



Protecting & Promoting Digital Rights in Africa

A Toolkit for National Human Rights Institutions

ICNL

INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

October 2024



TABLE OF CONTENTS

Section 1: An Overview of Digital Rights for NHRIs

1.1. What are Digital Rights?	1
1.2. The Purpose of this Toolkit	2
1.3. International and Regional Norms	2
1.4. The Important Role of NHRIs in Promoting and Protecting Digital Rights	6
1.5. How is Digital Rights Monitoring Different from Traditional Human Rights Monitoring?	7

Section 2: Governance of the Internet & Digital Technologies

2.1. The Actors Responsible for Internet Governance	13
2.2. Types of Laws and Regulations that Impact Digital Rights	15

Section 3: Examples of Digital Rights Violations

3.1. Network Disruptions	20
3.2. Vague or Disproportionate Online Content Restrictions	24
3.3. Untargeted or Invasive Digital Surveillance	28

Acknowledgements

34



SECTION 1

An Overview of Digital Rights for NHRIs

1.1 What are Digital Rights?

THE SAME RIGHTS THAT PEOPLE HAVE OFFLINE MUST ALSO BE PROTECTED ONLINE.

The United Nations Human Rights Council

A/HRC/RES/20/8, 5 July 2012, at 2, para. 1

Digital rights are an extension of the rights set out in the Universal Declaration of Human Rights. The same rights that have always been fundamental – such as freedom of expression, privacy, and access to information – are also protected in the era of the Internet, social media, and technology.

Digital technologies have opened new avenues for expressing ideas and exchanging information, yet digitalization has also enabled abuses and violations of rights. Whether intentionally or out of ignorance, driven by commercial interests or the desire to exert control, various actors – states, corporations, politicians, and tech developers – may perpetrate harms that impact fundamental freedoms. Human rights actors and justice institutions need to understand the means of abuse and how best to document and assess alleged violations in order to protect and promote digital rights.

1.2 The Purpose of this Toolkit

The goal of this Toolkit is to provide National Human Rights Institutes (NHRIs) in Africa with practical information that will assist them to better document, analyze, and report on digital rights topics in their countries. The Toolkit presents NHRIs with an introductory primer on the most salient digital rights topics, such as network disruptions, surveillance, and online content restrictions. It also provides links to additional resources from United Nations (UN) human rights mechanisms, the African Commission on Human and Peoples' Rights (ACHPR), and digital rights organizations to help Commissioners explore the topic deeper as they develop their strategies and methodologies for incorporating digital rights protection and promotion into their work, including when they are monitoring violations. The Toolkit seeks to answer the following questions:

- »»» What are digital rights and how is digital rights monitoring different from traditional human rights monitoring?
- »»» What is the role of NHRIs in promoting and protecting digital rights?
- »»» What are the types of laws that impact rights online and who are the actors involved in making decisions about the Internet?
- »»» What are the key considerations when NHRIs address specific types of digital rights issues, such as intentional network disruptions?
- »»» What are the data sources and key civil society initiatives that NHRIs can utilize when engaging in digital rights promotion and protection?

The Toolkit does not provide an exhaustive list of digital rights topics. It is designed as a starting point for NHRIs to understand these complex issues and connect with the digital rights community. Commissioners are encouraged to delve deeper into the sections and topics that are most relevant to their work. We hope this content enables NHRIs to jumpstart their engagement in digital rights promotion and protection.

1.3 International & Regional Norms

In 2012, the UN Human Rights Council **affirmed** that human rights in the digital realm must be protected and promoted to the same extent and with the same commitment as human rights in the physical world. Since then, standards and norms have been developed that interpret how these rights apply in the context of the Internet, online surveillance, social media, artificial intelligence (AI), and other technologies.



The following are key UN documents related to digital rights.

UN Treaty Body Comments

Committee on Economic, Social and Cultural Rights, E/C.12/GC/25 (Apr. 2020)	General Comment No. 25 interprets Article 15 of the International Covenant on Economic, Social, and Cultural Rights. It states that emerging digital technologies may enhance the enjoyment of economic, social, and cultural rights, but calls on States to put in place policies to ensure that these technologies do not “intensify social inequalities” or “reinforce discrimination.”
Human Rights Committee, General Comment 16 (Apr. 1988)	General Comment 16 stipulates that Article 17 of the International Covenant on Civil and Political Rights (ICCPR) not only prevents States from violating the right to privacy, but also requires States to institute a legal framework to prohibit violation of privacy by non-state actors. Such laws must give individuals the right to know “what personal data is stored in automatic data files, and for what purposes,” and “which public authorities or private individuals or bodies control or may control their files.” Individuals should also have the right to request correction of incorrect data and the elimination of the data altogether.
Human Rights Committee, CCPR/C/GC/34 (Sept. 2011)	General Comment 34 interprets Article 19 of the ICCPR. It not only sets forth the narrow circumstances in which the right to freedom of expression can be restricted by States, it recognizes the Internet as an important means for exercising this right. In the context of journalism, it calls on States to take steps to foster the independence of “new media,” to ensure that restrictions on websites, blogs, and other Internet-based media are compatible with Article 19, and to abolish general licensing and registration systems for bloggers and other Internet-based publications as these are incompatible with Article 19.
Committee on the Rights of the Child, CRC/C/GC/25 (Mar. 2021)	General Comment 25 interprets the Convention on the Rights of the Child in relation to the digital environment, including in the context of the rights to privacy, non-discrimination, education, protection, and play. It identifies the risks to children online and tasks States with addressing the risks through education campaigns and by ensuring that businesses comply with their responsibilities under the law. It also explains that the Internet is a crucial space for children to express themselves and to advocate for their rights.

UN General Assembly Resolutions

A/RES/68/167 (Dec. 2013); A/RES/73/179 (Dec. 2018); A/RES/75/176 (Dec. 2020); A/RES/77/211 (Dec. 2023)	Right to Privacy in the Digital Age: The General Assembly has passed several resolutions on the right to privacy in the digital age. Recent iterations of the resolution cover topics like biometrics, AI, the right to non-discrimination (e.g., in the context of police surveillance of minority communities), the importance of encryption and anonymity tools, specific challenges to privacy related to the Covid-19 pandemic, virtual reality technologies, data protection regulations, and the right to effective remedy for victims of unlawful or arbitrary surveillance.
A/C.3/78/L.19/Rev.1 (Nov. 2023)	Children’s Rights in the Digital Environment: The Resolution calls on States to put in place strong national legal frameworks on data protection and privacy and ensure that companies fulfill their due diligence responsibilities to protect children’s rights, prioritize their best interests, and prevent risks that may arise from the design and conception of their products and services. States are also asked to set aside adequate resources to fully realize children’s rights in the digital environment.

<u>A/RES/78/132</u> (Dec. 2023)	Information and Communication Technologies (ICTs) for Sustainable Development: The General Assembly has adopted over a dozen resolutions on the ways in which ICTs can contribute to the Sustainable Development Goals. Stemming from the World Summit on the Information Society 2003 Plan of Action, the resolutions call on States to address the digital divide and recognizes that ICTs can play a role in the realization of human rights and fundamental freedoms.
<u>A/RES/78/265</u> (Mar. 2024)	Artificial Intelligence (AI): This non-binding resolution was co-sponsored by 125 States and represents the first General Assembly resolution specifically addressing AI. The Resolution acknowledges the potential for AI to contribute to the Sustainable Development Goals; promotes the adoption of frameworks to ensure that AI systems are safe, secure, and trustworthy; and calls on States to support developing countries to close digital divides so they can effectively adopt AI technologies.

UN Human Rights Council (HRC) Resolutions

<u>A/HRC/RES/20/8</u> (Jul. 2012); <u>A/HRC/RES/26/13</u> (Jun. 2014); <u>A/HRC/RES/32/13</u> (Jul. 2016); <u>A/HRC/RES/38/7</u> (Jul. 2018); <u>A/HRC/RES/47/16</u> (Jul. 2021)	The Promotion, Protection, and Enjoyment of Human Rights on the Internet: This series of five resolutions covers a variety of issues including the digital divide, Internet shutdowns, net neutrality, online gender-based violence, and encryption. Since adopting the first Resolution in 2012, the HRC has affirmed “that the same rights people have offline must also be protected online.” Most recently, the 2021 Resolution recognized the important role of the Internet in the context of the Covid-19 pandemic and called upon all stakeholders in the ICT sector to fully consider the human rights, health, and socio-economic impacts of the pandemic.
<u>A/HRC/RES/28/16</u> (Apr. 2015); <u>A/HRC/RES/42/15</u> (Oct. 2019); <u>A/HRC/RES/48/4</u> (Oct. 2021)	The Right to Privacy in the Digital Age: The HRC has also adopted a series of resolutions on privacy rights. The 2015 Resolution created a mandate for a Special Rapporteur on the right to privacy, and subsequent resolutions extended this mandate. Recent resolutions have expressed concern that States and businesses increasingly use advanced technologies, like AI, to track and analyze people’s communications and behavior outside of the law.
<u>A/HRC/RES/38/5</u> (Jul. 2018)	Violence Against Women and Girls: The Resolution condemns tech-facilitated gender-based violence and the ways in which it restricts the ability of women and girls to exercise their right to freedom of expression. It also credits encryption and anonymity tools with enabling women and girls to safely navigate digital spaces.

