Regional and International Benchmarks on Surveillance, Cybercrimes and Computer Crimes

Co-authored by Arthur Gwagwa and Kuda Hove

Surveillance,[1] cyber espionage,[2] cybercrimes and computer crimes transverse various regional and international standards and norms as set by the relevant standard setting,[3] norm sharing bodies as well as security forums. They also implicate technical rules, for example relating to internet protocols and the management of internet infrastructure, critical resources such as internet assigned numbers and letters.[4] This report will confine itself to the examination of the standards and norms that have a direct bearing on the exercise of human rights online.

International Norms and Standards

1. Right to Freedom of Opinion and Expression

Free expression, encompassing imparting and receiving, including in the digital age is a fundamental right, enshrined in various international instruments.[5] The internet's contested role as means of both expression and repression has been subject to intense scrutiny.[6] This is the case since advances in information communication technology are dramatically improving real-time communication and information sharing. By improving access to information and facilitating global debate, they foster democratic participation. By amplifying the voices of human rights defenders and helping to expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights.[7]

2. The Right to Privacy Including Data Protection

Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[8] 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, access to information, and association.[9] The right to privacy embodies the presumption that individuals should have an area of

---

[1] Especially state surveillance, but this may also include surveillance by business entities and the market for surveillance

[2] The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.

[3] E.g. United Nations Human Rights Council & General Assemblies

[4] An example is the current Internet Assigned Numbers Authority (IANA) transition done by technical bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the ITU. See Arthur Gwagwa et al, *Internet Governance and its effects of achieving sustainable social development goals in Zimbabwe*. Academia. Retrieved at: http://bit.ly/1ImZVxZ. Accessed on 24 February 2016.

[5] Article 19 of the Universal Declaration of Human Rights, Article 19 of International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR)International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), ILO Convention N° 135, Workers' Representatives Convention, General Comment 10 [19] (Article 19) of the Human Rights Committee (CCPR/C/21/Rev.1 of 19 May 1989), General Comment 11 [19] (Article 20) of the Human Rights Committee (CCPR/C/21/Rev.1 of 19 May 1989), The public's right to know: Principles on Freedom of Information Legislation. Annex II Report E/CN.4/2000/63

[6] See UN High Commissioner for Human Rights, Report on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014, and UN Special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the UN Human Rights Council, UN doc. A/HRC/23/40, 17 April 2013.

[7] UN OHCHR (ibid).

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

[9] The 1993 Vienna Declarations and Programme of Action, the most important human rights covenant of the past 20 years, reaffirmed the rights outlined in the previous treaties, clarified the hierarchy of rights and strengthened the human rights protection mechanisms, particularly by setting up of the Office of the High Commissioner for Human Rights. It also stressed that the violation of a right is interconnected to the violation of other human rights. It then follows that the violation of the right to privacy also violates the right of expression or speech and vice versa.

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.[10] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when law, necessary to achieve a legitimate aim, and proportionate to the aim pursued, prescribes them.[11]

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.[12] A number of international instruments enshrine data protection principles,[13] and many domestic legislatures have incorporated such principles into national law.[14]

At the international level, the period beginning 2010 has been a defining moment in the development of international norms and standards relating to the protection of human rights online. Although this was due to combined effort of diverse stakeholders, the work of Frank La Rue[15] was instrumental in this regard. In addition, the Snowden disclosures and post-Snowden environment have had a huge impact in the development of both liberal and illiberal norms. From June 2013 onwards, a seemingly endless stream of riveting disclosures from former NSA contractor Edward Snowden has gripped the world's attention and put a spotlight on the world's most powerful signals intelligence (SIGINT) agencies: the National Security Agency (NSA), Government Communications Headquarters (GCHQ), and their allies.

These disclosures also have, and will continue to have, a major impact on illiberal norms in the cyberspace.[16] They have deflected attention away from China, Iran, and Russia-based offensive cyber espionage campaigns, created an atmosphere of suspicion and raised questions about the legitimacy of US and allied governments' "Internet Freedom" agenda, have opened up ICT investment opportunities where before there were reservations. US companies now have a "Huawei" problem and they (unintentionally) "normalise" mass surveillance practices in the global South, and provide an excuse for national controls disguised as "technological sovereignty."[17] In no particular order, the paper will now examine some of the liberal norms that have been developed just before and mainly after the Snowden disclosures.

