The Right to Privacy in Zimbabwe

Stakeholder Report

Universal Periodic Review

26th Session - Zimbabwe

Submitted by the Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the

International Human Rights Clinic at Harvard Law School, and Privacy International

March 2016

Introduction

1. This Universal Periodic Review (UPR) stakeholder report is a submission by **Privacy International** (PI), the **International Human Rights Clinic at Harvard Law School** (IHRC), the **Zimbabwe Human Rights NGO Forum** (the Forum), and the **Digital Society of Zimbabwe** (DSZ).

    - **PI** is a human rights organisation that works to advance and promote the right to privacy around the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.
    - The **IHRC** seeks to protect and promote human rights and international humanitarian law through documentation; legal, factual, and strategic analysis; litigation before national, regional, and international bodies; treaty negotiations; and policy and advocacy initiatives. The IHRC works to protect the human rights of clients and communities around the world; through supervised practice, Harvard Law School students learn the responsibilities and skills of human rights lawyering.
    - The **Forum** is a coalition of 21 human rights non-governmental organisations (NGOs) in Zimbabwe. Its mission is to provide leadership and coordination for the human rights agenda in Zimbabwe.
    - The **DSZ** is a network of voluntary digital security trainers, information technology professionals, and privacy advocates working to empower Zimbabwean activists, human rights defenders, and everyday internet users to become more resilient and secure in their use of digital tools online and offline, through capacity building assistance, technical support, and knowledge sharing.

2. Together **PI**, the **IHRC**, the **Forum**, and the **DSZ** wish to bring their concerns about the protection and promotion of the right to privacy in Zimbabwe before the Human Rights Council for consideration in Zimbabwe's upcoming review. This stakeholder report highlights five areas of concern:

- The Interception of Communications Act 2007, primary legislation that governs communications surveillance, fails to abide by international human rights standards, such as the requirement that a competent judicial authority makes determinations about communications surveillance.
- Mandatory registration of all SIM cards and the establishment of a database containing information about users of mobile phone services are measures that contravene international human rights standards on the right to privacy because they are neither necessary to achieve a legitimate aim nor proportionate to the aim pursued.
- Intelligence agencies conduct surveillance and largely operate beyond the law, in violation of international human rights standards.
- Criminal penalties for certain types of speech unjustifiably limit the right to privacy.
- No data protection legislation exists and the new legislation proposed in this area threatens to put in place an ineffective data protection regime.

3. In its resolution on the right to privacy in the digital age, adopted by consensus on 18 December 2014, the United Nations (UN) General Assembly called on all states "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law."[1] The UPR offers a significant opportunity for states to demonstrate that they are implementing this recommendation, by systematically reviewing states' compliance with their obligations to respect and protect the right to privacy. In the first UPR cycle, there was no mention of the right to privacy in Zimbabwe's National Report or the Working Group report.[2]

[1] "The right to privacy in the digital age," UN General Assembly Resolution, A/RES/69/166 (18 December 2014). The same language appears in a similar resolution passed in the 2013 General Assembly session: "The right to privacy in the digital age," UN General Assembly Resolution, A/RES/68/167 (18 December 2013).

[2] *National report submitted in accordance with paragraph 15 (a) of the annex to Human Rights Council resolution 5/1, Zimbabwe*, 2011, A/HRC/WG.6/12/ZWE/1; *Report of the Working Group on the Universal Periodic Review, Zimbabwe*, December 2011, A/HRC/19/14. In particular, members of the Working Group raised freedom of assembly, association, and expression concerns about the Public Order and Security Act and the Access to Information and Protection of Privacy Act.

The Right to Privacy

4. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[3] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals.[4] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[5]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing, and sharing personal data, the right to privacy has evolved to encapsulate state obligations related to the protection of personal data.[6] A number of international instruments enshrine data protection principles, and many domestic legislatures have incorporated such principles into national law.[7]

---

[3] *Universal Declaration of Human Rights*, art 12; *United Nations Convention on Migrant Workers,* art 14; *Convention on the Rights of the Child*, art 16; *International Covenant on Civil and Political Rights,* art 17; *African Charter on the Rights and Welfare of the Child*, art 10; *American Convention on Human Rights*, art 11; *African Union Principles on Freedom of Expression*, art 4; *American Declaration of the Rights and Duties of Man*, art 5; *Arab Charter on Human Rights*, art 21; *European Convention for the Protection of Human Rights and Fundamental Freedoms*, art 8; *Johannesburg Principles on National Security, Free Expression and Access to Information*; *Camden Principles on Freedom of Expression and Equality*.

[4] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, *Martin Scheinin,* 2009, A/HRC/17/34.

[5] See *Universal Declaration of Human Rights*, art 29; Human Rights Committee, *General Comment No. 27: Article 12 (Freedom of Movement),* 2 November 1999, CCPR/C/21/Rev.1/Add.9; Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988; see also, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, *Martin Scheinin* 2009.

[6] Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy).*

[7] See the *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*; *Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*; *Guidelines for the regulation of computerized personal data files* (UN General Assembly Resolution 45/95 and E/CN.4/1990/72). As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, *National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map*, 8 December 2014, available at http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

Domestic Law on Privacy

6. Zimbabwe's constitution, enacted into law in 2013 after a referendum, explicitly recognises the right to privacy. Section 57 provides:

> Every person has the right to privacy, which includes the right not to have
> (a) their home, premises or property entered without their permission;
> (b) their person, home, premises or property searched;
> (c) their possessions seized;
> (d) the privacy of their communications infringed; or
> (e) their health condition disclosed.