The following are key resolutions in the African system related to digital rights.



African Union (AU) Documents

<u>Convention on Cyber Security and Personal Data Protection (Malabo Convention)</u>	The Malabo Convention addresses cybercrime and personal data protection. It lists model provisions relating to attacks on computer systems, breaches of computer data, content prohibitions, and electronic message security measures. It also sets out several rights for data subjects, including the right to information, the right of access, the right to object, and the right to be forgotten.
--	--

<u>Interoperability Framework for Digital Identification</u>	The 2024 Framework promotes the idea of an interoperable digital identification (ID) system in Africa and addresses challenges, including exclusion of marginalized groups, weak cybersecurity systems, the need for personal data protection, public distrust in institutions, inadequate technical and financial capacities, the shortage of data storage facilities, and a lack of appropriate governance to securely and effectively deploy digital ID. While the Framework states that digital ID helps citizens access their rights, it does not discuss the inherent human rights risks related to digital ID systems.
<u>Continental AI Strategy for Africa</u>	In February 2024, the African Union Development Agency (AUDA-NEPAD) published the AUDA-NEPAD Continental Strategy for Africa and a white paper on <i>Regulation and Responsible Adoption of AI in Africa Towards Achievement of AU Agenda 2063</i> . The last section of the Strategy provides a strategic framework roadmap for African countries to develop, adopt, and utilize AI technologies. It also provides guidance and recommendations for African countries on how to harness the potential of AI responsibly and sustainably. The roadmap was endorsed in June 2024 by the AU Council of Ministers.
<u>African Digital Compact</u>	The Compact builds off <u>Agenda 2063</u> and the <u>AU Digital Transformation Strategy</u> to propose commitments that will enable States to harness the “potential of digital technologies to foster sustainable development, economic growth, and societal well-being throughout Africa.” It also serves as the AU’s positions on a similar international initiative, the Global Digital Compact, spearheaded by the UN Secretary General.

African Commission on Human and Peoples’ Rights (ACHPR) Resolutions

<u>ACHPR/Res.362</u> (Nov. 2016)	Freedom of Information and Expression: Resolution 362 calls on countries to guarantee, respect, and protect citizens’ right to freedom of information and expression through Internet access. In 2019, the Commission adopted <u>“The Declaration of Principles of Freedom of Expression and Access to Information in Africa,”</u> which highlights 43 principles that address universal access to the Internet, intermediary liability, privacy protections, communication surveillance, and the rights of individuals to express themselves freely online.
<u>ACHPR/Res.573</u> (Nov. 2023)	Mass and Unlawful Targeted Communication Surveillance: Resolution 573 calls for States to refrain from deploying targeted mass communications surveillance to attack vulnerable groups such as human rights defenders and the media and to ensure all restrictions to the right to privacy are necessary and proportionate.
<u>ACHPR/Res. 522</u> (Aug. 2022)	Protection of Women Against Digital Violence: Resolution 522 calls on States to adopt or review legislation to combat digital violence against women and facilitate women’s access to education in digital technology domains.
<u>ACHPR.Res.580</u> (Mar. 2024)	Internet Shutdowns and Elections in Africa: Resolution 580 calls for States to refrain from ordering the interruption of telecommunications services, shutting down the Internet, and/or disrupting access to any other digital communication platforms before, during, or after elections.
<u>ACHPR/Res.473</u> (Feb. 2021)	Artificial Intelligence: Resolution 473 recognizes that AI and other new and emerging technologies present both opportunities and perils for the promotion and protection of human and peoples’ rights and calls for a study on AI, robotics, and other new and emerging technologies and their implications on rights in Africa.

1.4 The Important Role of NHRIs in Promoting and Protecting Digital Rights

According to the [UN Paris Principles](#), NHRIs have two areas of responsibilities: human rights promotion and human rights protection.

‘Promotion’ NHRIs are tasked with fostering a society where human rights are more broadly understood and respected through functions like education, training, advising, public outreach, and advocacy. In the context of digital rights, NHRIs may:

- Provide **technical advice to the government, legislators, ministries, the judiciary**, and other stakeholders to help shape rights-based laws, policies, and practices related to digital technology, datafication, and the Internet.
- Participate in the **design of digital literacy curriculum** to ensure that rights-based norms are incorporated in public education about how to safely and effectively use and benefit from information and communication technologies.
- Encourage **capacity building for institutional actors and civil society** so they better understand digital technologies, the human rights risks, and Internet and data governance approaches that comply with States’ human rights obligations.
- Support and publish **research on the impact of digital technologies** in the country to address gaps in knowledge that can help stakeholders design targeted policies to address online harms.
- Increase **public awareness of digital rights** through campaigns, seminars, and press conferences.
- Apply the human rights-based framework, including the UN’s Guiding Principles on Business and Human Rights, to the domestic technology sector and **conduct assessments that evaluate the sector’s impacts on human rights** (e.g., assessing risks arising from the design and deployment of AI systems).
- Call for and facilitate **meaningful and inclusive and participatory multi-stakeholder engagement** to ensure diverse voices, including those from impacted communities, are included in policymaking related to digital technologies.
- Call for **increased transparency and independent oversight in public sector procurement** of digital technologies.

‘Protection’ NHRIs are tasked with addressing human rights violations when they occur and preventing violations from being perpetrated through functions like

monitoring, inquiring, investigating, and reporting on human rights violations, including the handling of individual complaints. In the context of digital rights, NHRIs may:

- **Monitor proposed legislation** with respect to its impact on digital rights and submit recommendations on how to ensure human rights compliance.
- Incorporate digital rights topics, such as online privacy rights violations and incidents of government ordered network disruptions, into **annual reporting as well as submissions to UN mandate holders and the Universal Periodic Review (UPR)** and other regional and international human rights monitoring processes.
- Connect with **domestic and regional digital rights organizations** to coordinate efforts to address digital rights violations.
- Revise existing intake material to **systematically receive complaints** of digital rights violations.
- Ensure **internal policies and methodologies** for investigating, analyzing, and reporting take into consideration the types of information, data, and tools needed to address digital rights violations.
- When supporting complainants and victims, **provide resources and referrals for digital security best practices and capacity building** so they can better protect themselves as they seek redress.
- Investigate **digital rights violations** and call for the necessary measures to end them and ensure non-recurrence.

According to paragraph 20(B)(a) of the **2018 Marrakech Declaration**, NHRIs should commit to: “Monitor and report on civic space – **online and offline** – through the collection and analysis of disaggregated data, including gender-based disaggregation and statistics related to killings, fabricated legal charges, misuse of specific laws and other attacks against human rights defenders, journalists and trade unionists, lawyers, students, academics. . . .”

1.5 How is Digital Rights Monitoring Different from Traditional Human Rights Monitoring?

TYPES OF VIOLATIONS AND INDICATORS

While traditional human rights monitoring focuses on protecting human rights in the physical world, digital rights monitoring addresses rights in the context of technology,

the Internet, and digital communication. However, our online and offline worlds are often interrelated, and digital tools can be abused in ways that cause physical harm. The following table demonstrates the intersection between digital and non-digital rights. Please note that the table is non-exhaustive.