---

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

[11] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40; Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[12] See Paragraph 1 of Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[13] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the Regulation of Computerized Personal Data Files (General Assembly resolution 45/95 and E/CN.4/1990/72)

[14] As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (December 8, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

[15] Frank La Rue is a Guatemalan labour and human rights law expert and served as UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, from August 2008 to August 2014.

[16] Analysing the World Movement against Democracy. Authoritarian Influence on the Internet Session. December 10, 2014. A panel Discussion led by Chris Walker of the National Endowment for Democracy and Ron Deibert of Citizens Lab.

[17] Walker and Deibert, ibid

3. United Nations General Assembly Resolution 68/167 (Also known as the Brazil-German Resolution)[18]

In December 2013, the United Nations General Assembly adopted Resolution 68/167, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.[19]

The objective of this resolution is to expound that violations of this right to privacy are not acceptable, irrespective of the means used to carry them out. As Brazil's Ambassador Antonio de Aguiar Patriota noted, the resolution "establishes for the first time that human rights should prevail irrespective of the medium, and therefore need to be protected online and offline". While not legally binding, such documents are highly relevant in international politics and mirror public opinion. This is the first time that Internet surveillance has come to be the focus of a UN resolution and marks the tightening of the framework protecting the right to privacy.

4. Resolution A/HRC/28/L.27 on Special Procedure Mandate on the Right to Privacy.

On March 25th 2015, the Human Rights Council, by consensus, adopted Resolution A/HRC/28/L.27 that established a special procedure mandate on the right to privacy. This decision was a key step forward for the UNHRC; it elevates the right to privacy to the priority level that the Human Rights Council ascribes to most other human rights. Most importantly, it gives the right to privacy the international recognition and protection it deserves.[20] This step acknowledges the importance of the right to privacy in the realisation of other human rights such as free expression.[21] The Special Rapporteur will provide much-needed leadership and guidance on the guarantee of the right to privacy, as well as strengthening the monitoring of states and companies' compliance with their responsibility to respect and protect the right to privacy in their laws, policies, and practices.[22]

5. Human Rights Council resolutions 20/8 of 5 July 2012 and 26/13 of 26 June 2014

Council Resolutions 20/8 of 5 July 2012 and 26/13 of 26 June 2014 both emphasise on the importance of the promotion, protection and enjoyment of human rights on the Internet.

6. UN General Assembly Resolution (UNGA Resolution) on the Right to Privacy in the Digital Age

This was adopted by consensus on 18 December 2014. It provides practical guidance on the steps States need to take at national level to protect human rights online. The UNGA Resolution recognises the need "to further discuss and analyse, based on international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age. It also examines procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices."

The UN General Assembly resolution calls on states "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of

---

[18] The Draft Resolution was submitted by Brazil and Germany on 8 October 2013. See http://bit.ly/1QRnAw9

[19] OHCHR,The Right to Privacy in the Digital Age. Available at http://bit.ly/1nNZQsc

[20] Statement by Electronic Frontier Foundation (EFF), dated 26 March, 2014, 'UN Human Rights Council Appoints Special Rapporteur on the Right to Privacy'

[21] For example, see reports by the UN OHCHR & SR on Freedom of Expression (ibid)

[22] Statement by Privacy International soon after the adoption of resolution A/HRC/28/L.27

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".

The Resolution builds upon the previous resolutions and the UN High Commissioner for Human Rights' Report on the right to privacy in the digital age, UN doc. A/HRC/27/37 of 30 June 2014, and UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report to the UN Human Rights Council, UN doc. A/HRC/23/40 of 17 April 2013.

7. International Principles on the Application of Human Rights to Communications Surveillance

Although these do not have the force of law, these International Principles have been widely accepted as 'soft law' as they are the outcome of a global consultation with civil society groups, industry, and international experts in communications surveillance law, policy, and technology. Generally modelled on but an expansion of the Human Rights Committee General Comment 16 on the interpretation of article 17 of the ICCPR, they attempt to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These principles can 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.

8. The Association for Progressive Communications - La Rue Framework

The Association for Progressive Communications (APC) has developed the framework based on the work of Frank La Rue and on General Comment 34 on Article 19 of the ICCPR. The questions in the framework are meant to provide guidance in monitoring and reporting on internet-related human rights violations, specifically those related to freedom of expression. Further work is needed, and is underway, to develop more comprehensive guidance. In the meantime, we welcome comments, criticism, and review on its use.

