adapt

Data Protection Advocacy Frameworks for Repressive or Closed Environments

Kuda Hove & Otto Saki

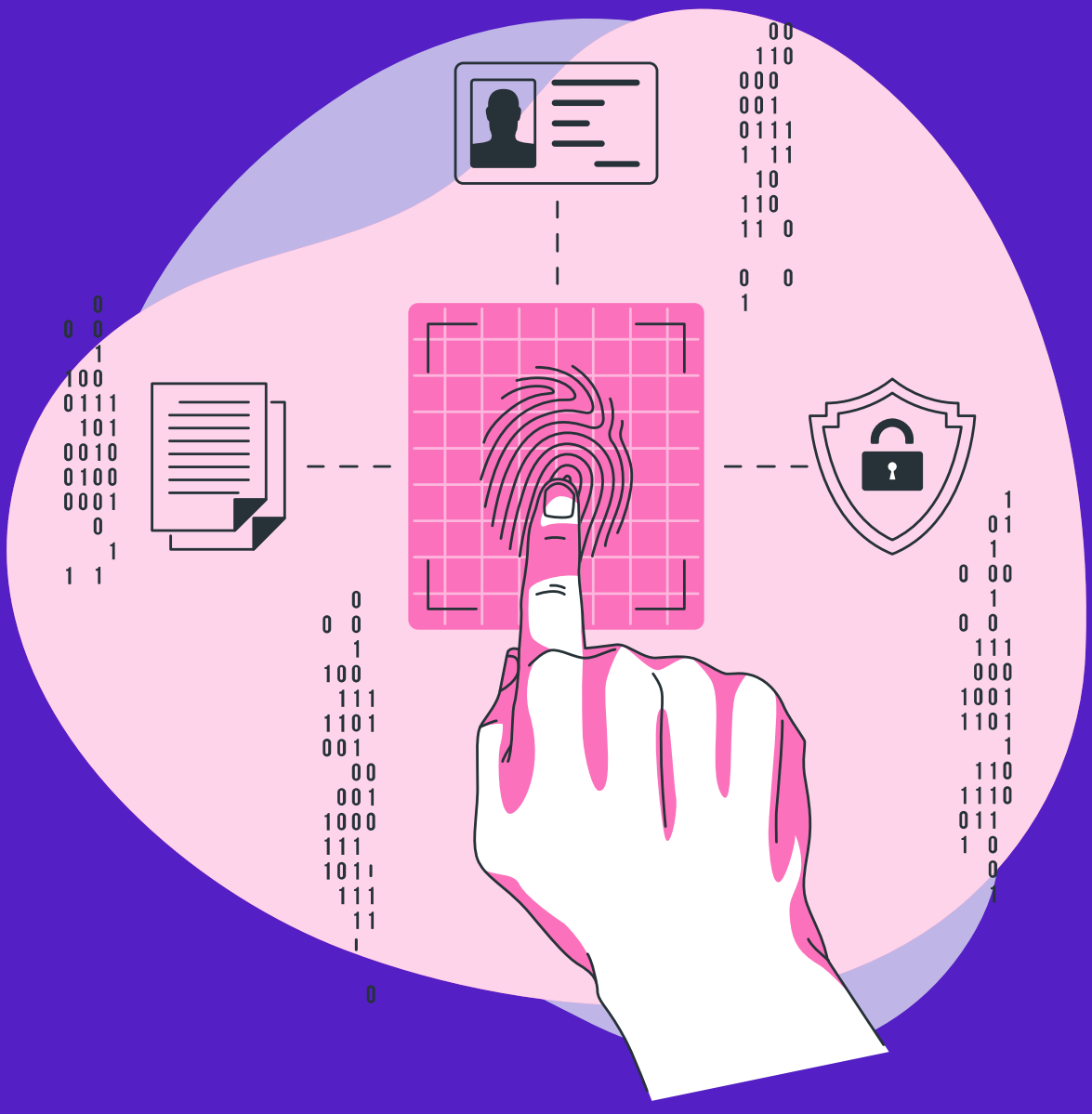


Table of Contents

INTRODUCTION

The development of new technologies has improved the ability of people to engage, share information, express themselves, associate, and assemble, contributing to economic and societal development. As most technologies have dual use, many countries have witnessed the instrumentalization of technology through increased surveillance or invasive practices undermining an individual's right to privacy and other associated rights. The right to privacy is "a prerequisite for freedom – the freedom to live and develop independently." [1]Historically, the right to privacy has been defined as the right to be, let alone. [2]This definition is insufficient given the ever-changing technological landscape and privacy threats emanating from the collection and use of personal information by a wide range of actors. Safeguarding these data and protecting them from unauthorized use and access constitute critical elements of privacy.

The right to privacy is closely related to the concept of data protection, which refers to the legal mechanisms that ensure online privacy.[3]Data protection frameworks in the form of legislation and policies set out the conditions under which personal information can be collected, stored, and processed. These limitations are necessary for the protection and enjoyment of the right to privacy, especially in an increasingly digital world. The right to privacy is not absolute, as is the modern right to data protection. Any limitations to these rights must be clear and precise and are necessary for achieving a legitimate aim. Furthermore, the least intrusive option for the enjoyment of these rights must be used. The onus of proving compliance with these limitations rests on the authorities.

This paper explores data protection law advocacy in the contexts of Uganda, Zimbabwe, and Ethiopia as emblematic of countries that have repressive and closed civic spaces.

This exploration seeks to uncover lessons and strategies that data protection campaigners might use to advocate data protection rights in their respective jurisdictions. Definitions of what amounts to repressive and closed civic spaces are provided and discussed in the first section of this paper. The next section identifies four considerations that data protection campaigners, especially civil society and non-governmental actors, are likely to encounter when advocating the introduction of data protection laws in repressive and closed environments. The four considerations are as follows:

- **How do** we conduct advocacy (particularly that focused on privacy and data protection) in states with weak rules or laws?
- **What happens** when there are many laws that undermine existing or proposed privacy and data protection frameworks?
- **What can** advocates do when data protection laws are inadequate for protecting privacy rights and providing exemptions?
- **How do** advocates anticipate how data protection laws can be repurposed or weaponized by state actors?