Human Rights Violation	Non-Digital Harm	Digital Rights Intersection
Arbitrary deprivation of Life	Extrajudicial execution	Unlawful digital surveillance leading to detention, trial without due process, and/or execution
Arbitrary arrest and detention	Unlawful imprisonment without due process	
Cruel, inhumane, or degrading treatment	Physical or psychological abuse	
Vague/disproportionate restrictions to freedom of expression	Raiding or forcing closure of the offices of media outlets Arbitrary detention in retaliation for legitimate speech (offline) Harassment, physical assaults in retaliation for speech Strategic lawsuits against public participation (SLAPPs) Non-compliance with access to information laws	Blocking access to a media outlet's website or social media page Arbitrary detention in retaliation for legitimate speech online and criminalizing vague categories of online speech (e.g., fake news, sedition) Cyberattacks (e.g., DDoS attacks), online harassment in retaliation for speech Online content takedowns, filtering based on vague content bans Civil or criminal sanctions for platform intermediaries that do not take down content based on vague content bans
Arbitrary, disproportionate restrictions to association, assembly	Arrest or abuse of peaceful protesters Imposing onerous requirements to obtain permits for peaceful protests Arbitrarily denying applications by civil society actors for legal personality Arbitrarily preventing access to domestic, foreign funding	Network disruptions during protests (e.g., partial or full Internet shutdowns, throttling, or platform blocking) Arbitrarily preventing civil society from registering country-level domain names Unlawful search of civil society organization (CSO) offices to seize digital tools

Violation of the right to non-discrimination	Law enforcement actions targeting a certain racial, ethnic, or religious group (e.g., racial profiling)	Algorithmic decision making unduly impacting certain groups (e.g., racial bias in facial recognition) and reinforcing existing biases. Digital exclusion reflected in discriminatory policy
Private sector abuses	Threatening, harassing, or attacking environmental rights protestors and union organizers Initiating SLAPP lawsuits when journalists and human rights defenders criticize their business practices Exploitation across the supply chain by using cheap labor and allowing unsafe work conditions	Failure to publish meaningful transparency reports on privacy practices, content moderation policies, or use of algorithmic decision making Failure to safeguard personal data Different rates charged by Internet Service Providers (ISPs) for various content, violating net neutrality
Violence against women	Domestic abuse, sexual assault, and femicide	Technology-facilitated gender-based violence (e.g., online dissemination of non-consensual sexual images)
Violation of the right to privacy	Raids, searches, and seizures without an authorized warrant	Extralegal, invasive digital surveillance (e.g., spyware) Untargeted, bulk data collection without due process

ACTORS

In the context of the Internet and digital technologies, many State and non-State actors play relevant roles that give rise to human rights obligations and responsibilities. NHRIs should consider how these actors impact digital rights in order to effectively monitor their compliance with relevant laws and norms. While NHRIs will monitor and engage with many of the same actors regardless of whether the right is exercised online or offline, there might be key differences that should be considered:

- 1. Same Actors, Different Tactics:** The same State actors, such as law enforcement, interior and national security ministries, and parliamentarians, have instrumental roles in both the digital and non-digital sectors. In the digital space, these actors might be responsible for enforcing regulations or deploying certain tools and tactics that impact digital rights. For example, police officers

may use invasive surveillance tools during investigations, while political parties may utilize social media for disinformation campaigns or to facilitate cyberattacks against opposition candidates during elections.

- 2. New Actors:** In the context of digital rights, there may be new actors that NHRIs should monitor because a ministry or office was created by law, or an existing ministry is tasked with new enforcement powers. Data protection offices, digital affairs bureaus, and ICT ministries often fall into this category.
- 3. Role of the Actors:** While certain actors may have always been relevant in the context of human rights monitoring, they may have an expanded role in the digital space. In most countries, the government relies heavily on the private sector to procure public sector technologies and to manage online space. Thus, NHRIs must give due consideration to the role of the private sector in facilitating or assisting with digital rights abuses.

The following table provides examples of the type of actors NHRIs might encounter in non-digital as opposed to digital monitoring and engagement:

Actor	Non-Digital	Digital
Head of State	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
National Security Authorities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Law Enforcement	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Parliament/Legislators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Political Parties/Politicians	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Protection Office		<input checked="" type="checkbox"/>
ICT Ministry		<input checked="" type="checkbox"/>
Digital Affairs Ministry		<input checked="" type="checkbox"/>
Private Sector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

SCALE

Digital technologies and the modern capacity of technologies to collect and process large volumes of data has enabled governments and the private sector to extend their reach in ways that would otherwise be unfeasible.

As a result, violations tend to impact a far greater number of victims than traditional human rights violations. For example, a countrywide Internet shutdown impacts all Internet users in the country. Even people who are not connected to the Internet could

experience harm if the services they access, such as healthcare, rely on Internet connectivity to effectively function. Meanwhile, mass surveillance practices, such as social media monitoring and CCTV cameras enabled with facial recognition tools, impact the privacy rights of a greater number of people than traditional surveillance methods.

SOURCES & METHODS OF COLLECTION

Both digital rights monitoring and traditional human rights monitoring **require** “observing, collecting, cataloguing, and analyzing data and reporting on a situation or event” by seeking information from State agencies, CSOs, victims, and media sources.

Traditional human rights monitoring involves the collection and review of **documentary evidence**, such as letters; transcripts; court, police, and prison records; videos and photographs; medical records; and forensic evidence. Secondary documentary sources may include news reports, books, articles, and other written resource materials.

Both traditional human rights and traditional human rights monitoring will include review of laws, regulations, or other government documents.

Interviews with victims, experts, and whistleblowers are also relevant regardless of the type of violation an NHRI is investigating. Fact-finding may also include (1) gathering information through focus groups and community meetings; (2) documentation and case file review; (3) observation of processes like trials or elections; (4) media monitoring; (5) legislative monitoring; and (6) on-site inspection of specific places where the risk of human rights violation is high or at least relatively higher than elsewhere, for example, places where persons are detained or forced to reside.

Sample Interview Questions to Establish Digital Rights Violations

- Q: Name (with leeway for anonymity where preferred)
- Q: What is the human rights violation being reported?
- Q: Where did it occur (offline or online)?
- Q: What tools were used to violate the right(s)?
- Q: Who was involved in causing harm?
- Q: Who was affected or could potentially be affected?
- Q: Is information readily available in the public realm concerning the violations?
- Q: What action is required to address the challenge?

In addition to these methods, digital rights monitoring relies more heavily on digital tools and digital forensic analysis, including:

- Online government records and databases
- User-generated content on social media, such as videos/images taken by eyewitnesses
- Disinformation analysis on social media to identify patterns and the coordinated use of bots and trolls to influence elections or attack journalists and human rights defenders
- Internet traffic data to measure network disruptions
- Forensic analysis of digital devices to determine if a phone has been illegally accessed

Digitization of NHRIs

NHRIs are increasingly digitizing their operations, using computers, mobile phones, email, data management systems, social media monitoring, analysis tools, and commercial software to conduct their work. Even when investigating physical violence by law enforcement during an in-person protest, for example, an NHRI may speak to victims using a mobile phone application, record the interview using Google or Microsoft software, and input information from the interview into a database.

There are many considerations to integrating digital data into human rights monitoring effectively and securely. [DatNav](#), a guide developed by Benetech, the Engine Room, and Amnesty International, can help NHRIs better understand the types of digital data available and methods for collection, storage, analysis, and reporting.



SECTION 2

Governance of the Internet & Digital Technologies

2.1 Actors Responsible for Internet Governance

The Internet is a complex, global, interconnected network managed by Internet service providers (ISPs), private companies, academic institutions, and governments. Digital technologies may be connected to the global Internet, or they may be operable without any network connection. When a digital rights violation occurs, there may be several different actors responsible. Understanding the ecosystem of responsibility and control can help NHRIs conduct investigations and effectively report digital rights. The most relevant entities that NHRIs should consider monitoring are described below:

MULTILATERAL MECHANISMS pass resolutions, develop principles, make treaties, and interpret how international law applies in the digital space.

