[320]

---

[314] Catalina Devandas Aguilar, *supra* note 234, ¶ 76.
[315] *Id*. at ¶ 93.
[316] For example, as of September 4, 2021, the ECtHR's database contained 9,520 press releases in English and 7,396 in French. *See European Court of Human Rights: Press*, HUDOC, https://hudoc.echr.coe.int/eng-press#%20 (last visited Sept. 4, 2021).
[317] *See, e.g.*, *CERD - International Convention on the Elimination of All Forms of Racial Discrimination, 107 Session (08 Aug 2022 – 30 Aug 2022)*, OFF. HIGH COMM'R HUM. RTS., https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/SessionDetails1.aspx?SessionID=2556&Lang=en (last visited Sept. 4, 2022) (listing session document links, which mostly show only English-language versions when opened).
[318] *See Informes de Admissibilidade: 2019*, INTER-AM. COMM'N H.R., http://www.oas.org/pt/cidh/decisiones/admisibilidades.asp?Year=2019 (last visited Sept. 4, 2021).
[319] *See generally*, *AFCHPR Cases: Finalised Cases*, AFR. COMM'N HUM. & PEOPLES' RTS., https://www.african-court.org/cpmt/finalised (last visited Sept. 4, 2021) (with English, French, Portuguese, and Arabic interfaces, although documents are not all available in those languages).
[320] *See, e.g.*, *Garífuna Punta Piedra Community and Its Members v. Honduras*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 304 (Oct. 8, 2015), http://www.corteidh.or.cr/docs/casos/articulos/seriec_304_esp.pdf.

Online Publication of Certain Documents and Information, as April 2021

Entity	Instruments	Ratifications	Decisions & Opinions	Announcement of Decisions	Complaints & Briefs	Other Inputs ○	Translation of Outputs	Search *	Sessions & Opportunities	Recordings	Election Details △	Term Dates □	Staff & Titles
UN	✓	✓	-	-	-	-	-	○	✓	✓	○	○	✗
OHCHR	✓	○	-	-	-	✓	○	○	✓	✗	✗	✗	✗
CAT	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
CED	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
CEDAW	✓	○	✓	○	✗	✓	○	○	○	✓	✓	✓	✗
CERD	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
CESCR	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
CMW	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
CRC	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
CRPD	✓	○	✓	○	✗	✓	○	○	○	✓	✓	○	✗
HRC	✓	○	✓	○	✗	✓	○	○	○	✓	✓	✓	✗
SPs	✓	-	○	✗	✗	○	○	○	○	✗	✓	○	✗
AU	✓	○	-	-	-	-	○	✗	○	○	○	○	✗
ACERWC	✓	✓	✓	✗	✗	✗	○	✗	○	✗	✗	○	✓
ACHPR	✓	○	○	✗	✗	✗	○	○	○	○	✗	✗	✗
AfCHPR	✓	✓	✓	✓	✗	-	○	✗	○	○	✗	○	✗
OAS	✓	✓	-	-	-	-	○	○	✓	✓	✗	✗	✓
IACHR	✓	○	✓	○	✗	✗	○	○	○	○	✗	✓	○
IACtHR	✓	○	✓	✓	○	-	○	✗	✓	○	✗	✗	✗
COE	✓	✓	-	-	-	-	○	○	✓	○	✗	✗	✓
Comm'r	✓	-	-	-	-	-	○	✗	✗	○	✗	○	✓
ECSR	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	○	✗
ECtHR	✓	○	✓	○	✗	-	○	✓	✓	○	✗	✗	✗

○ Inconsistently available or incomplete.
- Not applicable.
○ Refers to submissions by civil society, including for purposes of State reviews, thematic reports, or country visits.
* Indicates existence of a searchable database or other tool for finding particular documents, beyond a basic search bar on the website.
△ Refers to information on the timing, process, and candidates in the election of human rights bodies' members or intergovernmental organization's secretary, on the entity's own website.
□ Where current and former term dates (start and end) are readily available.