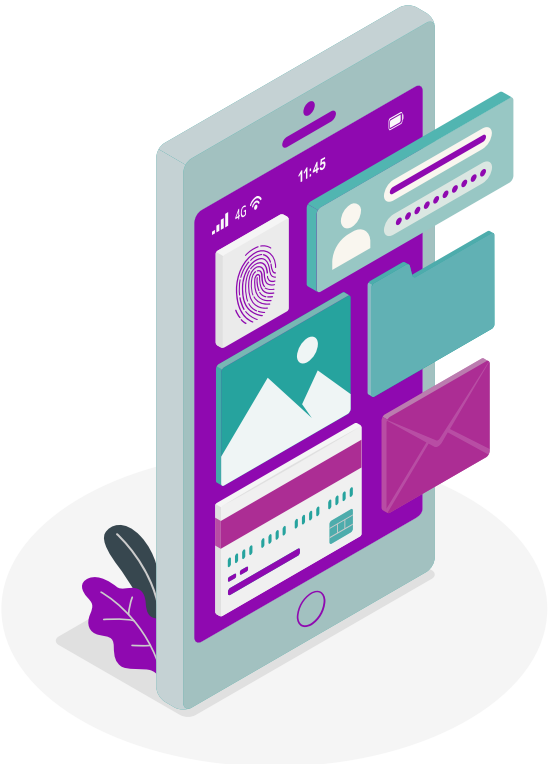
These considerations inform the section on recommendations for advocates to provide more practical and field-tested approaches. The recommendations are not structured as absolutes or final solutions; they might work in some instances and be insufficient in others.

[1]Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/
[2]The right to be let alone. Cooley A Treatise on the Law of Torts 29 (2d ed. 1888), which was popularized in the seminal article by Warren & Brandeis 'The Right to Privacy' Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), 193-220
[3]https://dig.watch/issues/privacy-and-data-protection

METHODOLOGY

This study was developed through desk legal research and expert interviews conducted with key informants from three countries classified as "repressive" by established global institutions monitoring civic space.[4] The three countries of Ethiopia, Uganda, and Zimbabwe were selected as case studies because of the current efforts being made to pass or implement data protection laws amidst challenges with rule of law, constitutionalism, violation of rights (including privacy rights), and one-party system forms of government. Each of these countries is at a different stage of the data protection policy and law-making process, providing an opportunity to conduct nuanced analyses of the challenges data protection advocates have encountered and how they have dealt with them. Uganda's president signed the Data Protection and Privacy Act into law on February 25, 2019, and the Data Protection and Privacy Regulations in 2020. In Zimbabwe, the Data Act came into effect on December 3, 2021, bringing to end a drafting process that spanned almost 9 years. Compared to Uganda and Zimbabwe, Ethiopia is at the nascent stage of the data protection law-making process.

Through key informant interviews, activists and legal experts engaged on these issues answered questions around the constraints to advocacy and civic space in their respective countries, how these constraints impact data protection and privacy advocacy, and the approaches they have taken to confront these challenges. The key informants provided observations on practical challenges in advocating data protection reforms and laws from their vantage points, including what has worked and not worked well. Furthermore, they elaborated on the rationale and motives of the three case study governments to develop, implement, and enact data protection laws, despite being classified as closed or restricted environments. As part of this research, the authors also analyzed the constitutional and legislative frameworks that protect privacy and data in each country.



[4] These are primarily CIVICUS, ICNL and Freedom House.

REPRESSIVE & CLOSED CONTEXTS AND DATA PROTECTION

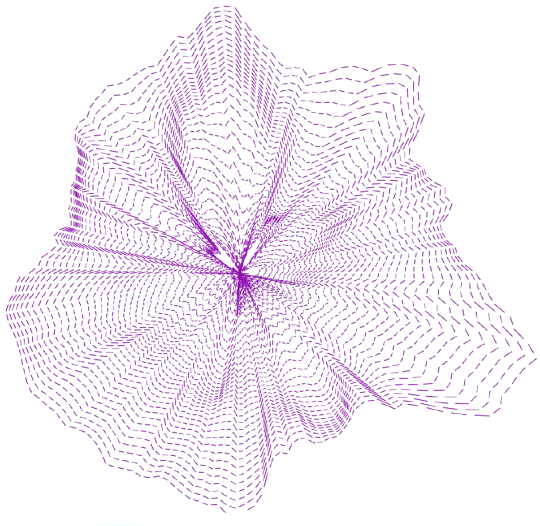
It is important for this paper to define what is meant by repressive and closed contexts to better determine where the proposed data protection advocacy framework will find its application and relevance. This paper uses existing methodologies developed by CIVICUS,[5]Freedom House,[6]and the International Center for Non-Profit Law (ICNL) [7]to assess and measure changes in civic space. A brief overview of each of the respective methodologies is provided in the Appendix. These three methodologies are also selected because they have all been recently used to assess and monitor the civic spaces in the three countries.

The findings in CIVICUS, Freedom House, and ICNL reports on the situation in Ethiopia, Uganda, and Zimbabwe show that these three countries are repressive contexts. These conclusions are also supported by the key informants' experiences and analysis of the legal landscape and practices on personal information protection.

According to these methodologies, repressive civic spaces are characterized by the targeting of "active individuals and civil society members who criticise power holders risk surveillance, harassment, intimidation, imprisonment, injury and death." [8]Repressive civic spaces are also characterized by internet shutdowns, a biased state media, and civil society organizations that are restricted in their work.

A closed civic space is where "an atmosphere of fear and violence prevails, where state and powerful non-state actors are routinely allowed to imprison, seriously injure and kill people with impunity for attempting to exercise their rights to associate, peacefully assemble and express themselves."

At a glance, these three methodologies are specific to fundamental rights, such as the right to free expression, the right to association, the right to assembly, and individual rights. However, these rights are closely related to the right to privacy and, therefore, data protection. For example, in a 2015 report, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression described the right to privacy as "a gateway for freedom of opinion and expression."[9]



[5]https://www.civicus.org/index.php/what-we-do/innovate/civicus-monitor
[6]https://freedomhouse.org/report/freedom-world
[7]https://www.icnl.org/resources/civic-freedom-monitor
[8]https://monitor.civicus.org/Ratings/
[9]http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

Data protection has many facets enhanced by the protection of other rights of assembly, association, and expression, as all these rights are interdependent. For instance, freedom of assembly requires that individuals freely assemble and are free from unwarranted intrusion into their congregated physical or virtual space. Intrusion, in this instance, includes the use of digital surveillance tools, such as facial recognition cameras, to collect physiological personal information. Similarly, when exercising an opinion or expression, interference with the choices and decisions to exercise an opinion or expression constitutes a violation of privacy. Restricting this right on digital spaces depends on the use of personal information.