9. The NETmundial Initiative

NETmundial identified a set of common principles and important values that contribute for an inclusive, multi-stakeholder, effective, legitimate, and evolving Internet governance framework and recognized that the Internet is a global resource which should be managed in the public interest. These principles also call for the protection and promotion to the right to freedom of expression, to freedom of association and the right to privacy. Protecting the right to privacy includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data.

International to Regional Norms Diffusion

Regional Standards

This part of the paper examines to what extent Africa's regional and national cybersecurity regulatory frameworks are keeping up with the emerging international norms on the protection of privacy and civil liberties in the cyberspace.[23]

The African Charter on Human and Peoples' Rights (ACHPR)

The African Charter is comprehensive in its coverage and protection of human rights, [24]including the right for every individual to receive information and to express and disseminate his or her opinions within the law. As expressed, the right to free expression, including in the digital age falls

[23] Adopted from Arthur Gwagwa. Cybersecurity, Sovereignty, and Democratic Governance in Africa. Academia. Retrieved at: http://bit.ly/21fwwAk. Accessed on 24 February 2016.

[24] Guaranteeing the individual's right to respect for dignity, respect for the integrity of his person, and respect for "liberty and... the security of his person". The rights to freedom of conscience, and the profession and free practice of religion are also protected, as well as the rights to receive information, express and disseminate opinions within the law, and to freely associate and assemble within the boundaries of the law.

short of the international standards. Secondly, the expressly guaranteed right to "privacy", however, is notably absent. In addition to this omission, the ACHPR has been criticised for failing to provide the African Commission on Human and Peoples' Rights, established by Article 30 of the Charter, with sufficient powers with which to implement decisions or recommendations in cases in which a state has been found to violate a guaranteed human right. Reports produced by the Commission are to be transferred to the states concerned, and although the Commission "may make... such recommendations as it deems useful"; critics have argued that it has been denied "teeth with which to bite those found to have flouted it".

The African Union Convention on Cyber Security and Data Protection (AUCyC)

In view of the limited right to freedom of expression and in the absence of the right to privacy in the ACHPR, it is necessary to examine the free expression and privacy protection, including in the digital age provided by other supranational bodies. Of particular relevance for present purposes is the Draft Convention on Cyber Security. This Convention seeks to establish an integrated regional legal framework for cyber security, which simultaneously protects the fundamental rights and freedoms of persons affected.

The provisions of AUCyC, which requires states to adopt similar measures mirrors the practical guidance in the UN General Assembly resolution (UNGA Resolution) on the right to privacy in the digital age, adopted by consensus on 18 December 2014. This is not surprising given that UNESCO part of the AUCyC. However, not many countries have adopted the Convention,[25] although some Francophone countries such as Senegal and sub-regional bodies such as ECOWAS have been harmonising their digital information laws and institutions.

The African Declaration on Internet Rights and Freedoms

Probably an African equivalent to the International Principles, this is a Pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. The Declaration is intended to elaborate on the principles which are necessary to uphold human and people's rights on the internet, and to cultivate an internet environment that can best meet Africa's social and economic development needs and goals. The African Declaration on Internet Rights and Freedoms is organised around twelve key principles, including Freedom of Expression and the Right to Information and Open Data."

General Practical Challenges and Questions that Remain

National Legal Frameworks: The main challenge relates to the gap between the evolving norms both at international and regional levels and the practice at national/ domestic levels. An example relates to the way the countries facing terrorism threats responding to these legitimate national security concerns. As pointed out in UNGA Resolution (ibid), the main challenge is at national level - domesticating the developments at both international and regional level in balancing the dictates of economic growth, national security, and individual freedoms.

For instance, the Kenyan foreign ministry is reportedly seeking additional help in the area of intelligence, surveillance, and reconnaissance (ISR) in light of the latest al Shabbab terrorist attacks[26]. This builds up to its existing joint military strategy with the U.S. Concerns are being raised about Kenya's policy goals, transparency in its surveillance capabilities, in particular whether Kenya needs to boost its intelligence capabilities or change its regional policy.

In the case of Africa's big economies such as South Africa, the extent to which they are balancing the opportunities and threats that cyberspace presents is still subject to debate. The police, intelligence

[25] By end of 2015, only 4 countries had adopted the Convention.