7. Despite constitutional recognition of the right to privacy and Zimbabwe's international obligations to uphold the right to privacy, few protections for privacy exist in Zimbabwe's domestic law.[8] Although in 2002 Zimbabwe enacted the "Access to Information and Protection of Privacy Act," the Act's title is a misnomer, as it does not serve to protect privacy, but instead allows the government to control aspects of the media, through measures such as the accreditation of journalists.[9] Zimbabwe lacks data protection legislation and does not have a data protection authority to investigate breaches of data protection principles and order redress.

8. As a general matter, Human Rights Watch has noted, "[In 2015, President Robert] Mugabe's government continued to ignore human rights provisions in the country's 2013 constitution, neither enacting laws to put the constitution into effect nor amending existing laws to bring them in line with the constitution and Zimbabwe's

[8] Zimbabwe is a party to the *International Covenant on Civil and Political Rights* (ICCPR), which protects the right to privacy: Article 17 provides "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]." Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)*, para 1.

[9] Access to Information and Protection of Privacy Act [Chapter 10:27]. For concerns about the Act, see Article 19 and the Media Initiative of Southern Africa – Zimbabwe, *Access to Information and Protection of Privacy Act: Two years On*, 2004, available at https://www.article19.org/data/files/pdfs/publications/zimbabwe-aippa-report.pdf.

international and regional human rights obligations."[10] Based on surveys to assess how the general public experiences the rule of law, the World Justice Project Rule of Law Index 2015 ranked Zimbabwe 100th of 102 countries.[11]

Areas of Concern

Interception of Communications Act

9. The Interception of Communications Act sets out the legal basis for state authorities to conduct communications surveillance.[12] Little information about how authorities apply and interpret the Act is publicly available; nonetheless, there are problems with the legislation itself as well as rule of law concerns that have implications for the right to privacy. The Act was enacted in 2007 and has not yet been revised to bring it into line with the 2013 constitution: the 2013 constitution protects the right to privacy, but the previous constitution did not.[13]

10. Five aspects of the legislation raise specific concerns with regards to international human rights standards:

- Authorities may obtain warrants to intercept private communications through a process that is controlled by members of the executive and not subject to independent scrutiny and oversight, whether from a judicial or other monitoring body or the public.
- The Act does not require authorities to notify individuals that they are or have been subject to surveillance and there are insufficient avenues for victims of unlawful surveillance to seek redress.
- The Act places wide-ranging duties on telecommunications providers to facilitate state surveillance.
- Key terms in the Act, such as "monitoring," are not clearly defined, opening the door to abuse, especially in relation to the collection and analysis of metadata.

[10] Human Rights Watch, *World Report 2016*, 2016, available at https://www.hrw.org/world-report/2016/country-chapters/zimbabwe.
[11] *World Justice Project Rule of Law Index 2015,* available at http://worldjusticeproject.org/rule-of-law-index.
[12] Interception of Communications Act [Chapter 11:20].
[13] Article 17 ("Protection from arbitrary search and entry") of the previous constitution (known as the "Lancaster Constitution") did, however, contain minimal privacy protections.

- The Act has been used by government authorities to restrict access to encrypted services that allow people to communicate privately.

Warrant regime

11. The Interception of Communications Act "provide[s] for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunications, postal or any other related service system."[14] The Act defines "intercept" as "to listen to, record, or copy, whether in whole or in part" communications sent through telecommunications or radio systems and "to read or copy the contents" of communications sent by post.[15] Intercepting a communication without a warrant or the consent of at least one of parties to the communication is an offence punishable by a fine or imprisonment of up to five years.[16]

12. The Act authorises four senior officials (or their nominees), representing police, intelligence, national security, and tax interests, to individually make applications for warrants of interception.[17] An application must include information such as the name of the target of the surveillance (if known), the basis on which the warrant is sought, facts to support the application, and information on whether other means of investigation have been pursued.[18] Under the Act, applications are submitted to the Minister of Transport and Communications or "any other Minister to whom the President may from time to time assign the administration of [the] act," who is the only official with the power to issue a warrant of interception.[19] Grounds for issuing a warrant relate to the commission of crimes and threats to national security, public safety, or national economic interest. Warrants are initially valid for three months, but can be renewed.

13. Under international human rights standards articulated in the *International Principles on the Application of Human Rights to Communications Surveillance*, determinations

[14] Interception of Communications Act, long title.
[15] Ibid, s 2(2).
[16] Ibid, s 3(3).
[17] Ibid, s 5(1): the Chief of Defence Intelligence, the Director General of National Security, the Commissioner of the Zimbabwe Republic Police, and the Commissioner General of the Zimbabwe Revenue Authority.
[18] Ibid, s 5(3).
[19] Ibid, ss 2(2) and 6.

concerning communications surveillance must be made by a competent judicial authority that is independent and impartial.[20] The Act violates these standards because the warrant regime is controlled by members of the executive and precludes independent and impartial judicial scrutiny. In 2014, using powers granted to him under the constitution, President Mugabe assigned the Act's administration to the Office of the President and Cabinet (OPC). The OPC has thus been performing the functions that the Act allocates to the Minister of Transport and Communications, such as issuing warrants of interception.[21] There is no public information on how these functions are exercised in practice within the OPC, which is an executive body led by the President and the Head of the Civil Service.[22] For ease of reference, this section uses the Act's terminology of "Minister" to refer to functions that are currently assigned to the OPC.