Note that data protection is more than just personal information interests, expressions, and opinions. Noam observed that "privacy is an interaction, in which the information rights of different parties collide."[10]This is the tension among freedom of expression, the right to know and access information, and the right to privacy. What the right to privacy seeks to protect, the right to freedom of expression and access to information seeks to provide. No right is more important than the other right. Data protection laws protect personal information, while freedom of expression and access to information promote the right to know. As a respondent from Uganda observed,

There is a relationship between civic spaces (the operating environment of civil society actors) and policies, regulations and practices guaranteeing their rights to privacy and data protection. If civil society actors cannot guarantee the anonymity of their communications, this greatly impacts on their ability to enjoy and advance other rights such as assembly.

The interdependence of rights is also highlighted by the fact that in open and democratic countries, protecting the right to privacy does not undermine or threaten the information openness that characterizes democracy. This illustrates how the right to privacy enables the enjoyment of other rights, as a person is more likely to legitimately express themselves when they are assured of their privacy. Similarly, a person is likely to seek and access information without any fear only when they are confident that their search history, for example, will not be accessed without consent.

In summary, governments that do not prioritize and even restrict the right to free expression or the right to assembly and association are not likely to respect, promote, or protect the right to privacy or to push for the introduction of robust data protection policies or laws that are influenced by and grounded on human rights principles. If these governments enact data protection laws, there is a higher chance that the laws will be insufficient in advancing the right to privacy and other related rights. Countries with no freedom of expression are unlikely to have a robust right to privacy or personal information protection laws. There is also an intersection of these closed countries and environments with countries that are suspected of using personal information extraction technology to stifle expression, opinion, and invasion of privacy.[11]

The latest CIVICUS Monitor report[12] indicated that the civic space in each of the three countries is repressed. According to CIVICUS, a repressive rating means that "Civic space is significantly constrained. Active individuals and civil society members who criticise power holders risk surveillance, harassment, intimidation, imprisonment, injury and death. Although some civil society organisations exist, their advocacy work is regularly impeded and they face threats of de-registration and closure by the authorities."[13] Similarly, in 2020, all three countries were rated as not free by Freedom House in its Global Freedom Status.[14] The ICNL reports on each country[15] highlight several laws and policies that restrict the exercise and enjoyment of the right to assembly and association, along with the right to free expression.

---

[10]Noam EM Privacy and Self-Regulation: Markets for Electronic Privacy (1997).
[11]See https://giswatch.org/en/country-report/communications-surveillance/ethiopia; Huawei and Surveillance in Zimbabwe https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe; Ethiopia Ethiopia: New Spate of Abusive Surveillance Spyware Industry Needs Regulation https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance
[12]https://www.civicus.org/index.php/what-we-do/innovate/civicus-monitor
[13]https://monitor.civicus.org/Ratings/
[14]https://freedomhouse.org/explore-the-map?type=fiw&year=2021
[15]https://www.icnl.org/resources/civic-freedom-monitor

ETHIOPIA, UGANDA, AND ZIMBABWE: DATA PROTECTION CONTEXTS IN BRIEF

Ethiopia

The Constitution of Ethiopia provides for the right to privacy,[16]which relates to the privacy of a person and extends to their property as well as communications.[17]Public officials are obligated to respect and protect the right to privacy; however, there are limitations on the right in circumstances that relate to the safeguarding of national security or public peace, the prevention of crimes, or the protection of health, public morality, or the rights and freedoms of others.[18]As confirmed by ICNL, CIVICUS, and Freedom House reports, over the years, the government of Ethiopia has undertaken actions that undermine the protection of personal information and freedom of expression. For instance, Ethiopia has had recurrent country-and region-specific internet shutdowns.[19]Additionally, laws that purport to fight online misinformation and hate speeches have been promulgated with heavy penalties against offenders. [20]The response to the COVID-19 pandemic witnessed the adoption of laws banning the sharing of information that might cause terror and undue distress among the public.[21]Investment in online surveillance infrastructure enables stifling of online expression and unlawful access to personal information.[22]

The Ethiopian Ministry of Innovation, Science and Technology has tabled a draft data protection law, titled the Personal Data Protection Proclamation, before the House of People's Representatives. The law is modeled after the European General Data Protection Regulations (GDPR) and will, among other things, establish a data protection authority. Ethiopia's constitution states that the country is bound by all international agreements, including human rights conventions to which Ethiopia is a party state. Some of these international conventions, including the Universal Declaration of Human Rights, the International Covenant on Political and People's Rights, and the Convention on the Rights of the Child, call for protecting the right to privacy.

[16]Constitution of Ethiopia, 1994 https://www.constituteproject.org/constitution/Ethiopia_1994.pdf
[17]Art. 26(1); Art. 26(2)
[18]Art 26(2)
[19]https://www.hrw.org/world-report/2021/country-chapters/ethiopia#761225
[20]Freedom of the Net: Ethiopia 2020.
[21]Freedom of the Net; Ethiopia 2020.
[22]Ethiopia Ethiopia: New Spate of Abusive Surveillance
Spyware Industry Needs Regulation https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance

ETHIOPIA, UGANDA, AND ZIMBABWE: DATA PROTECTION CONTEXTS IN BRIEF

Uganda

Uganda's constitution protects fundamental rights and freedoms of its citizens. The political landscape of Uganda is dominated by a ruling party that has been in power since 1986. The interview participants noted that the current government has held onto power through the deployment of repressive state instruments, malicious prosecution and suffocation of Uganda's civil society, and independent media sectors through legal and extralegal harassment. For instance, laws such as the Regulation of Interception of Communications Act, the Anti-Terrorism Act, Uganda Communications Act of 2013, and the Computer Misuse Act are instrumentalized to undermine rights to free expression, privacy, and opinion. [23]Some of these laws have been used to shut down the Internet, block social media platforms,[24] or support procurement and installation of digital surveillance equipment.[25] In addition, these laws are "vague and ambiguous, and there is not oversight nor accountability mechanism of the intelligence agencies' carrying out surveillance risking personal information."[26]

Uganda's Data Protection Act came into effect in 2019. In March 2021, the Ugandan Data Protection and Privacy Regulations were published, which established a Personal Data Protection Office within the National Information Technology Authority-Uganda. The data protection authority is responsible of, among other things, providing guidance on generally accepted information security practices and industry-specific professional rules and regulations that promote the security of personal data.