[26] Kenya seeks more Western help after university attack, 8 April, 2015, http://www.dnaindia.com/world/report-kenya-seeks-more-western-help-after-university-attack-2075797

community, the police, and corporates are not resilient enough to adequately respond to incidents like the recent massive attack on Sony Pictures or the hacking of the Pentagon's social media accounts.

Disproportionate response to national security concerns: National security threats are real and evolving therefore, the personal data provided through surveillance and monitoring of telecommunications network have a value in preparing for such threats. However, while such legitimate concerns may justify limitations to civil liberties and privacy, such activities that restrict the right to privacy, including communications surveillance, can only be justified when prescribed by the law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued. The definition of legitimate parameters for national security surveillance, which, increasingly, affects the right to privacy of individuals, is subject to debate. In the pursuit of legitimate national security interests, governments are entitled to gather and protect certain sensitive information, as well as to restrict access of the public to certain information (such as that pertaining to operations, sources, and methods of intelligence services). In so doing, however, they must ensure full compliance with international human rights law. Serious concerns are raised over the potential for national security overreach, without adequate safeguards to protect against abuse.

In his report to the Human Rights Council in 2010, the former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, highlighted the erosion of the right to privacy in the fight against terrorism, as a result of the use of surveillance powers and new technologies which are used without adequate legal safeguards. He noted that the increasing use of "data mining" by intelligence agencies "blurs the boundary between permissible targeted surveillance and problematic mass surveillance which potentially amounts to arbitrary or unlawful interference with privacy". Effective national legal frameworks are critical to ensuring protection against unlawful or arbitrary interference. Yet, in general, national legislation in Africa has not been adopted to match developments in communications technology and the surveillance measures these developments have facilitated. In addition, in some jurisdictions there is a lack of independent oversight to review surveillance measures, as a safeguard against abuse.

Enforcement: A second challenge is related to the fact that, even where adequate legislation and oversight mechanisms do exist, a lack of effective enforcement is bound to contribute to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy.

Role of Businesses, cyber espionage, and the market for surveillance: The last challenge relates to the responsibility of businesses themselves to respect privacy rights in the digital age. The challenge lies ensuring that corporations in the communications technology industry respect the right to privacy as well as other related human rights. Locally, companies such as the Econet group of companies have engaged the skills of data miners and data analysts whose scope of activities are not known to the State or the consumers.

A recent study by the University of Toronto's Citizen Lab found that human rights groups in the study are targeted by persistent China-based digital attacks of the same nature hitting Fortune 500 companies and governments. These capabilities are proving particularly attractive to many governments that face ongoing insurgencies and other security challenges, as well as persistent issues around popular protests and street-level demonstrations. The sale and deployment surveillance capabilities is often done in violation of the Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011 which set out a global standard for preventing and addressing adverse impacts on human rights linked to business activity.

Regional to National Norms Diffusion

Zimbabwe Practical Challenges and Questions that Remain

This section will examine the practical challenges and questions that remain in Zimbabwe, through and examination of:

- Existing and pending laws and policies affecting internet use and governance in Zimbabwe Regional and International standards on surveillance, cybercrime, and computer crime crimes regulation,
- The extent to which these laws conform to the regional and international standards

The discussion will highlight relevant case law .i.e. how the Zimbabwean and other courts have treated cases relating to the issues under discussion. It will also include issues such as intermediary liability issues, protection of the right to personal security, right to privacy, freedom of expression and access to information on online platforms.

Existing Laws

Section 61 of the Zimbabwe Constitution protects the right to freedom of expression however; there are still several laws that criminalise freedom of expression. These include the Access to Information and Protection of Privacy Act (AIPPA) [*Chapter 10:27*] 2002, the Broadcasting Services Act [*Chapter 12:06*] 2001, Official Secrets Act [*Chapter 11:09*] 2001, and the Censorship and Entertainment Controls Act [*Chapter 10:04*]**.**[27] This paper will examine the Postal and Telecommunications Act [*Chapter 12:05*] 2000, the Interception of Communications Act [*Chapter 11:20*] 2007, the AIPPA, the Criminal Law (Codification and Reform) Act *[Chapter 9:23]* 2004, Subscriber Registration Regulations, 2013,[28] and the Central Subscriber Database Regulations. Consideration is also given to the proposed Zimbabwe Computer Crime and Cybercrime Bill 2014 as well as the proposed statutory instrument on mandated infrastructure sharing as well as the provisions of the proposed National ICT Policy, some of which will be implemented through legislation.