14. The Minister is the sole arbiter of whether the grounds for a warrant are met and determines the warrant's duration, up to a period of three months.[23] Before a warrant expires, or within six months of its expiry, the Minister may renew a warrant for an additional three month period "for good cause shown by [the applicant]", a vague term whose interpretation is left to the Minister.[24] In some circumstances (when the warrant relates to a particular limited set of crimes), the Minister must consult the Prosecutor-General about the renewal; there is no requirement that the Prosecutor-General consent to the renewal, only that he is consulted.[25] Under the constitution, the Prosecutor-General is an independent and non-partisan office, whose holder is

[20] See "Competent Judicial Authority," *International Principles on the Application of Human Rights to Communications Surveillance*, 2014, available at https://en.necessaryandproportionate.org/. The *International Principles* were developed by a range of civil society groups, as well as industry and international experts in communications surveillance law, policy, and technology. They "provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights." *International Principles on the Application of Human Rights to Communications Surveillance*.
[21] Statutory Instrument 19 of 2014, Assignment of Functions (Office of the President and Cabinet). The Statutory Instrument states that functions were assigned "in terms of s 104(1) of the Constitution, as read with s 37(2) of the Interpretation Act."
[22] See "Office of the President and Cabinet," available at http://www.opc.gov.zw/.
[23] Interception of Communications Act, s 7(1).
[24] Ibid, s 7(2).
[25] Ibid, s 7(1). The Act itself specifies the Attorney-General must be consulted, but following the 2013 constitution, functions that were assigned to the Attorney-General are now the responsibility of the Prosecutor-General.

appointed in the same way judges are appointed.[26] In February 2016, the incumbent Prosecutor-General was arrested on charges that appear politically motivated.[27]

15. Judicial authorities become involved in the interception warrant regime only if officials seek a second renewal for a warrant relating to certain crimes (such as murder) or a third renewal for a warrant relating to all other grounds. At that point, the Administrative Court, a statutory court that deals with matters such as liquor licensing and administrative decisions by local authorities, may renew the warrant for periods of up to three months.[28] The Act contains no limit on the number of times the Administrative Court may renew a warrant.

16. The Administrative Court operates in an environment where judicial independence may be difficult to maintain. Although Zimbabwe's Constitution contains protections for judicial independence, judges have been subject to intimidation and pressure from political actors: for example, in March 2015, the International Bar Association's Human Rights Institute condemned comments made by President Mugabe about a case brought by two former members of the ruling party, ZANU-PF, in which the President questioned the right of the courts to examine the case; the International Bar Association Executive Director declared that President Mugabe's "continued undermining of the independence of the judiciary [was] unacceptable."[29]

17. International human rights standards require that every decision to undertake communications surveillance is made on the grounds that the surveillance is

[26] Constitution of Zimbabwe, ss 259 ("Prosecutor-General and other officers") and 260 ("Independence of Prosecutor-General"). The President appoints the Prosecutor-General on the advice of the Judicial Service Commission (established under s 189 of the constitution), a body that is designed to have some measure of independence from the executive.
[27] The Prosecutor-General was arrested on charges of abuse of office and defeating the course of justice; the basis for the arrest was an allegation that he dropped charges against two people suspected of being part of an alleged plot to bomb a dairy farm owned by the President and his wife. Human Rights Watch has called the alleged plot "highly suspect." Peta Thornycroft, and Aislinn Laing, "Zimbabwe's prosecutor-general arrested 'for failing to take up Mugabe dairy bombing plot,'" *The Telegraph,* 3 February 2016, available at http://www.telegraph.co.uk/news/worldnews/africaandindianocean/zimbabwe/12136906/Zimbabwes-prosecutor-general-arrested-for-failing-to-take-up-Mugabe-dairy-bombing-plot.html.
[28] Interception of Communications Act, s 7(2)(b), (3), and (4). See "Administrative Court – Judicial Service Commission," available at http://www.jsc.org.zw/index.php/court-addresses-judges/administration-court.
[29] Constitution of Zimbabwe, ss 164 and 180; "President Mugabe comments undermining the independence of the judiciary in Zimbabwe condemned by IBAHRI," *International Bar Association,* press release, 16 March 2015, available at http://www.ibanet.org/Article/Detail.aspx?ArticleUid=e8abed5a-b67d-4bfa-810f-a6c5e4b574a8.

necessary to achieve a legitimate aim and proportionate to the aim pursued.[30] The Act fails to prescribe a test of necessity and proportionality and instead grants the Minister broad discretion to issue warrants. The Minister is empowered to issue a warrant "if there are reasonable grounds for the Minister to believe" that it is necessary to gather information concerning "an actual threat to national security or any compelling national economic interest" or "a potential threat to public safety or national security."[31] The legislation provides no guidance for determining whether an actual or potential threat exists or on the meaning of the terms "national security," "public safety," and "national economic interest." The Minister may also issue a warrant if he or she has reasonable grounds to believe that certain offences "are being or will probably be committed."[32] The offences covered by the Act range significantly in terms of seriousness: they include murder and robbery, but also offences "relating to the unlawful possession of, or dealing in, precious metals" and breaches of regulations governing foreign currency exchange.[33]

18. Best practices around warrants authorising communications surveillance highlight the importance of transparency, in the form of published reports containing aggregated information on warrants, and public oversight, through independent oversight mechanisms that have the ability to hold authorities accountable.[34] Under the Act, the only oversight of the warrant regime comes from Prosecutor-General, but there is secrecy surrounding the process. The Prosecutor-General receives an annual summary from the Minister detailing "the particulars of every warrant which, during that calendar year, was issued by him or her but not renewed."[35] However, this