[23]See reports CIPESA Uganda State of Internet 2021.
[24]Uganda Key Informant noted that Uganda Communications Commission (UCC) in 2011 and 2016 directed all service providers to temporarily block access to certain services which included Facebook and Twitter in fear of these social media networks being used to escalate opposition protests and spreading lies.
[25]Uganda the use of surveillance technologies; https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda;
[26]Uganda Key Informant

ETHIOPIA, UGANDA, AND ZIMBABWE: DATA PROTECTION CONTEXTS IN BRIEF

Zimbabwe

The Constitution of Zimbabwe also protects fundamental rights and freedoms, including the right to privacy. For 42 years, Zimbabwe has been under the rule of a dominating political party, which retained power through the manipulation of processes, violence, and selective application of the law, thereby curtailing fundamental rights and freedoms. Laws such as the Criminal Law Codification and Reform Act and the Interception of Communications Act have contributed to state-enabled and enhanced surveillance, infringing on data protection and privacy. These laws, as the key informants observed, allow for the arbitrary breach of individuals' privacy and communication without authorization from the judiciary. These, in an informant's words, "are signs of a country that has a closed civic space."

Furthermore, having laws allowing for arbitrary surveillance and collection of personal information contradicts and erodes media freedoms and freedom of expression and opinion.

The Zimbabwean Data Protection Act, which was passed in December 2021, establishes a data protection authority along with setting guidelines for processing personal information. Zimbabwe's data protection law has been in pipeline since 2013, and has since gone through several revisions. This data protection law was introduced after the repeal of the Access to Information and Protection of Privacy Act (AIPPA), an oppressive act that was instrumental in the crippling of Zimbabwe's independent media. The current government repealed the AIPPA to distance itself from the government regime led by Robert Mugabe.

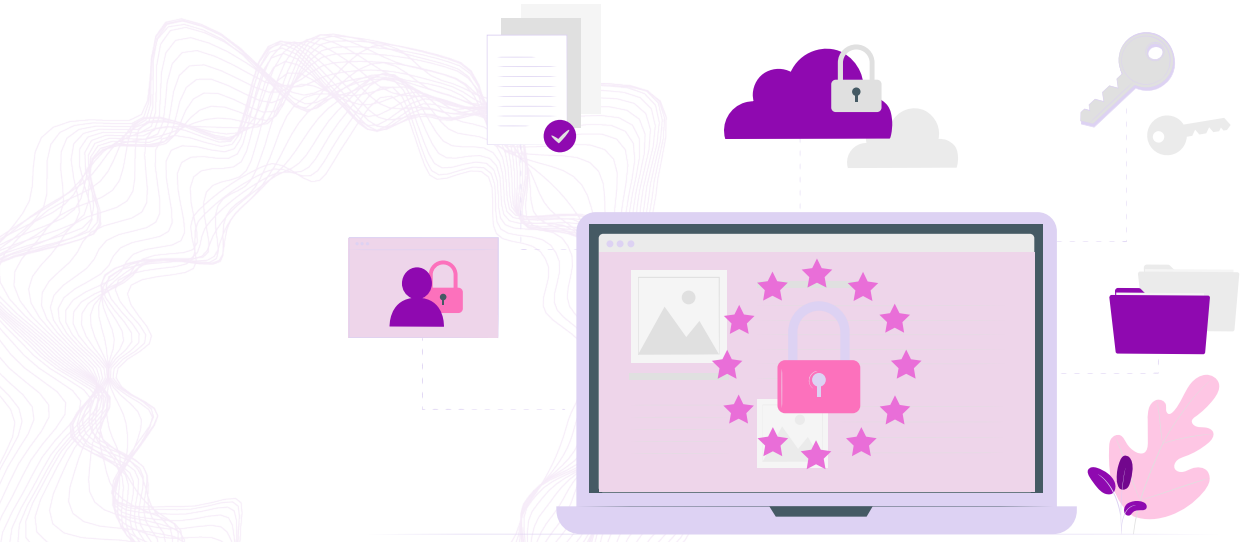
CONSIDERATIONS FOR PRIVACY ADVOCACY

Working in closed or repressive environments on data protection requires advocates and civil society to be considerate of the operational contexts and factors that inhibit the protection of online privacy and data privacy. There are correlations between repressive states and insufficient or weak data protection laws. For this report, we identified the following four core considerations from the interviews and secondary materials that advocates confront in these contexts.

- **How do** we conduct advocacy (specifically advocacy around privacy and data protection) in states with weak rules or laws?
- **What happens** when there are many laws that undermine existing or proposed privacy and data protection frameworks?
- **What can** advocates do when data protection laws are inadequate for protecting privacy rights and providing exemptions?
- **How do** advocates anticipate how data protection laws can be repurposed or weaponized by state actors?

This part of the paper focuses on the considerations faced by data protection advocates. These four considerations are by no means meant to serve as a comprehensive list of obstacles that hinder the introduction of adequate data protection laws in countries with repressed or closed civic spaces. The considerations discussed here are based on themes that emerged from the expert interviews. They also illustrate some of the ways in which politics and other factors can influence the data protection law-making process by either stalling the introduction of such laws or by permitting only the introduction of data protection laws that offer inadequate protection or can be easily used by a sitting government for its own preservation. This part of the paper not only highlights the challenges faced by data protection advocates but also provides insight into some of the solutions that these advocates have used in their fight for adequate data protection laws in Ethiopia, Uganda, and Zimbabwe.

Each consideration is discussed separately below, but the overlapping lessons learned in pushing back against these challenges are discussed together.



CONSIDERATIONS FOR PRIVACY ADVOCACY

How do we conduct advocacy (particularly advocacy focused on privacy and data protection) in states with weak rules or laws?