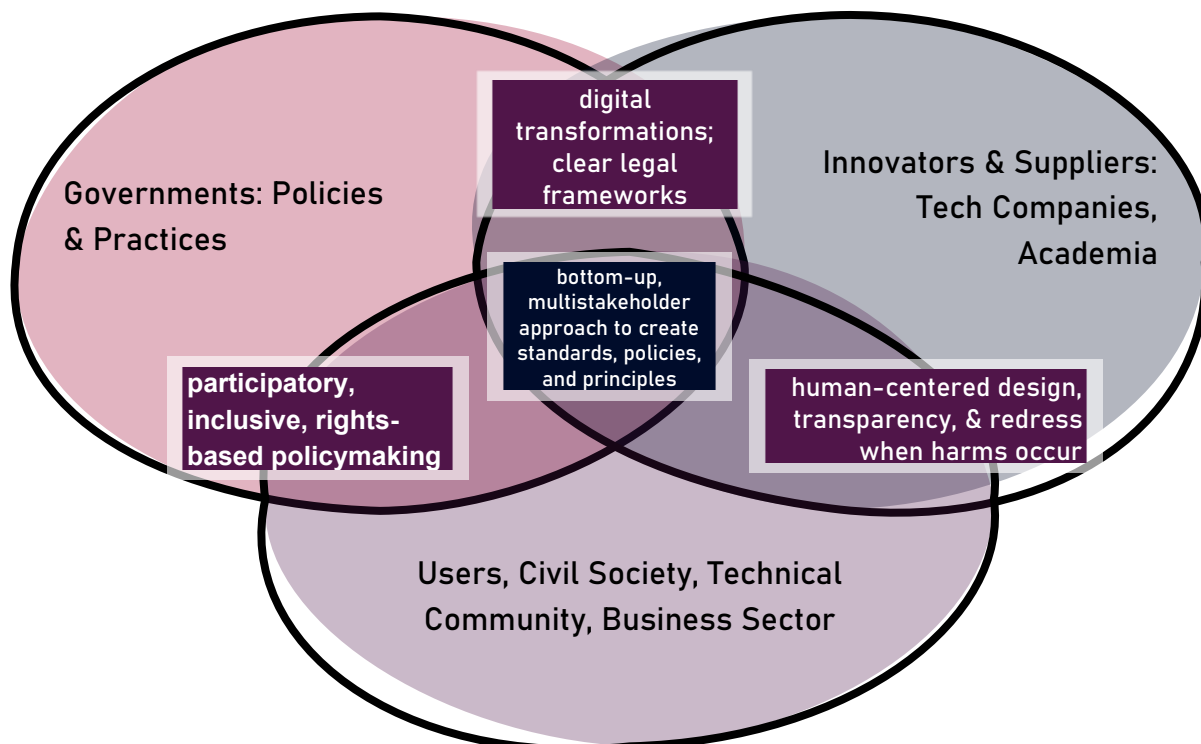


GOVERNMENTS pass laws, regulations, and policies that impact digital rights. Governments are increasingly regulating the digital space, putting in place legal frameworks for data flows, investigation of cybercrimes, and social media companies.

THE PRIVATE SECTOR includes telecommunication providers that own subsea cables, cloud service providers that own data centers, ISPs that provide consumers access to the Internet, social media companies that run platforms and instant messaging applications, hardware developers, and domain name registries, to name a few. In the absence of regulation, companies decide how their technologies are designed, developed, and deployed. The United Nations (UN) Guiding Principles for Business and Human Rights provides a framework for preventing, addressing, and remedying human rights abuses, but it is non-binding, so adherence is varied across companies and sectors.

Public-Private Partnerships have been a key mechanism for expanding broadband access, bolstering cybersecurity of critical infrastructure, and implementing e-governance programs. The relationship and roles of each stakeholder must, therefore, be considered when assessing the digital rights environment in a country.

MULTISTAKEHOLDERISM is the concept that effective, rights-based Internet governance that recognizes the Internet as a global public resource must be governed through informed, participatory, and transparent engagement across sectors, including governments, the private sector, civil society, the technical community, academia, and others. The following graphic demonstrates how the multistakeholder model envisions stakeholders working together to manage the Internet in the public interest.



2.2 Types of Laws and Regulations that Impact Digital Rights

Laws and regulations can either protect or hinder digital rights, depending on their design and implementation. Balancing the interests of users, businesses, and governments remains a complex challenge in the digital age.

TELECOMMUNICATIONS REGULATORY FRAMEWORKS seek to manage the communications industry, including Internet service providers (ISPs) and mobile carriers. Frameworks may aim to:

- Outline the roles and responsibilities of regulatory authorities and detail decision-making processes.
- Foster effective competition in the telecommunications industry, creating licensing regimes and protecting consumer interests related to access, affordability, and privacy.
- Define types of critical infrastructure while setting forth a framework for their protection and security.

In providing regulatory frameworks for communication networks, framework laws may also include provisions that impact on Internet access, data protection, online speech, and electronic surveillance.



DEMOCRATIC REPUBLIC OF CONGO (DRC) Although Law No 20/017 on Telecommunications and Information Communication Technologies includes many positive provisions establishing consumer protections, it also provides the government with broad discretion to order ISPs to shut down the Internet in whole or in part due to national security, public order, or any other reason it deems necessary.

CYBERCRIME AND CYBERSECURITY LAWS establish legal frameworks to prevent various forms of cybercrimes such as hacking, identity theft, online fraud, and cyberstalking. These laws may:

- Define the standard of behavior for using digital technologies and the activities that constitute crimes, such as hacking, online fraud, cyberbullying, and incitement to violence.
- Outline the investigative measures and powers for obtaining and handling digital evidence.
- Safeguard personal, financial, and sensitive information from unauthorized access, theft, and misuse.

These laws may also set standards and regulations for organizations, encourage implementation of adequate cybersecurity measures, and provide mechanisms for

holding cybercriminals accountable. However, if not carefully balanced, cybercrime laws can also negatively impact digital rights:

- States have used overly broad cybercrime laws with vaguely worded provisions to criminalize otherwise legitimate speech, targeting journalists, activists, and political opposition. In some instances, the **penalties are harsher** for speech disseminated online as compared to through traditional means.
- They may include vague content restrictions that impede individuals' rights to seek, receive, and impart information.
- Investigatory authorities may enable mass surveillance or interception of communication data without due process safeguards, such as independent judicial oversight.



EGYPT Anti-Cyber and Information Technology Crimes Law, Law No. 175 of 2018 authorizes broad state censorship, website blocking, and online surveillance. In addition, the law mandates that ISPs keep and store users' data, including phone calls, text messages, and browsing and application history, for 180 days. Such data is made accessible to law enforcement **without necessary human rights safeguards** and stiff penalties apply for failure to comply.



KENYA The Computer Misuse and Cybercrimes Act No. 5 of 2018 aims to protect the confidentiality, integrity, and availability of computer systems, programs and data, and to facilitate the prevention, detection, investigation, prosecution, and punishment of cybercrimes. However, the Act contains several worrying provisions, such as those that outlaw the publication of "false information." At the height of the COVID-19 pandemic, the government used the Act to **prosecute media and human rights activists** for allegedly publishing and spreading "false and alarming information" on social media about COVID-19.

PENAL CODES In some countries, definitions of cybercrimes and surveillance authorities are included in penal codes rather than standalone cybercrime legislation. Penal code provisions can be just as problematic, however, by criminalizing speech using vague language and disproportionate penalties and authorizing disproportionate, unchecked surveillance powers.



BURKINA FASO The Penal Code criminalizes expression against military forces and increases penalties for insults made "via an electronic means of communication," which are punishable by a sentence of up to five years imprisonment.



DRC The Penal Code **criminalizes defamation**, public insult, slanderous denunciation, insults against government bodies and the "publication, dissemination or reproduction" of "false news." It is also an offense to knowingly spread false rumors that are likely to alarm the public, worry the public, or incite the public against "the established powers."

OTHER LAWS REGULATING SPEECH

Governments may also pass standalone legislation that regulates speech online, such as “fake news” laws. The laws may criminalize speech and impose liability on content providers (e.g., social media companies, ISPs, instant messaging services, websites, etc.) that do not remove prohibited content from their platforms. It may require content providers to register in the country, obtain licenses, or use automated tools to filter or take down content. Like cybercrime laws, the provisions prohibiting categories of speech may be **vague and ambiguous** and the registration provisions are typically disproportionately onerous. In both cases, the impact is to stifle expression and public debate.



TANZANIA 2022 amendments to the Electronic and Postal Communications (Online Content) Regulations (EPOCA) makes licensing for online media services mandatory. The penalty for non-compliance is a large fine, imprisonment of at least twelve months, or both. This creates disproportionate regulatory burdens and restrictions on the freedom of expression of independent bloggers, citizen journalists, and community-based media that cannot afford the license fees and onerous licensing requirements.

DATA PROTECTION LAWS

create a framework for the processing of **personal information or personal data**. Data protection laws provide greater notice and control to users over personal information. Data protection laws can safeguard the fundamental right to privacy by:

- Regulating the processing of personal data based on principles of lawfulness, fairness, transparency, and accountability.
- Providing individuals with rights over their data (e.g., the right to request their data be erased, the right to restrict how their data is processed, the right to object to automated decision-making, etc.).
- Setting up systems of accountability and clear obligations for those who control or undertake the processing of the data.