[30] See "Legality," "Legitimate Aim," "Necessity," "Adequacy," and "Proportionality," *International Principles on the Application of Human Rights to Communications Surveillance*.
[31] Interception of Communications Act, s 6(1)(a)-(c).
[32] Ibid, s 7(1).
[33] These are offences falling under the Third Schedule or in paragraphs 1-8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [Chapter 9:07]. Offences for which an interception warrant can be sought also include "a serious offence by an organised criminal group," (s 6(1)(a)(i)). The Act defines "an organised criminal group" broadly, as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious offences in order to obtain, directly or indirectly, a financial or other material benefit"; a "serious offence" is defined as "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty" (s 2(1)).Offences that are punishable by a maximum of four years or more of imprisonment include perjury, assault, and illegal abortion. Criminal Law (Codification and Reform) Act [Chapter 9:23]. See Nhlanhla Ngwenya, "Surveillance under the garb of rule of law," in GISWatch, *Communications Surveillance in the Digital Age,* 2014, available at https://giswatch.org/en/country-report/communications-surveillance/zimbabwe.
[34] See "Transparency" and "Public Oversight," *International Principles on the Application of Human Rights to Communications Surveillance*.
[35] Interception of Communications Act, s 19.

information is not made public in any form. The Prosecutor-General can also request additional information from the Minister and make binding recommendations to the Minister; however, these recommendations are not public.[36] There is no additional mechanism for independent parliamentary or judicial oversight of the regime as a whole.

Notification

19. According to international human rights standards, as a general matter, every person who is subject to surveillance should be notified of the decision authorising surveillance; delays may be justified only in limited circumstances, such as when notification would seriously jeopardise the purpose of the surveillance, and for a limited time, usually until the reason for the delay no longer exists.[37] While the Act allows individuals to appeal a decision to the Administrative Court once they have been "notified or becom[e] aware" of a warrant, the Act itself does not require authorities to notify individuals that they are or have been the subject of a warrant and renewal proceedings.[38]

20. Proceedings in the Administrative Court under the Act are *ex parte*, meaning that the targeted person or group is not notified about the proceeding or represented at it.[39] Consequently, individuals may only become aware that they have been under surveillance if they are charged with a criminal offence and evidence obtained through surveillance is presented in court. In all other cases, there is no official route by which they may be notified of the surveillance decision, greatly undermining the possibility of obtaining redress for illegal surveillance through the courts. Individuals also struggle to obtain redress for rights violations outside the court system as Zimbabwe's Human Rights Commission is underfunded and generally considered ineffective.[40]

---

[36] Ibid, s 19(c).
[37] See "User Notification," *International Principles on the Application of Human Rights to Communications Surveillance*.
[38] Interception of Communications Act, s 18(1). The right to administrative justice is guaranteed under s 68 of the Constitution of Zimbabwe; the Administrative Justice Act [Chapter 10:28] "provide[s] for the right to administrative action and decisions that are lawful, reasonable and procedurally fair."
[39] Interception of Communications Act, s 7(2)(b), (3), and (4).
[40] See United Kingdom Home Office, *Country Information and Guidance: Zimbabwe: Political Opposition to ZANU-PF*, October 2014, p 15, available at

Duties of telecommunications providers

21. To achieve its purposes, the Act requires every service provider to "provide a telecommunications service which has the capacity to be intercepted" and to ensure that "its services are capable of rendering real time and full time monitoring facilities for the interception of communications," among other duties.[41] (The Act defines "service provider" as "the provider of a postal service or telecommunications service," which includes internet service providers.[42]) In practice, this means that service providers must install, at their own expense, any surveillance technology the government demands. Three of the largest service providers, Econet, TelOne and Telecontract, are believed to have complied with this requirement.[43] A refusal by a service provider to assist the government with interception can result in imprisonment of up to three years and a fine.[44]

22. The Act may also require service providers to retain massive amounts of data about their customers and their communications, potentially indefinitely, for retrospective querying and analysis by authorities. A provision in the Act requires telecommunication service providers to "store call-related information in accordance with a directive [issued under the Act]."[45] "Call-related information," is defined in the Act to include "information that identifies the origin, destination, termination, duration ... of each communication generated or received by a customer or user ... and, where applicable, the location of the user within the telecommunications system."[46] (Although this definition appears to refer to mobile and fixed-line telephone calls, the definitions of "call" and "telecommunication system" indicate that

---

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/364128/CIG_Zimbabwe_Political_Opposition_v1_0.pdf; Zimbabwe Human Rights NGO Forum, *Zimbabwe: Human Rights, Rule of Law & Democracy 2013*, 2013, p 55, available at http://www.hrforumzim.org/wp-content/uploads/2014/01/HumanRights-RuleofLaw-Democracy20131.pdf.

[41] Interception of Communications Act, ss 12(1)(a) and 9(1) (c).

[42] Ibid, s 2(1).

[43] Arthur Gwagwa and Charlie Blagbrough, "State Surveillance in the digital age: the implications for freedom of expression and the right to privacy," *Zimbabwe Human Rights NGO Forum,* 4 June 2013, available at http://www.hrforumzim.org/wp-content/uploads/2013/06/Are-privacy-and-expression-protected-in-Zimbabwe_.pdf

[44] Interception of Communications Act, s 9(2). The Act does not specify which employees or officers of the service provider may be subject to imprisonment.

[45] Ibid, s 12(1)(b).