Challenges faced

Ethiopia,[27] Uganda,[28] and Zimbabwe,[29] respectively, have national constitutions in place. The right to privacy is expressly mentioned as a fundamental right that deserves protection in each country's constitution. All three countries have supreme constitutions, taking precedence over any law or practice. These constitutions, as demonstrated below, protect the rights to privacy.

In Ethiopia, Article 26 of the Constitution states that every person has the right to privacy, which relates to the privacy of the person and extends to their property (Art. 26(1)) and communications (Art. 26(2)). Public officials are obligated to respect and protect the right to privacy in terms of Art. 26(3) of the Constitution. Art. 26(2) of the Constitution provides for the restriction of the right to privacy in circumstances that relate to "the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others."

In Uganda, protection for the right to privacy is found in Article 27 of the country's constitution. Again, the right is comprehensive, covering both the privacy of a person and that of their property. Art. 27(2) extends the exercise of the right to privacy to a person's communications as well.

Similarly, Zimbabwe's constitution protects the right to privacy, as set out in Article 57. Art. 57 is comprehensive and clear in setting out the right to privacy, which includes the right to not have a person's health information shared without their consent as well as the privacy of a person's communications. In contexts where constitutionalism and the rule of law are respected, the fact that the right to privacy is protected in the constitution is enough to ensure that privacy is respected through both adequate laws and policies as well as implementation. However, in repressive and closed contexts, such as those in Ethiopia, Uganda, and Zimbabwe, the constitutional guarantee of privacy is undermined by a litany of laws that promote state-sponsored surveillance, excessive processing of personal data, and general impunity against privacy-related violations. As has been repeatedly shown by reports from CIVICUS, Freedom House, and ICNL, countries with repressive and closed civic spaces are under the control of governments that do not care to observe laws or constitutional provisions.

The dismissal of the court case on the abuse of voter information in Zimbabwe[30] is one example among many that shows general state impunity when it comes to the respect of the rule of law and for individual fundamental rights. Examples of state impunity are manifold in Ethiopia, where the government has arbitrarily detained and arrested individuals,[31] journalists, and political actors without any charge.[32]

---

[27] Constitution of Ethiopia, 1994 https://www.constituteproject.org/constitution/Ethiopia_1994.pdf
[28] Constitution of Uganda, 1995 https://www.constituteproject.org/constitution/Uganda_2005.pdf
[29] Constitution of Zimbabwe, 2013 https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf
[30] https://www.newsday.co.zw/2018/07/lawyer-drags-zec-zanu-pf-econet-to-court/
[31] https://ethiopia.un.org/en/128792-un-condemns-arbitrary-and-brutal-arrest-least-200-idps-military-led-raids-shire-town-tigray
[32] https://www.humanrightsleague.org/?p=16544

In the country's Tigray region, there has been a prolonged telecommunication blackout, along with reports of state-sponsored ethnic profiling, war crimes, and genocide.[33] This is all happening, even though Ethiopia has a constitution that is strongly against such acts.

In summary, the three countries have supreme constitutional provisions protecting fundamental rights to privacy; moreover, these constitutions are binding on all state and private actors. In open civic spaces, adequate data protection laws and policies build on constitutional frameworks. However, in closed contexts, as in these three countries, the constitutional guarantee of privacy is undermined by a litany of laws that promote state-sponsored surveillance, excessive processing of personal data, and general impunity against privacy-related violations. The government narrative in these three countries, as well as other countries that have similar repressive and closed civic spaces, is that national security is a justifiable reason to undertake mass surveillance activities. Clearly, national security and the mass surveillance it enables are used to repress the exercise of civil liberties[34] and to keep the ruling parties in power.

What happens when there are many laws that undermine existing or proposed privacy and data protection frameworks?

Challenges faced

Advocating for data protection policies and laws does not only mean pushing for the drafting and introduction of such policies and laws. Advocacy efforts must also involve calls for the adequate amendment or removal of existing laws that restrict the exercise of the right to privacy.

Above all, legislative reforms would not be complete if they do not include measures which ensure that bodies tasked with enforcing and overseeing the enforcement of the law are independent, adequately funded, and staffed with competent officers.

In Ethiopia, laws such as the Anti-Terrorism Proclamation No. 652/2009 are passed for one purpose, which in this instance is to prevent acts of terrorism by intercepting the communications of suspected terrorists. However, in practice, this law has been used by the Ethiopian ruling party to undertake surveillance on the phones and computers of its perceived opponents.[35] The Electronic Signature Law provides the widest mandate to the Ethiopian Information Network Security Agency (EINSA), a body that has been in the forefront of surveillance, tapping and intercepting citizens' communications. All electronic signatures, electronic encryption, and route authorities are certified by EINSA. This is provided for by the data protection proclamation, but in practice, the certification is performed by the government intelligence unit. The Regulation of Interception of Communications Act in Uganda[36] and the Interception of Communications Act in Zimbabwe[37] are abused by governments to carry out surveillance of political and civil society actors that are of interest.

The continued existence of Zimbabwe's Interception of Communications Act allows arbitrary breaches of individuals' privacy and communication without any effective judicial oversight. The interview participants from both Uganda and Zimbabwe highlighted that these countries' governments used national security as a justification for introducing and maintaining communication surveillance laws.

[33] https://www.latimes.com/world-nation/story/2021-08-11/amnesty-reports-widespread-rapes-with-impunity-in-tigray
[34] https://carnegieendowment.org/2017/05/18/surveillance-and-state-control-in-ethiopia-pub-69960
[35] https://giswatch.org/en/country-report/communications-surveillance/ethiopia
[36] http://www.ulrc.go.ug/content/regulation-interception-communications-act-2010
[37] http://www.veritaszim.net/node/252

The term national security is often not clearly defined, and when it is defined, the definition is wide enough to fit any measures the respective ruling party might deem necessary to keep its hold on power. The government narrative in these three countries, as well as other countries that have similar repressive and closed civic spaces, is that national security is a justifiable reason to undertake mass surveillance activities. Clearly, national security and the mass surveillance it enables are used to repress the exercise of civil liberties[38] and to keep the ruling parties in power.