D. Assessment of Human Rights Mechanisms' Practices

How do the access-to-information policies and practices of human rights mechanisms stack up against international norms? The answer: very poorly. Human rights mechanisms' information falls within the scope of access-to-information standards. Multiple national and international interpretations expressly require the disclosure of information on human rights violations and investigations (or, rather, prohibit exceptions to disclosure of such information).[321] Moreover, the United Nations Human Rights Committee and other entities have specified that individuals have a right of access to information with respect to any public body, including intergovernmental organizations.[322] Even the ECtHR's more limited understanding of the right of access to information extends to civil society organizations seeking information for the purposes of advocating for human rights. However, while IGOs and human rights mechanisms do share considerable information online, they fail to satisfy the most fundamental components of access to information, which include having an established policy and process.

Yet even adherence to international standards might not be enough. Or perhaps a discussion focused on the legal application of those standards "misses the most salient points."[323] After all, human rights mechanisms are only as effective as they are accessible; human rights advocates can only hold governments accountable to those standards, or via those mechanisms, that they know of and understand. Moreover, transparency is an essential component of trust. Individuals would not be expected to put their faith in national courts whose members are selected in secret, nor would they be eager to solicit the help of a national human rights institution that does not operate in some of the major languages of its jurisdiction. Generally speaking, people cannot just show up at the doorstep of a human rights body to find out who to talk to or to request the

---

[321] *See, e.g.*, OAS, Inter-American Model Law 2.0 on Access to Public Information, art. 27, https://www.oas.org/en/sla/dil/docs/publication_Inter-American_Model_Law_2_0_on_Access_to_Public_Information.pdf. *See also Country Data*, GLOBAL RIGHT TO INFORMATION RATING, *supra* note 247 and national laws of Bangladesh, Guatemala, India, Kenya, Tunisia, and Uruguay cited therein.

[322] *See, e.g.*, U.N. Hum. Rts. Comm., General Comment No. 34, *supra* note 73, ¶ 7; UNESCO, Brisbane Declaration: Freedom of Information – The Right to Know (2010); OFF. HIGH COMM'R HUM. RTS., *Factsheet: Access to Information*, *supra* note 223 (stating, "The right of access to information equally applies within and towards international organizations, such as the United Nations"). *Contrast* Alan Boyle & Kasey McCall-Smith, *Transparency in International Law-making*, *in* TRANSPARENCY IN INTERNATIONAL LAW 419–35, 434-35 (Andrea Bianchi & Anne Peters eds., 2013) (arguing "it is doubtful whether the principle of access to information has any direct application to international organizations or treaty bodies: they may choose to make a great deal of information available, but there is only a limited basis for compelling them to do so").

[323] David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *supra* note 211, ¶ 18.

information they need. The headquarters in Geneva, Banjul, Washington, and Strasbourg are thousands of miles from many of the people whose rights they protect and even for those who make the journey, a contact, an appointment, and identification are likely to be required. In their online presence, then, human rights mechanisms should meet a higher standard of transparency, whether or not required by international law. Their legitimacy depends on it.

E. Benefits and Challenges of Outside Resources and Tools

Given the gaps in access to human rights mechanisms' information, third parties have stepped in to fill the void.[324] Academic institutions, non-governmental organizations, governments, and others have built databases of different categories of human rights documents, with a particular focus on case law. Some databases, such as African Human Rights Case Law Analyser[325] and WorldCourts,[326] upload machine-readable versions of international courts' and human rights mechanisms' decisions and make them searchable and filterable using multiple criteria. Others, such as the Columbia Global Freedom of Expression Case Law database[327] and ESCR-Net Caselaw Database[328] offer a searchable collection of summaries of select significant decisions from international (and national) bodies, along with links to the primary documents. Some other databases include resolutions, general comments, policy documents, and other outputs from intergovernmental and human rights mechanisms, often in connection with a particular theme.[329]

These databases vastly improve access to human rights mechanisms' documents and have pushed forward the free-access-to-law movement[330] more broadly, setting new standards for transparency, accessibility, and user