1. **Interception of Communications Act**[29]

   The Interception of Communications Act 2007 sets out the legal basis on which authorities may conduct communications surveillance. As little information about how authorities apply and interpret the Act is publicly available, the concerns raised in this stakeholder report largely concern flaws in the legislation itself. Five aspects raise specific concerns under international human rights standards:

   - First, authorities may obtain warrants to intercept private communications through a process that is controlled by members of the Executive and not subject to independent judicial scrutiny or public oversight;
   - Second, 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;
   - Third, the Act places wide-ranging duties on telecommunications providers to facilitate state surveillance;
   - Fourth, key terms in the Act, such as "monitoring," are not clearly defined, opening the door to abuse; and
   - Fifth, government authorities have used the Act to restrict access to encrypted services that allow people to communicate freely and privately.

[27] According to Zimbabwe Lawyers for Human Rights, government continues to use the antiquated Censorship and Entertainments Control Act (Chapter 10:04) to restrict content available to the public by way of film, written and spoken word and this has greatly undermined the right to access information.

[28] Statutory Instrument 142 of 2013 "Postal and Telecommunications (Subscriber Registration) Regulations, 2013"

[29] The summary is provided from the draft Stakeholders' UPR Report to the Human Rights Council by Privacy International (PI), the International Human Rights Clinic (IHRC) at Harvard Law School, and the Zimbabwe Human Rights NGO Forum (the Forum). The authors claim moral rights to this unpublished work.

The Interceptions 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."[30] It 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.[31] 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.[32]

- 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.[33]
- The Act violates these standards because the warrant regime is controlled by Office of the President and Cabinet.[34] There is no provision for independent and impartial judicial scrutiny.
- The Act fails to prescribe a test of necessity and proportionality, [35] but instead grants wide discretion to the Minister.[36]
- Additionally, the Minister may issue a warrant where 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 "concerning a potential threat to public safety or national security."[37] Such a wide provision, without a proper detailed guideline can be subject to abuse.

Under the Act, the only oversight of the warrant regime comes from Prosecutor-General, who 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."[38] This information is not made public in any form, therefore does not meet the test of transparency, especially given that there is no mechanism for independent oversight.[39]

While the Act allows a person or group 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 or groups that they are or have been the subject of a warrant and renewal proceedings in the Administrative Court. This violates international human rights standards which require every person who is subject to surveillance to be notified of the decision authorising surveillance.[40]

---

[30] Interception of Communications Act, long title
[31] Interception of Communications Act Section 2(2)
[32] Interception of Communications Act Section 3(3)
[33] The Chief of Defence Intelligence, Director General of National Security, Commissioner of the Zimbabwe Republic Police, and the Commissioner General of the Zimbabwe Revenue Authority. *Id*. at section 5(1)
[34] Statutory Instrument 19/2014
[35] International Principles on the Application of Human Rights to Communications Surveillance
[36] The Minister tasked with administration of the Act. Statutory Instrument 162/2012 assigned administration of the Act to the Office of the President and Cabinet headed by the Minister for Presidential Affairs in the President's Office.
[37] Interception of Communications Act section 6(1)(a), (b), (c). They also include "a serious offence by an organised criminal group," which the Act defines as an offence punishable by at least four years' imprisonment committed by "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." Offences that are punishable by more than four years' imprisonment include perjury, assault, and illegal abortion. *GISWatch, https://giswatch.org/en/country-report/communications-surveillance/zimbabwe*
[38] Interception of Communications Act section 6(1)(a), (b), (c)
[39] Interception of Communications Act section 6(1)(a), (b), (c)
[40] International Principles on the Application of Human Rights to Communications Surveillance

Intermediary Liability:- To achieve its purposes, the Act requires all service providers to have "the capability of interception"[41] and to ensure that "its services are capable of rendering real time and full time monitoring facilities for the interception of communications,"[42] among other duties. This opens doors for ISPS to collect and store large amounts of data and meta-data in contravention of international human rights standards as this is strictly necessary to respond to legitimate law enforcement needs.[43]

The Act also contains broad and vague language that allows for permissive interpretations of its provisions that potentially create gaps in its application, such as 'intercept' and 'monitoring' which are not distinguished.