In turn, state-sponsored surveillance plays a role in enabling targeted arbitrary arrests, abductions, detentions, and general harassment of opposition political figures and civil society actors who are perceived as enemies of the government.[39]

Furthermore, unaccountable surveillance infrastructure enabled by broad and vague laws facilitates access to data in the name of public interest or national security. This allows for invasive data practices through the surveillance infrastructure, targeting institutions and human rights groups that can be easily punished for data externalization. In worst cases, data privacy enhancing technologies will be criminalized with the intention of compelling data accessibility.

[38]https://carnegieendowment.org/2017/05/18/surveillance-and-state-control-in-ethiopia-pub-69960
[39]The chilling effects of surveillance on freedom of expression, not yet published

CONSIDERATIONS FOR PRIVACY ADVOCACY

What can advocates do when data protection laws are inadequate for protecting privacy rights and provide exemptions?

Challenges faced

Most governments are implementing data protection laws for protecting potential commercial interests and not for advancing a human rights agenda. This is supported by the continued existence of other laws that hinder data protection but that are not amended or repealed when data protection laws are passed. In fact, the passage of data protection laws is intended to enhance the ability of these laws to stifle other fundamental freedoms and rights.

This is usually the case in situations where a government will pass a data protection law that does not comprehensively protect the right to privacy, as it might contain exemptions and clawback provisions that undermine the very right to privacy that data protection is supposed to promote and protect. One reason why a state might decide to pass a data protection law relates to the financial benefits of data protection frameworks.

Countries with suitable data protection laws are more likely to be considered good business jurisdictions, which is why, for example, countries such as the United States of America work to meet the standards set by the European Union's GDPR. In this instance, the introduction of the data protection law will be for the purpose of aligning the country with other financially beneficial countries. Similarly, pressure from the international community might push states to introduce privacy and data protection frameworks. For example, access to international development funding or lines of credit is conditional on the presence of data protection laws.

In Zimbabwe, the passage of the Data Protection Act amended sections of the Interception of Communications Act and the Criminal Law Codification Reform Act, making these two laws even more restrictive in terms of rights and consolidation of state intrusive powers. Another critical component of data protection is the presence of an independent data protection authority capable of holding government, public, and private actors accountable. The proposed data protection authority in Zimbabwe is not independent and is vested in the presidency. This, according to the key informants, gives the state wide-ranging powers to invade people's privacy through the authority and to particularly surveil the "targets of interest."

The problem with the introduction of data protection laws that contain large carve outs/exemptions and data protection laws for promoting a country's business standing is that human right-centered privacy loses out in the process. Ideally, a data protection law must first protect the right to privacy, with financial benefits flowing from there. Ideally, civil society groups and groups focused on privacy and human rights can provide input to these policies during the law-making and drafting process. However, the interview participants from all three countries indicated that it was difficult to engage their respective governments on the issue of data protection laws because their governments were either not accessible due to a lack of public engagement platforms during the law-making process or because the governments were not interested in acting on the contributions/recommendations made by civil society and non-governmental stakeholders.

CONSIDERATIONS FOR PRIVACY ADVOCACY

How do advocates anticipate how data protection laws can be repurposed or weaponized by state actors?

Challenges faced

The introduction of China's Personal Information Protection Law has raised concerns about the repurposing of data protection laws by state actors. None of the participants we interviewed believed that China's data protection law would have an immediate influence on the shaping or interpretation of data protection laws in Ethiopia, Uganda, and Zimbabwe. However, all of them were worried that Chinese law provides a false sense of security that can be used to justify the transfer of personal information from African jurisdictions to China. According to 2018 media reports, China and Zimbabwe reached an agreement that would see Zimbabwe transferring biometric information to China as part of the acquisition of facial recognition technologies.[40]

Closed regimes and states have the capacity to weaponize the law (i.e., use existing laws to stifle fundamental freedoms and rights). For example, some countries have widely framed vague laws, which include the so-called miscellaneous offences covering everything marginally considered an irritation.[41] Data protection laws are not immune to such abuses, and they are likely to, in some instances, be invoked and justified as part of national efforts but then be actually used to undermine the exercise of, for example, access to information rights.

The most evident weaponization of data protection laws is the use of data localizations to enhance data privacy. Data localization theories have been embraced in countries, including open societies, under the mistaken belief that such measures realize economic returns,[42] safeguard data integrity, and advance national interests. These arguments have mixed value, as extreme data localization results in the closure of space, criminalization of free speech, and access to information advocates. The free flow of information is essential to advancing national and global democratic governance.

Despite the proliferation of data localization regulations, there are higher risks of these laws being used to hide information, reduce government transparency, or arrest data advocates for breaching these practices. Data localization regulations are an extension of national security practices, the same as those used to undermine fundamental rights and freedoms. The discussion on data localization requires data advocates to work with progressive countries and block setting norms to devise a human right-responsive data localization framework.

The restriction of data transfer must be resisted if it incorporates vague categories of data banned from transfer, such as sensitive or related to national security. These terms require unpacking, especially in closed regimes. If certain types of data are restricted from transfer, oversight mechanisms should be in place. Finally, while transfers might be allowed in law, the complicated processes and practices might deter transfers (e.g., transfers only after approval from the data protection authority, which compels domestic storage). Data advocates must be aware of the different forms of data localization trends that inhibit the full enjoyment of data privacy and protection.

---

[40]https://www.biometricupdate.com/201805/implementation-of-cloudwalk-facial-recognition-technology-in-zimbabwe-progressing-in-stages

[41]Miscellaneous Offences Act was on the statute books of Zimbabwe for decades and it covered every offence or conduct that the government felt was unacceptable or unbecoming conduct, a protestor could be arrested for blocking a pavement, even if they were arrested while walking. In a similar way, Uganda has the Miscellaneous Offences (Public Order and Nuisance) Act 1906

[42]There is evidence from groups such as OECD that data localization does not result in economic growth as the internet becomes more inaccessible and costly. López González, J. and J. Ferencz (2018), "Digital Trade and Market Openness", OECD Trade Policy Papers, No. 217, OECD Publishing, Paris, https://doi.org/10.1787/1bd89c9a-en.

BEST PRACTICES AND RECOMMENDATIONS TO ADVOCATES

The considerations that data protection advocates might incorporate as they navigate reform and the protection of privacy in closed civic spaces are varied and unique. These contexts require continuous reflection and flexibility in approach, as well as creativity and longer-term time horizons and strategic planning. Below, we outline a few key best practices distilled from the expert interviews.