---

[324] The author is on the board of Human Rights Information and Documentation Systems (HURIDOCS), one of the organizations building libraries of human rights legal documents.
[325] *See* AFRICAN HUMAN RIGHTS CASE LAW ANALYSER, http://caselaw.ihrda.org/.
[326] *See* WORLDCOURTS, http://worldcourts.com/.
[327] *See Global Freedom of Expression: Case Law*, COLUMBIA UNIVERSITY, https://globalfreedomofexpression.columbia.edu/cases/.
[328] *See Caselaw Database*, ESCR-NET, https://www.escr-net.org/caselaw.
[329] *See, e.g.*, RIGHTDOCS, https://www.right-docs.org/ (containing Human Rights Council resolutions and reports to the Council, including by special procedure mandate holders); *Girls' Rights Platform*, PLAN INTERNATIONAL, https://database.girlsrightsplatform.org/en/library (containing a multitude of U.N. and regional documents on girls' rights under international law); REFWORLD, https://www.refworld.org/cgi-bin/texis/vtx/rwmain (containing documentation related to country conditions and international law and policy documents related to refugee rights).
[330] In this regard, an enormous debt is owed to the Legal Information Institutes, which also increasingly provide access to international caselaw. For a brief history of the LIIs and free access to law movement, *see* Graham Greenleaf, Philip Chung & Andrew Mowbray, *UPDATE: Legal Information Institutes and the Free Access to Law Movement* (Feb. 2018), GLOBALEX, https://www.nyulawglobal.org/globalex/Legal_Information_Institutes1.html.

experience. Some of the key innovations of these tools are greater visibility of (and user interaction with) metadata: displaying the relationships between documents, hyperlinking references in the text, and using machine learning applications to improve online searching. However, external databases often have their own limitations in terms of scope, timeliness, language versions, and search functionality.

External databases raise fundamental questions. One key concern is whether these databases provide an excuse for intergovernmental organizations and human rights mechanisms to shirk their information management responsibilities. Another is what standards, if any, external databases must adhere to regarding transparency and timeliness. Given precarious funding, whether and how their work can be sustained in perpetuity is another open question. External databases pose a threat to human rights mechanisms in terms of how the public views the authenticity or authoritativeness of their versions of documents. They contribute to the fragmentation or siloing of geographic and thematic areas of human rights law. While it seems likely that third parties will always have an interest in curating particular document collections—for example, by theme from across multiple systems—it is less clear that external databases should be *necessary* in order to provide fundamental public access to human rights mechanisms' documents. After all, if the public has a right of access to this information, then human rights mechanisms have a duty to provide it.

VII. CONCLUSION: MOVING FROM LACUNA TO LEADERSHIP

For as long as governments choose to support them, human rights accountability mechanisms will remain vital for the elucidation, documentation, codification, and vindication of individuals' and groups' fundamental rights. These mechanisms must be built to last. Decades into the digital era, human rights mechanisms are alarmingly behind the times. How might they catch up?

First, human rights mechanisms would do well to keep Erika, and her dilemma, at the center of their approach. Advocates' information needs fit into a broader discussion related to human-centered design,[331] victim-focused

[331] *See, e.g.*, Margaret Hagan, *A Human-Centered Design Approach to Access to Justice: Generating New Prototypes and Hypotheses for Interventions to Make Courts User-Friendly*, 6 IND. J.L. & SOC. EQUAL. 199 (2018).

approaches to advocacy and reparation,[332] and procedural justice.[333] While each mechanism's relationship with the public is distinct, the image that stays with me is of the ACHPR's sessions, where civil society is relegated to the back of the room, with less comfortable chairs, fewer microphones, shorter speaking times, and the occasional admonishment to be a bit less demanding and a bit more appreciative.[334] Those seeking accountability for human rights abuses are not peripheral or incidental to the oversight mechanisms' missions; they are at the core.