Using the Act as a justification, the government agency that controls the licensing regime for service providers has placed restrictions on the technology providers may offer customers, limiting individuals' ability to communicate freely and 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 "Blackberry Messenger," an encrypted messaging service provided on Blackberry phones, arguing that under the Act, telecommunications services should have hardware and software to carry out surveillance for the government.[44] As of February 2016, the ban on Blackberry Messenger remains in place. Service providers' ability to challenge actions by POTRAZ is limited as the Postal and Telecommunications Act under which it is constituted, is administered by the Office of the President and Cabinet.[45] In addition, POTRAZ lacks independence since the president appoints its leaders.

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, "[e]ncryption 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."[46]

2. SIM Card Registration and Central Subscriber Information Database

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 registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups. It can have discriminatory effect by excluding users from accessing mobile networks. It facilities surveillance, makes tracking and monitoring of users easier for authorities. These concerns are especially acute in countries with ethnic conflict, political instability, and civil society suppression.[47] In Zimbabwe, these concerns compound due to the absence of data protection legislation needed to ensure adequate regulated access to information and information sharing among government departments. In 2014,[48] government replaced the 2013 regulations by new regulations that are substantially similar to the old regulations: the new regulations maintain

---

[41] Interception of Communications Act section 12(1)(a)
[42] Interception of Communications Act section 9(1) (c)
[43] *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, A/HRC/27/37, *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; see also Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.
[44] *Challenges in promoting privacy and freedom of expression in Zimbabwe*, NEHANDA RADIO (Oct. 12, 2015, 1:32 PM), *available at* http://nehandaradio.com/2013/06/11/challenges-in-promoting-privacy-and-freedom-of-expression-in-zimbabwe/.
[45] Statutory Instrument 19/2014 "Assignment of Functions (Office of the President and Cabinet) Notice, 2014"
[46] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 2015, Para 16.
[47] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, HUMAN RIGHTS COUNCIL, A/HRC/29/32 (2015).
[48] Statutory Instrument 95/2014 "Postal and Telecommunications (Subscriber Registration) Regulations, 2014"

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. 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.[49] While a judge or magistrate may issue a court order, police officers designated as justices of the peace,[50] can also issue warrants.[51]

3. Access to Information and Protection of Privacy Act (AIPPA) 2002

Although in 2002 Zimbabwe enacted the "Access of Information and Protection of Privacy Act," the Act's title is a misnomer, as it does not serve to protect privacy, but instead establishes restrictive barriers of entry to journalism and other media outlets. Additionally, Zimbabwe lacks data protection legislation. Based on surveys to assess how the public experiences the rule of law, the World Justice Project Rule of Law Index 2015 ranked Zimbabwe 100th of 102 countries.[52] Although AIPPA has hardly been used to invade privacy,[53] it is not so much about what it has not been used for but what it could have achieved had it been drafted properly. The proposed Data Protection Bill will govern both private and public bodies, which, if enacted, would "provide for the regulation of data protection" and allow for the establishment of a Data Protection Authority.[54] However, the government has failed to engage civil society and other stakeholders in the development of the legislation and associated policy, and there are concerns that the institutions it aims to establish will be partisan. The legislation would establish a board in charge of managing the operations of the Data Protection Authority, but the President, in consultation with the ICT Minister, would appoint the board's members.[55]

4. The Criminal Law (Codification and Reform) Act 2004

The Criminal Law (Codification and Reform) Act 2004 criminalises certain types of speech and grants the police broad powers. In their original form, Sections 31 and 33 of the Criminal Law (Codification and Reform) Act criminalised "publishing or communicating false statements prejudicial to the state" and "undermining authority of or insulting [the] President."[56] Police charged individuals under these provisions for statements made publicly or privately. For example, in 2013, a professor at Great Zimbabwe University was sentenced to three months imprisonment for calling the President a "dirty old rotten donkey" in a supermarket under Section 33. On February 3, 2016, Zimbabwe's Constitutional Court granted an application by MISA-Zimbabwe seeking confirmation of the fact that criminal defamation is no longer part of the law.

The ruling followed a concession by the State that Section 96, which provides for criminal defamation under the Criminal Law (Codification and Reform) Act (CODE), was void *ab initio* (from the beginning), which effectively brings the matter to finality. This application follows judgment in the case of *Madanhire and Others*[57] in 2013 in which the court ruled that Section 96 of the CODE was inconsistent with the provisions of Section 20 of the former constitution which provided for freedom of expression, and was therefore void. Government needs to take practical steps to ensure that the court ruling is implemented.