Strategic litigation

Some advocates might deploy lawfare in response to increased use of laws to undermine fundamental rights and freedoms of expression and opinion—which, as evidenced in this advocacy guide, are intricately connected to data privacy.

The lack of legitimate access to government and the policy-making process meant that data protection advocates had to use alternative platforms to raise awareness about the need for adequate data protection laws. One such platform that has been used is strategic litigation to promote the right to privacy. Speaking about their experience in Ethiopia, one activist had the following to say about strategic litigation in that country:

Litigation in local and regional courts is another strategy that activists can employ to try and demand as well as make the right to data protection and privacy a "real issue."

Strategic litigation is seen as a tool to challenge unconstitutional government behavior and laws. The use of targeted litigation can be useful in indicating the harms that are experienced in the absence of a data protection law, as was the case in Zimbabwe when the government was taken to court for sending unsolicited messages[43] and when the ruling party was sued for sending unsolicited, targeted SMSs to registered voters. Strategic litigation can also be useful in strengthening inadequate parts of existing data protection laws, as has been the case in progressive jurisdictions, such as South Africa.

Strategic litigation can be conducted in the public interest in the form of private prosecution of individuals infringing on peoples' rights to privacy. It can also be used in combination with legal and policy analyses of the relevant sections of the laws that affect data protection. Legal and policy analysis is useful in identifying unconstitutional laws that must be aligned with what each respective constitution says about the right to privacy.

Data protection activists have warned that the effectiveness of strategic litigation decreases because of the lack of judicial independence in Ethiopia, Uganda, and Zimbabwe. There was an agreement, though, that court challenges against the governments were useful in raising awareness about, for example, the need to align existing laws with constitutional provisions on privacy and to ensure that any data protection laws are also in line with the constitution.

[43] https://www.newsday.co.zw/2021/02/econet-loses-covid-19-messages-lawsuit/

Public awareness raising

Activists in Uganda have found the use of social media and press conferences as another good way to raise awareness of the hurdles they face in their work on advocating data protection laws. This includes using these platforms to discuss the violations of the right to privacy. This is part of the broader efforts made to increase citizen awareness of the importance of the right to privacy and the need for adequate data protection frameworks. The interview participants in all three countries agreed that citizens have a role to play in pressuring their respective governments to introduce adequate data protection laws. Only an informed citizenry can hold the government accountable for violations of the right to privacy. This is closely linked to the use of media campaigns that highlight the importance of data protection frameworks. The media campaigns were said to be a good way of sustaining pressure on governments while teaching citizens about the importance of such frameworks. The framing of the media content might be based on the issues data protection advocates seek to raise with the duty bearers, as well as when empowering the rights holders on key issues.

The repurposing of laws or their selective application is not new. With newer threats to political elites and power retention, new laws will be adopted. Data advocates must anticipate these changes throughout the legal reform agenda and indicate the possible scenarios and deployment of the law for other purposes. These scenarios must be widely publicized as a pre-emptive approach and use examples from other regions or countries to demonstrate trends and patterns.

Promoting horizontal accountability

While still on the point of civil society's role in civilian education and awareness raising, some interview participants highlighted the need for members of the judiciary to be trained on the right to privacy and the need for adequate data protection frameworks. This stems from the observation that there are very few judgments on the right to privacy or data protection from the courts in Ethiopia, Uganda, and Zimbabwe. In Zimbabwe, a main judgment that has explored the meaning of the constitutional right to privacy is a murder case hearing[44] in which the judge made remarks on the right as part of the case. Otherwise, there is no judgment yet that has appropriately explored what the right to privacy is and what it looks like in day-to-day life. If the judiciary were more knowledgeable about the right to privacy, they would be better positioned to better defend the right.

In instances with an insufficient national protection framework for data, advocates can consider raising the political and legal cost of inadequate frameworks through regional and continental engagements. African countries are concerned about the ease of doing business and the ability to raise revenue and develop economies reliant on technology, of which data protection is essential. One interview participant highlighted the importance of gathering evidence of human rights violations, including infringements on the right to privacy. If there are several laws that undermine the proposed privacy and data protection frameworks, data advocates might consider conducting wide privacy impact assessments and regulatory impact assessments, looking at the specifics of each law and how it will erode the proposed positive data protection laws and render the country unsafe for data processing.

This collected information would then be used to escalate calls for adequate data protection frameworks to relevant regional forums and platforms. This is usually in the form of transnational courts, such as the East African Court on Human and People's Rights, or economic blocs, such as the Southern African Development Community. These regional platforms were said to be important when the local court and parliamentary processes had been exhausted. Advocating data protection laws at the economic bloc level might be more successful when advocates indicate the economic advantages that countries with adequate data protection frameworks have over those that do not have such frameworks. For example, European Union countries are less likely to trade with countries that do not have adequate data protection frameworks in place.

[44] S v Nsoro (HH 190-16 CRB 57/16) https://old.zimlii.org/node/7107

Coalition building

In countries that have a weak rule or law and weak protection of fundamental rights, such as Uganda, Zimbabwe, and Ethiopia, data protection advocates must consider engaging and building allies and movements focusing on advancing the wider rights conversations. This might help demonstrate the connectivity and linkages of rights, rather than the pursuit of a single frame issue. However, combining issues and coalescing on wider reforms might not result in comprehensive data protection; in these instances, data advocates should consider a phased approach and targeted advocacy.

Several interview participants noted the need to build coalitions, including academia, lawyers, civil society, and allies in legislative bodies. To this list of stakeholders, we would add business stakeholders who are interested in data protection frameworks because of the advantage they present for conducting business with other jurisdictions. Data advocates might consider indicating the financial costs of insufficient data protection laws and impact on the economy. This might work in countries that are experiencing economic decline or instability; this criterion is met by the three case studies. However, stable economies might not be moved by economic arguments, especially if the free flow of data or technology is not one of their major economic means of production.

In building allies and partnerships, data advocates might consider working with unusual groups and voices. This will assist in building momentum and galvanizing sectors historically not concerned with data protection; for instance, consumer interest and consumer associations significantly influence regulatory agencies and institutions. They also have international reputes as neutral and non-political or partisan bastions of consumer interests.