Moreover, human rights mechanisms—or, more specifically, their parent IGOs—are likely bound by customary international norms to protect individuals' data privacy and freedom of information. Explicitly recognizing that the public is entitled to access information and communicate with human rights mechanisms without unnecessarily risking their safety or privacy could change the current dynamic and frame policy development for the better. As first steps, mechanisms could conduct an objective assessment of their public-facing digital security vulnerabilities and information management practices and survey users regarding their information and digital security needs.

Second, human rights mechanisms should look to available examples of good information management practices. Newspapers like *The Guardian* have long advised would-be whistleblowers on how to confidentially or anonymously communicate with them, and they provide the digital channels to do so using widely available technology.[335] The European Union and its Court of Justice[336] demonstrate how an intergovernmental organization can handle data privacy[337] and operate in multiple languages[338] with transparency. For its part, the

---

[332] *See, e.g.,* Sarah Knuckey et. al., *Power in Human Rights Advocate and Rightsholder Relationships: Critiques, Reforms, and Challenges*, 33 HARV. HUM. RTS. J. 1 (2020). *See also* Thomas M. Antkowiak, *An Emerging Mandate for International Courts: Victim-Centered Remedies and Restorative Justice*, 47 STAN. J. INT'L L. 279 (2011).

[333] *See, e.g.,* Eric Stover, Mychelle Balthazard & K. Alexa Koenig, *Confronting Duch: Civil Party Participation in Case 001 at the Extraordinary Chambers in the Courts of Cambodia*, 93 INT'L REV. RED CROSS 503, 531-33 (2011).

[334] *See* INT´L JUST. RES. CTR., CIVIL SOCIETY ACCESS TO INTERNATIONAL OVERSIGHT BODIES AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS, *supra* note 29, at 23.

[335] *See How to Contact the Guardian Securely,* GUARDIAN, https://www.theguardian.com/help/ng-interactive/2017/mar/17/contact-the-guardian-securely (last visited Sept. 4, 2022). *See also*, *How to Contact the Guardian and Observer*, GUARDIAN, https://www.theguardian.com/help/contact-us (last visited Sept. 4, 2022); *Privacy*, GUARDIAN, https://www.theguardian.com/info/privacy (last visited Sept. 4, 2022); *Cookie Policy*, GUARDIAN, https://www.theguardian.com/info/cookies (last visited Sept. 4, 2022).

[336] *See The Institution: Protection of Personal Data*, CT. JUST. EUR. UNION, https://curia.europa.eu/jcms/jcms/p1_2699100#protection_donnees_juridictionelles (last visited Sept. 4, 2022).

[337] *See Privacy Policy*, EUR. UNION, https://europa.eu/european-union/abouteuropa/privacy-policy_en (last visited Sept. 4, 2022).

[338] *See Languages on our websites*, EUR. UNION, https://europa.eu/european-union/abouteuropa/language-policy_en (last visited Sept. 4, 2022).

Organization of American States' access-to-information policy is straightforward and easily replicable.[339] Furthermore, human rights mechanisms' own statements and interpretations provide ample guidance on individuals' right to access public information.

Human rights mechanisms can also learn much from their peers in making their work more accessible and transparent beyond what may be required by international human rights law. While the Council of Europe human rights mechanisms showcase the premier document databases, the ACERWC goes further in transparency by sharing its staff list, and the OHCHR is far ahead of the curve in providing advanced, detailed information on treaty bodies' elections. The IACHR's nascent User Support Section is a welcome development that other mechanisms could emulate. As they consider the needs of individuals with disabilities, mechanisms should follow the lead of the United Nations Special Rapporteur on the rights of persons with disabilities and the Committee on the Rights of Persons with Disabilities.

Third, human rights mechanisms must marshal additional human and financial resources to develop new policies, efficiently handle requests related to data protection and information, implement new technology, and increase translation, among other necessary tasks. Most human rights mechanisms are chronically and critically underfunded. For example, in 2021, the OHCHR missed the deadline to submit its Human Rights Council-mandated report on access-to-information standards because of "ongoing financial constraints."[340] Such constraints cannot be the excuse for improperly managing the information that is their lifeblood. Human rights mechanisms should specifically request funding for improved public-facing information management.