While these rights and obligations provide a much-needed framework for personal data protection, they include many exemptions that can weaken privacy rights. One example is the **“legitimate interest” exception**, which exempts entities from seeking a user’s consent for processing personal data if it is necessary to achieve a legitimate aim pursued by the entity. This exemption is included in most, if not all, data protection laws, including the European Union’s General Data Protection Regulation (GDPR). However, some exemptions are even broader than the standards set in the GDPR. In some cases, the law might **exempt public sector entities** from its obligations. And in some cases, the data protection law might even threaten privacy rights by mandating that broad categories of data **must only be stored within the country’s jurisdiction** or including vague language that enables arbitrary investigations without adequate limitations or **judicial oversight**.



SOUTH AFRICA The Protection of Personal Information Act (POPIA) establishes rights for individuals and places data protection obligations on organizations. POPIA sets minimum standards aligned with international norms and creates a framework for accountability and enforcement.



UGANDA: The Data Protection and Privacy Act of 2019 and the Data Protection and Privacy Regulations of 2021 seek to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information. These laws provide for the rights of data subjects and the obligations of data collectors, data processors, and data controllers. However, these laws also allow government security agencies to access individuals' personal data during criminal investigations. Individuals' data is often used to monitor and track individuals who are suspected of involvement in criminal activities, including political activists, dissenters and government critics.

PROCUREMENT REGULATIONS apply to government contracts for technology services. They impact digital rights by setting and promoting standards such as transparency, fairness, accountability, and safety in public procurement processes. The benefits of procurement regulations are weakened when they include broad exceptions for surveillance technologies procured for national security or law enforcement purposes. In addition to increased transparency, rights-based procurement regulations can:

- Provide that contracts require companies to conform with data protection and privacy laws and be subjected to audits to ensure such conformity.
- Protect human rights by requiring that transactions be confined to companies that do not sell to governments with poor human rights records.



GHANA sets forth a comprehensive framework for public procurement, first established in a 2003 Public Procurement Act and further elaborated through regulations. This framework requires public bids and creates a Public Procurement Authority to oversee procurement processes. This Authority has issued guidance for the procurement of technology products. An online portal displays all public tenders, including for technology products and services, enabling greater transparency.

NATIONAL AI STRATEGIES AND AI REGULATIONS are being adopted in many countries in response to the growing development and deployment of artificial intelligence (AI) systems. National AI Strategies represent a roadmap for how States intend to approach AI, typically including:

- A plan for mapping national AI development to date and the prospects for future innovation and economic growth.
- Steps for how the government will support research and development.
- Governance plan to mitigate AI's ethical and safety risks and impacts on labor.

When it comes to ethical AI use, national strategies typically address bias, transparency, and accountability in the design, development, and deployment of AI

systems. However, if human rights considerations are not integrated into these strategies, there is a significant risk that the development and governance of AI could have a detrimental effect on individuals' rights. To better ensure that national AI strategies comprehensively consider the human rights impacts of AI systems, they should support research on the human rights risks of AI systems in the country during the mapping phase, include plans for human rights impact assessments, particularly in public sector procurement processes, and seek broad public participation in the development of the policy and any follow-on legislation.

As for AI regulation, no standalone law has been adopted in Africa, but the European Union recently passed an AI Act that will take effect in August 2026. It is likely that this Act will influence legislation around the world, including in Africa.

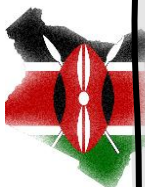


RWANDA released its National AI Policy with the aim of harnessing AI for sustainable development and mitigating its risks. Rwanda's Guidelines on the Ethical Development and Implementation of AI address the range of risks in the AI system lifecycle and considerations for responsible and trustworthy adoption of AI in Rwanda. The principles guide stakeholders in promoting the well-being of individuals, ensuring fairness and transparency and fostering innovation while upholding ethical standards.

TAX LAWS AND REGULATIONS may levy taxes on various forms of digital technology or Internet usage. Some countries have implemented "social media taxes" which require users to pay a levy to access certain social media platforms. Excise taxes imposed on mobile services and high import duties on mobile devices also contribute significantly to the overall cost of using the Internet. Particularly in Africa – a region that already has the highest financial barriers to access in the world – taxes on Internet consumption can make Internet access unaffordable, particularly for lower-income and underserved populations. This not only impacts the right to access information and the freedom of expression, but also many other rights that may depend on Internet access – for example, the right to work, the right to food, the right to health, the freedoms of association and peaceful assembly, and even the right to life.



UGANDA In 2018, Uganda introduced the Over-The-Top tax that required Ugandans to pay a daily levy to access over 50 online platforms, including Facebook, Twitter, and WhatsApp. Following the implementation of this tax, Internet penetration dropped by five million users within a period of just three months. The tax was replaced in 2021 with a direct 12% levy on the net price of Internet data.



KENYA The Finance Bill 2024/2025 proposed changes to the Kenyan tax regime intended to raise \$2.7 billion in additional taxes. The Bill imposed an eco-tax on products that are considered harmful to the environment, including computers and mobile phones; increased taxes on mobile money transfer services; increased the Value Added Tax on locally assembled and manufactured mobile phones; and increased the excise duty on telephone and Internet data services. On June 26, 2024, in response to two weeks of widespread anti-tax protests across Kenya, President William Ruto announced the withdrawal of the Bill.

SECTION 3

Examples of Digital Rights Violations

3.1 Network Disruptions

A **network disruption** is the intentional, significant disruption of electronic communication within a given area or affecting a predetermined group of citizens.

SHUTDOWNS involve the large-scale or complete disconnection of digital communication, with the impact radius covering a local area, an administrative region, several regions, or an entire country. These extreme disruptions are also called Internet shutdowns or blackouts.

THROTTLING is a reduction in bandwidth speed, decreasing the usability of Internet access. When the Internet is throttled, it takes a long time for a web page to load or for a user to access web tools. Throttling **frustrates** users and prevents them from meaningfully accessing the Internet.






BLOCKING is the prevention of access to a website, domain, or IP address.

Network disruptions **often occur** in the context of protests or during election periods. Dozens of countries have been affected by Internet shutdowns in recent years. Between January and May 2023, a period of just five months, Access Now **recorded** 80 network disruptions in 21 countries. In February 2024, the Internet **was disrupted** in Senegal after the President announced that the country's elections would be delayed. Shutdowns also occurred in Sudan, Libya, Somaliland, Sierra Leone, Tunisia, and Burkina Faso in 2022, and in Guinea, Mauritania, Uganda, Sudan, and Somaliland in 2023. In Zimbabwe in 2022, the opposition Citizens' Coalition for Change (CCC)

reported the throttling of Internet speeds and blocking of access to social media during a political rally held ahead of the national elections.

HUMAN RIGHTS IMPACTS

Several human rights mechanisms have addressed network disruptions. In 2016, the **ACHPR passed Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa** that condemns government-ordered shutdowns during elections and protests. The impacts on rights are numerous:

-  Network disruptions directly infringe upon ***the right to freedom of expression***. These restrictions on freedom of expression are not narrowly tailored to address a legitimate aim. Instead, when communication channels are blocked or slowed down, all individuals in the target area are impacted, losing the ability to access information, express opinions, or participate in online public debates.
-  Disruptions frequently target or restrict ***freedoms of association and peaceful assembly***. Social media are increasingly used as a tool of collective action, and play a leading role, or at least a complementary role, to traditional forms of coordination and organization.
-  The impact of disruptions on expression is perhaps most acute when they coincide with restrictions on ***freedom of the media***, particularly with the growing online presence of traditional media outlets across the world. In the context of armed conflicts and during mass demonstrations, the inability for people to communicate and promptly report abuses **seems to contribute** to further insecurity and violence, including serious human rights violations.
-  Internet access has become crucial for the enjoyment of socio-economic human rights. Therefore, disruptions limit ***access to health, education, and emergency services***, with an outsized impact on **underserved and marginalized groups** that cannot access alternative services. Disruptions in rural and remote areas could be the difference between life and death while also undermining access for women and girls to critical support and protection, exacerbating the gender divide. Meanwhile, Internet access has generally become an important tool in basic education and has become indispensable for higher education.
-  Network disruptions also ***negatively impact economic activity***: they have been shown to halt e-commerce, generate losses in time-sensitive transactions, increase unemployment, interrupt business-customer communications, and create financial and reputational risks for companies. Across 39 countries, 140 mobile money and banking services host about 280 million registered accounts, providing safe, low-cost, and rapid financial transfers while broadening financial inclusion. Economic shocks provoked by shutdowns are felt over long periods, greatly exacerbating pre-existing social and economic inequalities.