[46] Ibid, s 2(1).

service providers may also be required to retain information about communications sent through the internet, such as email.[47])

23. The Zimbabwe Human Rights NGO Forum understands that a directive requiring providers to retain call-related information has been issued, but to date, it has not been publicly available. Placing extensive mandatory data retention requirements on telecommunications providers, such as telephone companies and internet service providers, contravenes international human rights standards; mandatory and indiscriminate retention of communications data is a serious interference with the right to privacy that goes beyond what is strictly necessary to respond to legitimate law enforcement needs.[48]

Definitions

24. The Act's failure to clearly include metadata within the definition of "intercept" means that authorities may consider themselves free to collect, retain, and analyse metadata without seeking a warrant. Metadata is "data about data," and includes information such as the subject line of an email and where a phone call was made. Cumulatively, metadata can reveal more about an individual than the contents of communications; using metadata, comprehensive profiles of individuals, their movements, habits, friends, and communities can be built.[49] The Special Rapporteur on Freedom of Expression has noted that analysis of metadata "can be both highly revelatory and invasive, particularly when data is combined and aggregated."[50]

[47] The terms "call" and "telecommunications system" are defined in s 2 of the Postal and Telecommunications Act [Chapter 12:05]; these definitions apply by virtue of s 2(2) of the Interception of Communications Act.
[48] See *The right to privacy in the digital age,* Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, 2014, A/HRC/27/37, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; see also Court of Justice of the European Union, *Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.
[49] See Jane Mayer, "What's the Matter with Metadata," *The New Yorker*, 6 June 2013, available at http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata.
[50] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, April 2013, A/HRC/23/40, para 15, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

25. The Act's definition of "intercept" ("to listen to, record, or copy, whether in whole or in part" communications sent through telecommunications or radio systems) appears directed at the contents of communications, and not metadata. Additionally, the "call-related information" that service providers must store, which includes a broad range of metadata, is excluded by implication from the warrant regime: warrants are required only to "intercept a communication in the course of its transmission" and call-related information is automatically stored by service providers, rather than intercepted in the course of a communication.

26. Furthermore, although one of the Act's purposes is to provide for the "monitoring of certain communications," the term "monitoring" is undefined and seemingly not covered by the warrant regime. The Act requires service providers to "allow monitoring" and refers to "monitoring agents" without elaboration.[51] The Act also provides for the establishment of a "Monitoring of Interception of Communications Centre" (MICC) that "shall be the sole facility through which authorised interceptions shall be effected."[52] Under the Act, service providers transmit intercepted communications and call-related information about specific targets to the MICC.[53] Even though one of the Act's primary purposes is "to provide for the establishment of a monitoring centre," the Act does not set out the MICC's functions clearly or prescribe any sort of oversight of its operations.[54]

Restrictions on services using encryption

27. Using the Act as a justification, the government agency that controls the licensing regime for service providers has placed restrictions on the technology that providers may offer to customers, limiting individuals' ability to communicate privately. Although the Act does not specifically ban the use of encryption technology, the Postal and Telecommunications Regulatory Authority (POTRAZ) interprets broadly worded language in the Act as an authorisation for that agency to ban encrypted services. In 2011, POTRAZ banned encrypted messaging services provided on Blackberry phones, arguing they violated the Act because the Act requires that all

[51] Interception of Communications Act, s 9(h)(i) and (ii).
[52] Ibid, s 4(2).
[53] Ibid, s 9(1)(f).
[54] Ibid, long title.

services must have "the capability to be intercepted."[55] As of March 2016, this ban remains in place. Service providers' ability to challenge actions by POTRAZ is limited as POTRAZ is strongly aligned with the President: the Office of the President and Cabinet administers POTRAZ's governing legislation and POTRAZ's board is appointed by the President.[56]

28. Bans on the use of encryption technology violate the right to privacy and the right to freedom of expression. As the Special Rapporteur on Freedom of Expression has noted, "Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attack."[57] Consequently, "Outright prohibitions on the individual use of encryption technology disproportionately restrict freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression."[58]

SIM Card Registration and the Central Subscriber Information Database

29. Compulsory SIM card registration and the retention of information about mobile phone users in a centralised database threaten the right to privacy in Zimbabwe. SIM card registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups in a society.[59] It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilities surveillance and makes tracking and monitoring of users easier for authorities, concerns that are especially acute in countries with conflict, political instability, and civil society suppression. In Zimbabwe, these concerns compound due

[55] See "Blackberry Messenger a dream," *The Zimbabwean*, 5 June 2012, available at http://www.thezimbabwean.co/2012/06/blackberry-messenger-a-dream/; Janet Shoko, "BlackBerry to go full throttle in Zimbabwe," 9 April 2014, available at http://www.theafricareport.com/Southern-Africa/blueberry-to-go-full-throttle-in-zimbabwe.html.
[56] Statutory Instrument 19 of 2014, Assignment of Functions (Office of the President and Cabinet); Postal and Telecommunications Act [Chapter 12:05], s 6(1). POTRAZ's mandate is "[t]o exercise licensing and regulatory functions in respect of postal and telecommunication systems and services in Zimbabwe, including the establishment of standards and codes relating to equipment attached to the telecommunication systems." POTRAZ, "About Us," available at https://www.potraz.gov.zw.
[57] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* May 2015, A/HRC/29/32, para 16.
[58] Ibid, para 45.
[59] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 2013, para 70; see also *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* 2015, para 51.

to the absence of data protection legislation to appropriately regulate access to information and information sharing among government departments.