Multistakeholder and diverse coalitions are equipped to carry out an analysis of a country's data protection needs and to jointly come up with co-created policy recommendations and solutions that cater to the needs of not just the government but a diverse range of stakeholders that stand to benefit from the existence of adequate data protection frameworks.

CONCLUSION

It is difficult to predict each challenge that data protection advocates will encounter in their efforts to introduce data protection laws or to improve existing data protection laws in a way that adequately protects the right to privacy, especially in restrictive contexts where advocacy is complicated and requires additional flexibility, creativity, strategy, and patience. This paper provides some ideas and tools that can be used to leverage efforts to advocate data protection frameworks. In Uganda and Zimbabwe, where data protection laws have been introduced, it took a combination of methods to get the government to a point where it was willing to draft a data protection law. These efforts, mainly driven by civil society, would not have been possible without the collaboration of other stakeholders, such as business and other non-governmental entities.

The efforts of data protection advocates in Uganda and Zimbabwe continue as there is still room to improve the quality of both laws. In particular, there is a need to influence the way governments in both these countries will staff and maintain the regulatory and oversight bodies established by each country's data protection law. The same goes for the need for continued cooperation on the drafting and rolling of regulations and policies that are required to give full effect to data protection laws.

APPENDIX

CIVICUS Monitor: Tracking civic space

The CIVICUS Monitor[45] is a research tool that provides close-to-real-time data on the state of civil society and civic freedoms in 196 countries.[46] The data used in this research tool are compiled from the information gathered by 20 civil society research partners along with input from several independent human rights evaluations. Under this methodology, countries' civil spaces are rated as closed, repressed, obstructed, narrowed, or open.[47]

- **Closed:** According to CIVICUS,[48] a civic space is considered closed when "an atmosphere of fear and violence prevails, where state and powerful non-state actors are routinely allowed to imprison, seriously injure and kill people with impunity for attempting to exercise their rights to associate, peacefully assemble and express themselves."

- **Repressed:** A repressed civic space refers to an environment in which "active individuals and civil society members who criticise power holders risk surveillance, harassment, intimidation, imprisonment, injury and death."[49] Repressive civic spaces are also characterized by internet shutdowns, a biased state media, and civil society organizations that are restricted in their work.

- **Obstructed:** Obstructed environments often allow for peaceful protests and assembly but are usually broken up by law enforcement agencies that use excessive force, including rubber bullets, tear gas, and baton charges. Civil society organizations exist, but are often undermined by state authorities, including by illegal surveillance, bureaucratic harassment, and demeaning public statements.

- **Narrowed:** In narrowed environments, there is an opportunity to exercise fundamental freedoms, although violations of these rights take place. The full exercise of these rights is impeded by occasional harassment arrests or assault of people deemed critical of those in power. "Protests are conducted peacefully, although authorities sometimes deny permission, citing security concerns, and excessive force, which may include tear gas and rubber bullets, are sometimes used against peaceful demonstrators."

- **Open:** Countries are considered to have an open civic space when "the state both enables and safeguards the enjoyment of civic space for all people. Levels of fear are low as citizens are free to form associations, demonstrate in public places and receive and impart information without restrictions in law or practice." Additionally, "there is a free media, online content is uncensored, and citizens can access government information easily."

Figure 1: CIVICUS Monitor conceptualization of civic space[50]

[45]https://monitor.civicus.org/
[46]https://www.civicus.org/index.php/what-we-do/innovate/civicus-monitor
[47]Ibid.
[48]https://monitor.civicus.org/Ratings/
[49]https://monitor.civicus.org/Ratings
[50]Monitor Methodology Paper, https://civicus.org/documents/civicus-monitor-methodology-paper.pdf

According to the CIVICUS, a civic space is defined as respect in policy and practice for the freedoms of association, peaceful assembly, and expression. The state's duty to protect each of these rights is also assessed, along with the protective measures afforded to a country's civil society.

Each country's performance under each of these four sectors is rated from 0 to 5, where 0 is the lowest score, indicating a lack of respect for the respective right, and 5 indicates a situation in which the right is respected and strongly promoted.

Freedom House: Freedom of the World
Freedom House produces an annual Freedom in the World report, which is described as an annual global report on political rights and civil liberties. The Freedom in the World report uses a two-tiered system comprising scores and status. The scores are based on responses to questions that assess 10 political right indicators and 15 civil liberty indicators. The scores for these questions are then converted to status.

The political category questions are grouped into three subcategories: Electoral Process (3 questions), Political Pluralism and Participation (4 questions), and Functioning of Government (3 questions). The civil liberties questions are grouped into four subcategories: Freedom of Expression and Belief (4 questions), Associational and Organizational Rights (3 questions), Rule of Law (4 questions), and Personal Autonomy and Individual Rights (4 questions).

The response to each question is given a score between 0 and 4, with 0 representing the strongest restriction of a right and 4 representing the ability to enjoy a right freely. The combination of the overall score awarded for political rights and that awarded for civil liberties, after being equally weighted, determines the status of Free, Partly Free or Not Free.

ICNL: Civic Freedom Monitor

Civic Freedom Monitor is the third methodology considered in this study. According to ICNL, its Civic Freedom Monitor provides up-to-date information on legal issues affecting civil society and civic freedoms, including freedoms of association, expression, and peaceful assembly. Of relevance to this paper is that the Civic Freedom Monitor contains regularly updated reports on 55 countries as well as archived reports on 3 countries. Each country report provides an overview of key legal issues related to civic freedom, with a focus on legal barriers to civil society activity.

Unlike the CIVICUS Monitor and the Freedom of the World report, ICNL's Civil Freedom Monitor does not give any scores but only outlines and analyses the different legal issues and developments that affect the enjoyment of fundamental rights as well as the activities of civil society.

[51]Monitor Methodology Paper, https://civicus.org/documents/civicus-monitor-methodology-paper.pdf
[52]Ibid.
[53]https://freedomhouse.org/reports/freedom-world/freedom-world-research-methodology
[54]https://freedomhouse.org/reports/freedom-world/freedom-world-research-methodology
[55]https://www.icnl.org/resources/civic-freedom-monitor
[56]Ibid.

CONTACT INFO

DIGITALRIGHTS@INTERNEWS.ORG