In Nigeria, when the **government ordered the blocking of Twitter** from June 2021 to January 2022, over 80 million Internet users lost the ability to access one of the most popular social media platforms in the country. Given that the business community in Nigeria used Twitter to advertise, conduct commerce, and access customers, the network disruption also had a significant economic toll. The Twitter ban was announced during a press conference shortly after Twitter deleted posts from and suspended the account of then President Muhammadu Buhari for violating the platform's terms of service. These circumstances demonstrate that the ban had no basis in Nigerian law, did not have a legitimate aim, and was a disproportionate restriction that impacted the fundamental human rights of millions of Nigerians.

HOW DO NETWORK DISRUPTIONS HAPPEN?

An intentional network disruption is different from an accidental shutdown that might occur due to power failures, natural disasters and weather events, or hardware malfunctions.

There are many different mechanisms for intentionally disrupting the Internet. In some cases, the government orders all Internet Service Providers (ISPs) operating in a country to manipulate Internet traffic. The Internet is a network of networks, and ISPs (or other entities like universities and government agencies) own pieces of the network, enabling Internet traffic to move from networks operating globally to networks in the country where the ISP operates via international Internet gateways. As a result, ISPs can reroute Internet traffic so that data does not reach the networks within the country. Throttling is based on similar mechanisms, except the Internet traffic is slowed, rather than stopped completely. For blocking, ISPs can also manipulate Internet traffic for a specific domain name, like "facebook.com" so that only one website or application is blocked.

This is a very simple explanation of the technical apparatus that enables disruptions. For more information about:

- The technical protocols that enable Internet traffic to travel around the world, see this explainer from the company Cloudflare about the **[Border Gateway Protocols](#)**.
- Specific mechanisms used to facilitate intentional network disruptions, the civil society organization (CSO) Access Now has a helpful report, **[A Taxonomy of Internet Shutdowns: The Technologies Behind Network Interference](#)**.
- How government tactics to disrupt the Internet have changed over time, see the paper from the Carnegie Endowment for Peace **[Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?](#)**



There is a startling lack of transparency when it comes to network disruptions. As in the case of Nigeria's Twitter ban, governments rarely have legal grounding for a disruption. And since ISPs have licensing agreements with governments, they may be contractually forced to implement a shutdown even if it is not in their economic interest to do so. ISP licensing or *ad hoc* agreements are often not publicly available and might even include clauses that prevent them from publicly disclosing communications they receive from the government, including disruption orders. When ISPs have discretion to provide public notice, they should be encouraged to do so, in accordance with the UN Guiding Principles on Business and Human Rights.

Promotion

NHRIs can play a role by 1) requesting the public disclosure of all agreements between ISPs and the government, 2) reviewing the agreements to ascertain if and how the government is authorized to order an ISP to disrupt Internet access, 3) recommending that ISPs provide notice as to any government orders when they have discretion to do so, 4) advising the government on the civil, political, social, and economic impacts of disruptions as well as why network disruptions do not comply with their human rights obligations, and 5) calling for greater transparency and notice regarding intentional disruptions.

DATA SOURCES AND CIVIL SOCIETY EFFORTS

[Access Now's STOP Project and #KeepItOn Coalition](#) is the leading global initiative that monitors Internet shutdowns and advocates against them. The Coalition also engages with governments, companies, and civil society to preserve Internet access, document instances of disruptions, and raise awareness about their impact on human rights. To monitor and verify shutdowns globally, the #KeepItOn Coalition collects data from a variety of sources, including:

- Qualitative data from coalition members about Internet outages and local contexts; and
- Quantitative analysis from entities like the [Internet Outage Detection and Analysis \(IODA\)](#), [Cloudflare Radar](#), and [Open Observatory of Network Interference \(OONI\)](#). These sources can also provide NHRIs with helpful data about network disruptions.

Litigation challenging shutdown orders can also help uncover information about government practices, create domestic standards, and provide accountability for

violations of rights. After the **Togolese government ordered** two ISPs, Togocel and Moov, to shut down their networks in 2017 in the context of anti-government protests, seven CSOs and one journalist filed a complaint at the Economic Community of West African States (ECOWAS) Community Court. The Court found in favor of the applicants, thereby **ordering Togo** “to guarantee measures of non-recurrence” and to “enact and implement laws, regulations and safeguards in order to meet its obligations with respect to the right to freedom of expression in accordance with international human rights instruments.”

Protection

To advance protection in the context of network disruptions, NHRIs can

- 1) meet with regional and local CSOs that are members of the #KeepItOn Coalition to better understand their monitoring and advocacy efforts,
- 2) incorporate data from existing monitoring platforms into reports and submissions,
- 3) review existing and draft legislation for provisions that may authorize network disruptions and call for revisions that comply with human rights law,
- 4) document the domestic human rights impacts of network disruptions that have occurred in the past, and
- 5) be prepared to document and receive complaints about disruptions, particularly in the lead up to elections.

3.2 Vague or Disproportionate Online Content Restrictions

Content moderation targets specific speech online using automated technologies, the removal of content, deactivation of comments, or deplatforming of users. While this approach can be more targeted than the types of network disruptions described above, it often constitutes blanket censorship that is inconsistent with human rights law and, with respect to companies, the UN Guiding Principles for Business and Human Rights.

Filtering occurs when a government requires one or all ISPs in the country to implement technology that sieves through Internet traffic to identify keywords or URLs, preventing users from accessing certain sites or webpages that contain prohibited content.

Takedown Orders occur when a government entity determines that content online constitutes prohibited speech and submits an order directly to a website or platform to remove the content. The website or platform can either prevent the content from being seen by users within the government's jurisdiction or can remove the content altogether.

Intermediary Liability imposes legal responsibility on content providers, such as website, social media platforms, ISPs, or instant messaging services, for the content generated by its users. As a result, the content provider might incur civil or criminal penalties if it does not respond to a takedown order within a certain time period, does not remove content following a user complaint, or, in extreme cases, does not proactively take down content, such as through the use of automated filtering tools.

Content Moderation Policies are the internal policies and practices of content providers that users must adhere to as a condition for using their services. Many online platforms struggle with defining clear and consistent policies or with adapting their enforcement in countries where their staff do not understand the language or context. When these policies are vague or poorly enforced, the platform might arbitrarily remove content, fail to remove harmful content, or ban certain individuals or groups from using the platform altogether (otherwise known as deplatforming). If a platform consistently targets content related to specific political views or marginalized communities, it can perpetuate bias and can even lead to social instability.

HUMAN RIGHTS IMPACTS



Facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all states. Government content restrictions could violate ***the right to freedom of expression*** unless they adhere to a **three-part test**: the restriction must be provided by law, necessary to achieve a legitimate purpose, and narrowly tailored to address that purpose. Further, “any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences” Thus, responsibility to determine whether certain content is prohibited by law should not be given to political bodies like an ICT ministry or to content providers, like social media companies.



In order to implement content restrictions, governments and content providers constantly monitor platforms and websites manually or with automated tools. This is a type of mass surveillance that could violate ***the right to privacy*** of Internet users. The rights to privacy and freedom of expression are closely linked as

individuals may self-censor or otherwise alter the way they express themselves online when they fear that their speech is being constantly monitored, thereby causing a **“chilling effect” on speech**.

There is a high risk that intermediary liability and the use of automated content moderation could disproportionately harm marginalized groups, leading to **discriminatory application of the law**. AI systems are at high risk of reproducing **historic biases** and removing online content that is not problematic but that expresses the perspectives of historically marginalized groups. When intermediaries use content moderation staff or automated tools that are not adequately trained to address the language, context, or diversity within a given country, they can **negligently** foster discrimination, hate, and incitement by failing to account for the vast experiences of their users and the contexts where they operate.

Balancing Competing Rights

Website blocking and content removal is justifiable in limited circumstances, such as removing child sexual abuse material online to protect the rights of a child or to combat incitement to genocide and violence. However, content prohibitions must be provided by law and should be narrowly defined in order to comply with human rights obligations.