30. In 2013, the government introduced regulations under the Postal and Telecommunications Act requiring all SIM cards to be registered to an identified individual.[60] These regulations were replaced with a substantially similar set of regulations in 2014. In order to purchase a SIM card from a telecommunications provider in Zimbabwe, an individual must produce his or her national identity card or passport and provide personal information, such as full name, permanent residential address, nationality, gender, and subscriber identity number.[61] Under the regulations, the provider must send this information to POTRAZ where it is added to a database, controlled by POTRAZ, known as the Central Subscriber Information Database.[62] POTRAZ retains the information in the database until five years after the customer's contract expires.[63]

31. The original 2013 regulations were very controversial; in particular, civil society groups highlighted a number of concerns, such as the severe penalties faced by individuals who failed to register, which included imprisonment of up to six months.[64] In 2013, POTRAZ publicly threatened to arrest and imprison customers who failed to register their SIM cards and update their addresses.[65] In 2014, the Legal Committee of Zimbabwe's Parliament raised the concern that the 2013 regulations infringed on constitutional rights as law enforcement agents could access subscriber information without a court order.[66]

---

[60] Postal and Telecommunications (Subscriber Registration) Regulations, 2013 (Statutory Instrument 142 of 2013). Regulations made by the Minister of Transport, Communications and Infrastructural Development in terms of s 99 of the Postal and Telecommunications Act [Chapter 12:05] and in consultation with POTRAZ. Formally, SIM card registration predates the 2013 regulations: in June 2010, POTRAZ issued a directive requiring SIM card registration, but it was not widely implemented.
[61] Ibid.
[62] Ibid, art 8(1).
[63] Ibid, art 4(9).
[64] Carly Nyst, "Zimbabwe threatening privacy rights with new SIM registration database," *Privacy International Blog*, 2 October 2013, available at https://www.privacyinternational.org/node/381. On other concerns, see "SIM card registration under probe," *Zimbabwe Human Rights NGO Forum*, 26 January 2015, available at http://www.hrforumzim.org/news/sim-card-registration-under-probe/.
[65] "Sim card arrests improper: Chamisa," *The Zimbabwean*, 2 October 2013, available at http://www.thezimbabwean.co/2013/10/sim-card-arrests-improper-chamisa/.
[66] "Bill Watch 29-2014," *Veritas Zimbabwe*, 21 July 2014, available at http://www.veritaszim.net/node/1059.

32. In 2014, the 2013 regulations were replaced by new regulations that were substantially similar to the old regulations: the new regulations continue the existence of the Central Subscriber Information Database and maintain the penalty of imprisonment of up to six months for failing to register a SIM card or providing incorrect information. In November 2015, Zimbabwe's largest mobile service provider disconnected at least one million SIM cards because they were unregistered.[67] Although the new regulations introduced the requirement that a warrant or court order is required for POTRAZ to release information to law enforcement agents, the warrant regime contains a concerning loophole: while a court order is issued by a judge or magistrate, police officers designated as justices of the peace may issue warrants.[68] In practice, this loophole means that police can obtain warrants without judicial involvement in the process.

Concerns around Intelligence Agencies

33. International human rights standards require that intelligence agencies are subject to clear laws that appropriately delimit their powers; intelligence agencies should also be overseen by independent bodies to ensure they abide by domestic and international law.[69] Zimbabwe fails to meet these standards as its core intelligence agencies are executive bodies, operating without a legislative mandate, and there are no effective oversight mechanisms to assess their compliance with general law or hold them accountable for human rights violations. Although the constitution requires that "any intelligence service of the state must be non-partisan, national in character, patriotic, professional and subordinate to the civilian authority," President Mugabe is at the centre of an intelligence sector that acts in a partisan manner and lacks appropriate oversight.[70]

[67] Janet Shoko, "Telecoms: 1 million mobile phones disconnected in Zimbabwe," *The Africa Report*, 16 November 2015, available at http://www.theafricareport.com/Southern-Africa/telecoms-1-million-mobile-phones-disconnected-in-zimbabwe.html.
[68] Postal and Telecommunications (Subscriber Registration) Regulations, 2014, art 9(2). "Bill Watch 29-2014," *Veritas Zimbabwe*, 21 July 2014.
[69] See *International Principles on the Application of Human Rights to Communications Surveillance*.
[70] Constitution of Zimbabwe, s 224(2).

The Central Intelligence Organisation

34. The Central Intelligence Organisation (CIO) is Zimbabwe's national intelligence agency. The CIO is an executive agency: its mandate, functions, and powers are not outlined in law, in contravention of the constitution which requires that any intelligence service "must be established in terms of a law or a Presidential or Cabinet directive or order."[71] Human Rights Watch has observed that the CIO "lacks accountability and is answerable only to the president" and "its operations are shrouded in secrecy."[72] Nonetheless, the CIO is believed to be the central institution in Zimbabwe's intelligence apparatus; the Zimbabwean police, by contrast, are "ill equipped, underpaid, and poorly trained."[73] The CIO is known to employ informants and staff affiliated with the ZANU-PF, Zimbabwe's ruling party.[74]

35. Human Rights Watch has stated that the CIO "appears to function as an agency of ZANU-PF" and "[c]ivil society leaders and the media have reported on the CIO conducting surveillance and intelligence gathering on their work and on other people and groups within civil society and political parties, perceived as hostile to ZANU-PF."[75] Leaked documents released by *Al Jazeera* in 2015 showed that in 2011 the CIO developed a "joint action plan" with South Africa's State Security Agency (SSA). One of the objectives outlined in the plan was for both agencies "to monitor activities aimed at subverting [the] constitutional order," including "to monitor and exchange information on rogue NGOs and other institutions."[76] This task involved the "identification, profiling, and assessment of NGOs engaged in subversive activities."[77]