Member States may be receptive to the idea that human rights mechanisms need to keep pace, given how many of them have adopted data protection and freedom of information legislation. There are also signs that some funders are eager to help bring human rights mechanisms fully into the digital age. This is exemplified by Microsoft's partnership with the OHCHR and Google's funding to the IACHR.[341] States that already provide significant financial support, such as the United States, might be persuaded to see the wisdom and economic

---

[339] *See Frequently Asked Questions on Access to Information*, OAS, http://www.oas.org/airf/access_to_information_faq.aspx (last visited Sept. 4, 2022).

[340] U.N. Hum. Rts. Council, Freedom of Opinion and Expression: Report of the United Nations High Commissioner for Human Rights – Note by the Secretariat, U.N. Doc. A/HRC/47/48 (May 18, 2021), https://undocs.org/A/HRC/47/48.

[341] *See Technology for Human Rights: UN Human Rights Office Announces Landmark Partnership with Microsoft*, OFF. HIGH COMM´R HUM. RTS. (May 16, 2017), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21620&LangID=E; INTER-AM. COMM'N HUM. RTS., *Ch. VI: Institutional Development*, *in* ANNUAL REPORT 2020, 1109, https://www.oas.org/en/iachr/docs/annual/2020/Chapters/IA2020cap.6-en.pdf.

logic of helping safeguard human rights mechanisms' integrity in the face of hacking and its consequences such as diminished public confidence. Once implemented, increased transparency and security could also help expand human rights mechanisms' visibility and, in turn, public support.

Fourth, human rights mechanisms should develop, adopt, and implement policies on access to information and on users' digital security and privacy. These policies must, at minimum, satisfy customary international norms. From a moral and common-sense perspective, the relevant policies should also meet or exceed the recommendations human rights mechanisms have made to States based on their treaty obligations. In formulating their policies, mechanisms should solicit and incorporate public input, as discussed above. Upon adoption, these documents must be readily available online, along with information on the associated processes. Consistent implementation is critically important. For example, when budget cuts or unforeseen circumstances prevent or delay full adherence to a policy—such as with regard to translation—mechanisms should quickly and clearly inform the public.

Finally, in policy and practice, human rights mechanisms should implement internal safeguards and accountability measures for when lapses or breaches occur. For example, each institution should have a designated data protection officer to oversee internal compliance with its data protection policy. The European Commission provides a useful model. Human rights mechanisms should also include statistics on information requests, for example, in their annual reports. In a break with current practice, they should also proactively and publicly report hacking attempts and other illicit interceptions and directly inform the affected individuals.

As with any violation of an individual's human rights, a remedy must be available when a mechanism manages information in a way that contravenes human rights standards. This remedy could take many forms, although challenges include the lack of an existing, separate judicial institution to hear such claims, and the fact that human rights mechanisms' digital infrastructure is often intertwined with that of their parent IGOs. A possible model is available in the European Union, where individuals may file complaints with the European Court of Justice concerning the EU's handling of their data.[342] Perhaps IGOs' administrative tribunals or other supranational courts, such as the Court of Justice of the Economic Community of West African States, could be expanded to process complaints by the public against human rights mechanisms. These are

[342] *See* Parliament & Council Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 2018 OJ (L 295) 39-98, arts. 63, 64, https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

complicated questions. Prior efforts to hold IGOs accountable for human rights violations also demonstrate institutional resistance to judicial oversight. Nonetheless, they are questions worthy of discussion and resolution.

Technological advances mean we cannot quite know what the future holds. Will quantum computing render encryption useless? Will external search tools using artificial intelligence reduce the importance of, or the need for, human rights mechanisms' own document databases? Only time will tell. Meanwhile, human rights mechanisms can be better prepared for the future by maintaining an open dialogue with their constituents about their needs and vulnerabilities, by implementing policies tied to fundamental principles rather than particular technologies, by advocating for adequate resources, and—perhaps most importantly—by taking accountability for information transparency and security.