DATA SOURCES AND CIVIL SOCIETY EFFORTS

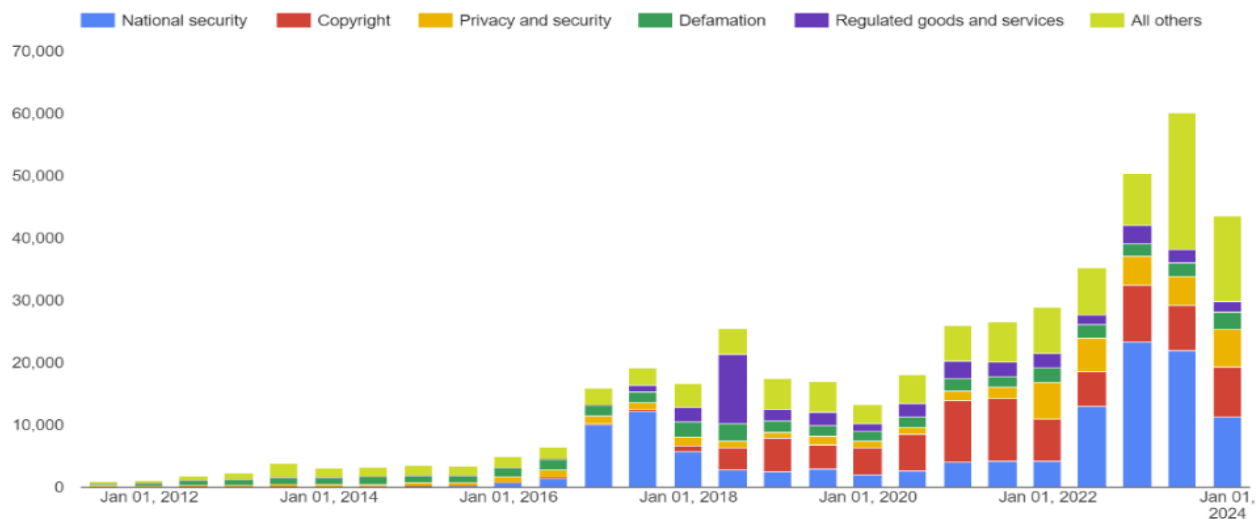
As with network disruptions, it can be incredibly difficult to monitor arbitrary content restrictions when governments and companies are not transparent about takedowns and filtering. Some social media companies issue transparency reports and publish data about the orders they receive from governments and the ways they enforce their own moderation policies, but the datasets are incomplete and do not provide detailed enough information for users to seek redress. And when ISPs implement tools to automatically filter content, users might not even know that they are losing access to potentially vast amounts of information online because they are prevented from seeing the content in the first place.

For more information about restrictions and examples of data that social media companies publish online, see:

- The Internet Society’s report on **how content filtering impacts the Internet way of networking**, which explains the processes and technologies that facilitate government mandated filtering and the impacts they have on the Internet and users’ ability to access information online.

- **Google's Transparency Report Platform**, which allows users to search content takedown orders by country, the type of entity issuing the order, the justification for the order, and whether Google complied. Since 2011 when Google started publishing these statistics, governments have requested the removal of over five million pieces of content. The following is a graph showing the reasons governments have cited for removal requests.

Reasons cited for content removal



- In 2018, Meta created an independent body called the **Oversight Board** to review the company's decisions to keep or remove content online. The Board does not review every appeal and only chooses a few a year that are the most exemplary and can have the biggest impact on the company's policies, but its analysis and decisions can provide important insight into how Meta implements its content moderation policies. As of 2023, Meta has implemented 75 of the Board's recommendations. Note that the Oversight Board only evaluates decisions based on Meta's internal policies – it is not authorized to evaluate the legitimacy of government orders to take down content.

Promotion

To better understand how the government's content restrictions impact human rights online, NHRIs can work with academic institutions and independent researchers in their country to evaluate companies' transparency reports, seek information from government institutions, and research public documents. NHRIs can also advise government institutions to be more transparent about content restrictions, establish independent oversight of content restriction decisions, and use existing guidance and best practices to develop laws and practices that comply with their human rights obligations.

There have also been several principles and guidance documents released on best practices for content restrictions online.

- The [Manila Principles on Intermediary Liability](#) was developed by CSOs to provide a framework for how policymakers should balance legitimate government interests to regulate content providers with their obligations to uphold the right to freedom of expression.
- The [Santa Clara Principles](#) outline minimum standards and call for Internet platforms to provide adequate transparency and accountability about their efforts to moderate user-generated content. The Principles were endorsed by a variety of companies, including Apple, Facebook, Google, and Twitter. In 2021, the Principles were expanded (Santa Clara Principles 2.0) to provide more operational guidance to companies and call on governments to assure transparency and due process.
- The CSO Article19 has a useful Handbook called [Freedom of Expression Unfiltered: How blocking and filtering affect free speech](#) that describes the relationship between filtering and freedom of expression. The Handbook can help NHRIs articulate the human rights concerns inherent in the use of these tools.

Protection

To advance protection in the context of filtering, NHRIs can review laws and practices related to content prohibitions and intermediary liability.

They can document if and how the government orders content takedowns or implements filtering and analyze whether these practices comply with human rights norms. In cases where publicly available information is unavailable, NHRIs can receive complaints from users who claim their content was removed and interview representatives of social media companies, civil society, and other stakeholders to corroborate their testimonies. When documenting content takedowns, NHRIs might find it valuable to speak with technical experts who can explain how filtering technologies function.

3.3 Untargeted or Invasive Digital Surveillance

Digital surveillance is any intentional monitoring of digital communications or information. When used in a manner consistent with applicable international law, surveillance technologies can be important tools for conducting criminal investigations to protect the rights and safety of the public. However, over the years, governments have often invoked national security, public order, and economic stability to justify vast

surveillance powers. Today, governments have access to advanced technologies that can indiscriminately collect and analyze communications data as well as digital images and video, and existing legal frameworks do not provide adequate oversight or constraints in many jurisdictions.

Mass Digital Surveillance: Mass surveillance is the collection of information about an indefinite or large portion of the population. Technological advances have expanded government surveillance in traditionally “public” places, prompting legal questions over the boundaries between permissible and non-permissible data collection. Some examples of digital mass surveillance practices include: 1) remote biometric identification (e.g., CCTV cameras enabled with facial recognition software), 2) use of mobile phone trackers (e.g., International Mobile Subscriber Identity trackers), 3) requirements that ISPs retain all traffic and location data to share with government authorities on demand without a warrant, and 4) indiscriminate interception of digital communications.

According to the CSO Privacy International, “Mass surveillance relies on the assumption that all information could be useful to address a hypothetical threat. . . . It creates an environment of threat and suspicion that is incompatible with democratic values and principles, where in the eyes of the state, all individuals become guilty until proven innocent.”

Invasive or Extralegal Digital Surveillance: Even in cases when digital surveillance is targeted, it may still be problematic if the surveillance is not prescribed by law or uses tools that are disproportionately invasive by gathering data and communications without regard to whether the data is relevant to a criminal investigation. One of the most notorious examples of extralegal, invasive surveillance is spyware technology. Advanced spyware tools can infect a mobile phone or other device without the knowledge of the user. Spyware gives the perpetrator total access to the device and can, therefore, intercept a user’s encryption and password protections. It enables access to the device’s location, all communications, and the phone’s microphone to record nearby conversations. While purportedly being deployed to combat terrorism and crime, such spyware tools have often been used for illegitimate reasons, including to clamp down on those that express critical or dissenting views, including journalists, opposition political figures, and human rights defenders. Governments in Africa, including Morocco, Togo, and Rwanda, are reportedly customers of spyware tools.

HUMAN RIGHTS IMPACTS



Untargeted or disproportionate surveillance violates ***the right to privacy*** protected by both the Universal Declaration of Human Rights (UDHR) and the International Covenant for Civil and Political Rights (ICCPR). The ACHPR

Declaration of Principles on the Freedom of Expression and Access to Information in Africa, 2019 disapproves of the indiscriminate and untargeted collection of data about a person's communications. It recommends that any law that authorizes targeted communication surveillance must provide adequate safeguards for the right to privacy, including the following:

- a. the prior authorization of an independent and impartial judicial authority;
- b. due process safeguards;
- c. specific limitation on the time, manner, place and scope of the surveillance;
- d. notification of the decision authorizing surveillance within a reasonable time of the conclusion of such surveillance;
- e. proactive transparency on the nature and scope of its use; and
- f. effective monitoring and regular review by an independent oversight mechanism.



Related to the right to privacy, untargeted and disproportionate surveillance impacts ***the right to freedom of expression***. It has a chilling effect on speech whereby individuals feel the need to self-censor. It creates an atmosphere of pervasive fear because constant, unrestrained monitoring may result in consequences for the expression of certain opinions. Because journalists are often the targets of surveillance, it also impedes the work of the media and public debate and participation, potentially eroding democratic governance.