---

[71] Ibid, s 224(1).
[72] Human Rights Watch, *The Elephant in the Room*, 2013, pp 28 and 3, available at https://www.hrw.org/sites/default/files/reports/zimbabwe0613webwcover_0.pdf.
[73] United States Department of State, Bureau of Democracy, Human Rights and Labor, *Zimbabwe 2013 Human Rights Report*, 2013, p 8, available at http://www.state.gov/documents/organization/220388.pdf.
[74] Human Rights Watch, *The Elephant in the Room*, 2013, p 28.
[75] Ibid.
[76] "State Security Committee Joint Action Plan Zimbabwe-Republic of South Africa 2011/2012," available at http://www.documentcloud.org/documents/1672718-south-africa-zimbabwe-joint-action-plan-2011-2012.html; see Rahul Radhakrishnan and Will Jordan, "Spy Cables: Greenpeace among intelligence targets," *Al Jazeera*, 24 February 2015, available at http://www.aljazeera.com/news/2015/02/spy-cables-greenpeace-intelligence-targets-150224115107221.html. The CIO is also a member of the Committee of Intelligence and Security Services of Africa (CISSA), a regional body that consists of intelligence organisations from 40 African Union member states, whose objectives include "[to] coordinate ... exchange of intelligence on common security threats." "Objectives - CISSA," available at http://cissaau.org/about-cissa/objectives/.
[77] "State Security Committee Joint Action Plan Zimbabwe-Republic of South Africa 2011/2012."

36. Government officials have boasted about the CIO's extensive surveillance capabilities. In 2014, Presidential Affairs Minister Didymus Mutasa stated that the government "sees everything," adding, "We have our means of seeing things these days, we just see things through our system. So no-one can hide from us in this country."[78] He warned Zimbabweans to "[b]e careful not to denigrate our president[;] we will visit your bedrooms and expose what you will be doing."[79] In 2015, after he had been ousted from office, Mutasa observed, "Your phones are listened to a lot. The CIO is huge and it produces many reports."[80] He also stated that the agency has a network of informants, including waiters in hotels.[81]

The Joint Operations Command

37. The Joint Operations Command (JOC) is another important component of the intelligence apparatus and consists of President Mugabe and the chiefs of the army, air force, police, prisons, and intelligence services.[82] Because of a lack of transparency around its mandate and powers, the JOC's exact role is not well understood. However, it is known to have been responsible for human rights abuses in the past and is likely to be involved in setting intelligence agencies' priorities, including around surveillance.[83]

38. In 2009, a power-sharing agreement between Zimbabwe's main opposition party, the Movement for Democratic Change (MDC), and ZANU-PF briefly resulted in the creation of the Zimbabwe National Security Council (NSC). The 2013 constitution provides for the formal establishment of the NSC with functions that include "to develop the national security policy for Zimbabwe."[84] In 2015, the government announced that it was proposing legislation on the NSC: commentators have argued

[78] "CIO watching your bedrooms, Mutasa warns critics," *New Zimbabwe*, 10 June 2014, available at http://www.newzimbabwe.com/news-16183-CIO+watching+your+bedrooms,+Mutasa/news.asp.
[79] Ibid.
[80] Richard Chidza, "I am ready for jail: Mutasa," *NewsDay*, 1 July 2015, available at https://www.newsday.co.zw/2015/07/01/i-am-ready-for-jail-mutasa/.
[81] Ibid.
[82] Alex Duval Smith, "Power sharing in Zimbabwe threatened by five-man cabal," *The Observer*, 15 January 2009, available at http://www.theguardian.com/world/2009/feb/15/zimbabwe-joint-operations-command.
[83] Human Rights Watch, *The Elephant in the Room*, 2013, p 10.
[84] Constitution of Zimbabwe, s 209.

that the aim of the legislation is to effectively "rebrand" the JOC as the NSC, allowing the JOC to continue its abusive tactics under the guise of the NSC.[85]

Surveillance technology and other concerns

39. The specific surveillance technology in use by intelligence agencies in Zimbabwe is unknown. There is, however, some evidence to suggest that the government has purchased sophisticated surveillance technology: in 2015, leaked Ugandan security documents revealed that Zimbabwe was one of several countries that Ugandan security services believed had purchased FinFisher surveillance technology from UK-German company Gamma Group.[86] FinFisher is "malware," malicious software that can be used to retrieve information from computers and spy on communications without the user's knowledge.[87]

40. While surveillance that falls within the ambit of the Interception of Communications Act should be authorised through the Act's warrant regime, it is not known if the intelligence agencies comply with the Act. Additionally, there are no mechanisms for ordinary Zimbabweans to seek redress for unlawful actions by the intelligence agencies. Although the constitution requires the establishment of an independent mechanism for complaints about misconduct by the security forces (which includes intelligence agencies), this body has not yet been created.[88]

Criminal Penalties for Public and Private Speech

41. Restrictive laws grant police the power to arrest individuals for statements made in the course of public and private conversations. In a February 2016 ruling, the Constitutional Court declared invalid a legal provision that made defamation a

[85] Richard Chidza, "Mugabe moves to dissolve JOC," *NewsDay*, 17 September 2015, available at https://www.newsday.co.zw/2015/09/17/mugabe-moves-to-dissolve-joc/.
[86] "Brief to President Museveni on Operation Fungua Macho, 20 January 2012" copy reproduced in Privacy International, *For God and My President: State Surveillance in Uganda*, October 2015, p. 45, available at https://privacyinternational.org/sites/default/files/Uganda_Report.pdf.
[87] Tom Fox-Brewster, "Wikileaks releases FinFisher files to highlight government malware abuse," *The Guardian*, 16 September 204, available at http://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance.
[88] Constitution of Zimbabwe, s 210.