---

[49] POSTAL AND TELECOMMUNICATIONS (SUBSCRIBER REGISTRATION) REGULATIONS, 2014, §9(2).
[50] Bill Watch 29/2014 of 21st July 2014, VERITAS WEBSITE, *available at http://veritaszim.net/node/1059*
[51] *See id. Zimbabwe*, FREEDOM HOUSE (Oct. 4, 2015, 7:57 PM), *available at* https://freedomhouse.org/report/freedom-net/2014/zimbabwe.
[52] http://worldjusticeproject.org/rule-of-law-index
[53] Statement by Otto Saki
[54] *Authorities move to control cyberpsace*, ZIMBABWE INDEPENDENT (Oct. 4, 2015, 8:07 PM), *available at* http://www.theindependent.co.zw/2015/07/24/authorities-move-to-control-cyberspace/.
[55] *Understanding Zimbabwe's draft Data Protection Bill*, TECHZIM (Nov. 18, 2015, 8:01 PM), *available at* http://www.techzim.co.zw/2015/11/understanding-zimbabwes-draft-data-protection-bill/.
[56] Sections 31, 33 of Criminal Law (Codification and Reform) Act
[57] Madanhire and Another v Attorney General, CCZ 2/2015

5. Zimbabwe Computer Crime and Cybercrime Bill 2014

If passed, this law would allow the authorities to install spying tools remotely onto a person's device. Such actions could be authorised by a magistrate if they are satisfied, based on an application by a police officer, that there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in the Bill, but is reasonably required for the purposes of a criminal investigation.[58]

The Bill raises a number of concerns, for instance, although the Bill does contain limitations on the power to hack, it still introduces an incredibly intrusive power and provides for its use in a wide array of circumstances. There is no requirement that the court oversee closely the implementation of the authorisation, nor is there any restriction on the repeated renewal of the authorisations. Hacking or the use of remote forensic tools is lawful in very few countries, and there are few examples of legislation that appropriately regulates the use of this power in a way that is compliant with human rights. The power instils in the police incredibly broad authority and responsibility that is highly prone to misuse and abuse, and which makes oversight and accountability very difficult. Further analysis is provided by Privacy International[59] and Gwagwa, A.[60]

6. Proposed laws on infrastructure sharing, backbone nationalisation and Establishment of Data Centre

The issue of Internet gateways, mandated infrastructure sharing, data retention and national ICTs backbone again resurfaced in the draft National ICT policy[61] that has been presented to the Office of the President and Cabinet (OPC).[62] It also states, 'The National Data Centre is a critical common infrastructure that should be provided by the government. It can be designed to support both public and high security services and information'[63]. If this system is implemented, it will result in the potential monitoring of all local internet traffic before it goes to the end user. There is rising concern that one company will control all Internet gateways and infrastructure. With control of all Internet gateways, it will be technically feasible to monitor, filter, or even block internet traffic. With the mandatory registration of all Internet and telephone accounts, mass surveillance and interception will be an achievable task. In addition, the setting up of a National Data Centre will facilitate the establishment of common infrastructure that may be designed to support both public and high-security services and information. Without adequate technical and legislative safeguards, this poses a threat to the privacy and security of data. Whether data is in transit, storage, cloud or at rest.[64]

---

[58] Arthur Gwagwa. *Implications of Zimbabwe's proposed cybercrime bill.* Academia. Retrieved at: http://bit.ly/1QDJ9QH. Accessed on 24 February 2016.

[59] Zimbabwe Computer Crime and Cybercrime Bill 2014 A summary of relevant provisions pertaining to the interception of communications, collection of traffic data and hacking

[60] Arthur Gwagwa. *Implications of Zimbabwe's Proposed Cybercrime Bill*. Academia. Retrieved at: http://bit.ly/1QDJ9QH. Accessed on 24 February 2016.

[61] Zimbabwe National Policy for Information and Communication Technology (ICT) 2015. As of 1 March 2016, this National ICT Policy still had not received Cabinet approval.

[62] Section 21.3 of the ICT policy; 21.3 The National Backbone Company

[63] Section 21.5 of the ICT policy

[64] Digital Society of Zimbabwe Statement