The prevalence of paranoia and mistrust, where unrestricted surveillance is in effect, is inconsistent with the establishment and maintenance of relationships that are fundamental for the exercise of ***the rights to freedom of association and peaceful assembly***. These rights are impacted when remote biometric identification or mobile trackers are used to identify individuals during peaceful protests. When tools are used to target CSOs and activists, it deters individuals from joining associations and stifles the work of non-governmental organizations.

In addition to the human rights impacts, victims of digital surveillance report ***psychosocial harm***, including stress, anxiety, depression, and fear as well as a feeling of distrust in institutions, the people around them, and even themselves.



Promotion

As a first step, NHRIs should evaluate existing research and reports about their country's surveillance industry to identify if and how journalists, human rights defenders, political opposition members, or others have been targeted by advanced surveillance technology (CSOs like the [Africa Digital Rights Network](#) and [Privacy International](#) have conducted in-depth research on countries in Africa in efforts to increase transparency on an otherwise clandestine topic). To complement existing research and fill gaps in knowledge, NHRIs can support local research and awareness raising about privacy rights in the country.

Next, NHRIs can 1) engage with parliamentarians, judiciaries, and government institutions to explain the harmful human rights impacts, 2) encourage the creation of an ombudsman or parliamentary committee to oversee government surveillance practices, 3) propose legal reforms to cybercrime and penal codes to increase safeguards, and 4) call for greater transparency in the sector.

RELEVANT DATA SOURCES AND CIVIL SOCIETY ACTORS

As surveillance technologies evolve in sophistication, detecting and documenting violations have become more complex. In some cases, such as with spyware, attribution of responsibility is difficult. Forensic analysis of infected devices can reveal some information about the technical attributes of the spyware, but knowing which government and authority within the government ordered its use either requires an admission of guilt (which is rare) or for researchers to piece together circumstantial evidence to pinpoint the most likely perpetrator(s).

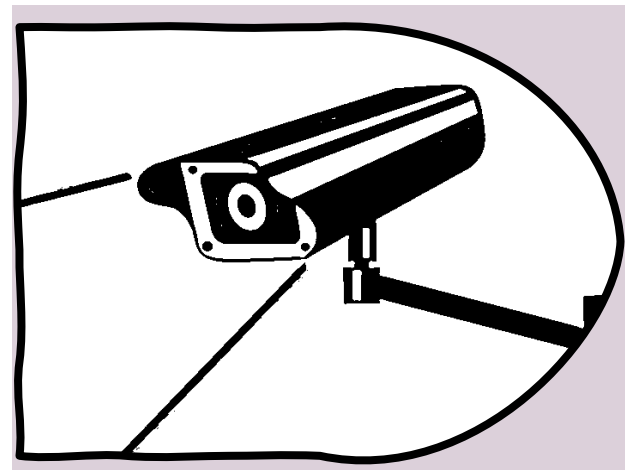
[Citizen Lab](#), a multidisciplinary research lab at the University of Toronto, has been at the forefront of investigating invasive spyware technology. The methods of Citizen Lab, Amnesty Tech, and other organizations that conduct spyware research include:

- **Forensic analysis** of devices (e.g., a phone's browser history) to discover suspicious activities and processes; this evidence can also be correlated to confirmed uses of the same spyware software, thereby identifying patterns. As forensic researchers have uncovered more evidence of spyware configurations, spyware companies have attempted to manipulate device records to make their detection more difficult. The work of forensic researchers is, therefore, constantly evolving to analyze the different tactics, exploits, and software used by the spyware industry.
- **Reverse engineering** the spyware software to identify the processes used to infect a device.

- Review of **reports released by smartphone companies, social media companies, and cloud computing services**, to determine whether certain devices have been infected and how the infections exploited vulnerabilities in the code of their devices and platforms. Since companies like Meta and Apple use proprietary software, when they share data publicly and collaborate with the surveillance research community, it can reveal information that researchers would have otherwise never known. These companies also benefit from the collaboration because they can use civil society research to fix vulnerabilities in their software and improve the services they offer their customers.
- **Interviews with victims of spyware** to provide context for why individuals might have been targeted, and who else in their networks could be compromised. The interviews can also help verify the timeline of when the infection occurred and pinpoint the most likely perpetrator(s).
- **Policy research** to gain context for which governments or institutions within governments could be likely perpetrators of spyware usage based on their past behaviors and existing surveillance infrastructure.
- Confidential information disclosed during **strategic litigation** about government orders, procurements, and communications.

As for mass surveillance programs in Africa, research from a human rights lens has been limited. Therefore, there needs to be more local and regional studies on how governments are gathering data about citizens through smart city projects, digital identification systems, social media monitoring, and mobile tracking systems. Research and reporting on these types of programs from other contexts can help NHRIs identify the most salient human rights risks when governments propose similar initiatives in their countries.

- The Immigrant Defense Project's report [Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"](#) explains what smart cities are, the relationship between digital ID programs and smart cities, and the commercial industry that drives the market for smart cities and digital ID technologies. It highlights New York City's smart city program and provides recommendations for policy actions to align the design and deployment of smart city projects with human rights principles.
- Privacy International has a detailed [legal analysis about international mobile subscriber identity \(ISMI\) catchers](#) that explains how this technology is used to locate and track all mobile devices in a given area and to indiscriminately monitor and intercept communications. It describes rulings from European courts regarding the legality of mass surveillance practices in the European Union, and the impacts on human rights.



- There is a trend in cybercrime laws to mandate that ISPs retain communications data and that they provide law enforcement authorities access to the data without requiring a warrant. In response to such a provision in the Australian Telecommunications Act, the [Australian Human Rights Commission drafted a submission that reviewed the mandatory data retention regime](#) against human rights principles and provided recommendations to the Parliament on how to amend the Act to comply with Australia's human rights obligations.

Protection

NHRIs need to improve their capacity to document digital surveillance abuses. NHRIs do not necessarily need to hire an internal forensic analyst; however, they can connect with international research institutions or local digital forensic researchers to 1) ensure their documentation methodology includes indicators that are relevant to digital surveillance research, 2) connect complainants to researchers who can investigate their devices and provide them with digital security support, and 3) collaborate on submissions to international and regional human rights mechanisms. Through interdisciplinary collaboration with technical experts, NHRIs can better ensure their documentation is comprehensive and persuasive. Additionally, NHRIs should carefully review any legislation related to cybercrime as well as policy proposals for the deployment of smart cities, digital ID systems, and other projects that rely on the bulk collection of personal data to assess their compliance with human rights norms.

Anyone who has been a target of digital surveillance or is concerned that they could be a victim should employ best practices to protect their devices and themselves. For rapid support, [Access Now hosts a Digital Security Helpline](#), available 24/7 in multiple languages. Longer term, organizations should adopt strong digital security policies and practices to ensure their staff and beneficiaries are not put at increased risk. To help victims of digital rights violations, it is important for NHRIs to collaborate with CSOs to monitor the digital rights landscape. [Paradigm Initiative has a Digital Security Toolkit - Ayeta](#) that highlights how digital security threats can be mitigated and a digital rights reporting platform [Ripoti](#). By using digital security tools and practices, organizations and individuals can better protect against cyberattacks and mitigate the severity of harm when attacks occur.



However, given that some advanced spyware can infect devices without the victim even clicking on a malicious link (i.e., zero-click exploits), digital security best practices cannot prevent all abuses. Rather, policy actions to curb the commercial surveillance industry, increase transparency of government surveillance practices, and create meaningful redress when abuses occur are the best way to address the risks of spyware as well as other forms of invasive digital surveillance.

The Freedom Online Coalition – a coalition of 39 member states that are committed to protecting and promoting human rights both online and offline – has developed [Guiding Principles on Government Use of Surveillance Technologies](#). These voluntary Guiding Principles are intended to prevent the misuse of surveillance technologies by governments and those acting on their behalf. They illustrate how governments can maintain their commitment to respect and protect democratic principles, human rights, and fundamental freedoms, consistent with their international obligations and commitments, in the responsible use of surveillance technology.



Acknowledgments

This Toolkit was developed by the International Center for Not-for-Profit Law through close collaboration and support from Paradigm Initiative and the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) through the Greater Internet Freedom initiative. ICNL consultant Faith Kisinga Gitonga contributed to the research and writing. ICNL would also like to thank NHRIs from the Central African Republic, the Democratic Republic of Congo, Mozambique, Tanzania, Uganda, Zambia, and Zimbabwe for providing insights that informed the content of the Toolkit. For more information about the Toolkit, please contact ICNL's Digital Team at digital@icnl.org and Africa Team at africa@icnl.org.