criminal offence.[89] However, provisions in the Criminal Law (Codification and Reform) Act and the Postal and Telecommunications Act continue to criminalise certain types of speech, affecting the right to privacy by diminishing individuals' willingness to communicate privately on political matters. For example, Section 33 of the Criminal Law (Codification and Reform) Act criminalises "undermining the authority of or insulting the President," a provision that police have used to charge individuals for remarks allegedly made in public and private conversations.[90] (For instance, in 2013, a woman was arrested and charged under Section 33 for sending a nude photograph of President Mugabe through WhatsApp; an informant relayed the conversation to security forces, who subsequently obtained the photo and conversation.[91])

Proposed New Legislation and Policy

42. The government has stated that it plans to establish a data protection regime in Zimbabwe through legislation, but there are concerns that the proposed legislation will not protect privacy in practice. In 2014, the Legal Committee of Zimbabwe's Parliament called for the enactment of data protection legislation.[92] In 2015, the government put forward a Data Protection Bill to govern both private and state bodies, which, if enacted, would "provide for the regulation of data protection" and establish a Data Protection Authority.[93] However, the government has failed to meaningfully involve civil society and other stakeholders in the development of the legislation and associated policy, and there are concerns that the institutions it aims to create would be partisan: the legislation would establish a board to manage the Data Protection Authority's operations, but the President, in consultation with the Minister responsible for the Authority, would appoint the board's members.[94]

[89] "Facts and implications of Zim ruling on criminal defamation," *Media Initiative of Southern Africa,* press release, 6 February 2016, available at http://www.misa.org/component/k2/item/3234-analysis-facts-and-implications-of-zim-ruling-on-criminal-defamation?Itemid=101.
[90] See Zimbabwe Human Rights NGO Forum, *Zimbabwe: Human Rights, Rule of Law & Democracy 2013*, 2013, p 4, available at http://www.hrforumzim.org/wp-content/uploads/2014/01/HumanRights-RuleofLaw-Democracy20131.pdf.
[91] Richard Muponde, "Whatsapp Lands Woman in Trouble," *NewsDay*, 4 January 2013, available at https://www.newsday.co.zw/2013/01/04/whatsapp-lands-woman-in-trouble/.
[92] "Bill Watch 29-2014," *Veritas Zimbabwe*, 21 July 2014.
[93] Hazel Ndebele, "Authorities move to control cyberpsace," *The Zimbabwe Independent*, 24 July 2015, available at http://www.theindependent.co.zw/2015/07/24/authorities-move-to-control-cyberspace/.
[94] "Understanding Zimbabwe's draft Data Protection Bill," *TechZim*, 10 November 2015, available at http://www.techzim.co.zw/2015/11/understanding-zimbabwes-draft-data-protection-bill/.

43. The government has also released a draft of a Computer Crime and Cybercrime Bill that has already raised privacy concerns.[95] For example, if the bill became law, police officers would require authorisation from a magistrate before they could compel an individual or company to release computer data or other information for the purposes of a criminal investigation; however, the basis for authorisation would be "reasonably required," a vague standard, and the police would not be required to consider other less invasive measures before accessing data. Additionally, the bill would permit the use of hacking as a forensic tool. The bill contains insufficient legislative and judicial safeguards for the exercise of these intrusive powers.

44. In 2015, the government made known its intention to establish a single internet gateway operator in Zimbabwe (currently there are five), which could facilitate surveillance and other rights-limiting measures, such as censorship.[96] The creation of a single internet gateway controlled by the government would generate significant scope for abuse: authorities would have the capability to intercept internet session information over time, block or permit online information flows coming through Zimbabwe, and identify users' internet activities and habits.

Recommendations

45. We recommend that the government of Zimbabwe should:

- Prioritise the revision of the Interception of Communications Act to bring it into line with the 2013 constitution and undertake a process of consultation with stakeholders to establish a regime that meets international human rights standards; in particular:

[95] Zimbabwe Computer Crime and Cybercrime Bill 2013, on file with Privacy International.
[96] Zimbabwe National Policy for Information and Communication Technology (ICT) 2015, on file with Privacy International. The policy states, at p 34, "The Government has long stated its policy for a single gateway operator. In order to coordinate the proliferation of international gateways and stem revenue losses, there shall be one Super Gateway which shall be the entry and exit point for all international traffic." See Hazel Ndebele, "Govt sharpens spying tools," *The Zimbabwe Independent*, 8 January 2016, available at http://www.theindependent.co.zw/2016/01/08/govt-sharpens-spying-tools/. In 2001, the government established a single gateway operator, but following a 2004 court ruling, private companies were able to establish their own gateways.

    - Reform the warrant regime so that the issuance and renewal of warrants is in the hands of a competent judicial authority that is independent and impartial;
    - Set up a public reporting mechanism on warrants issued under the Act and establish robust and impartial oversight mechanisms;
    - Establish a user notification regime, including explicit guidance on the narrow grounds for appropriate limits on notice;
    - Clarify in law the functions of the Monitoring of Interception of Communications Centre (MICC);
    - Establish a mechanism for redress for unlawful surveillance.

- In light of the importance of checking executive powers around surveillance, work to strengthen the independence of the judiciary.

- Establish intelligence agencies in primary legislation that clearly describes their functions and powers, provides for effective oversight, and adheres to international human rights standards.

- Establish, without delay, an independent mechanism for complaints about misconduct by the security forces as contemplated by Zimbabwe's constitution.

- Abolish mandatory SIM card registration and dismantle the Central Subscriber Information Database; ensure that any policy in this area is developed in consultation with civil society organisations and adheres to international human rights standards.

- Ensure that the Data Protection Bill meets international standards and that any data protection authority established by law is appropriately resourced and independent, and has the power to investigate breaches of data protection principles and order redress.