**Protecting the right to privacy in Africa in the digital age**

Authors: Arthur Gwagwa & Anna Wilton (Zimbabwe Human Rights Forum) & under the supervision of Carly Nyst & Alexandrine Pirlot De Corbion of Privacy International, with contribution from Ababacar Diop (Senegal), Godfrey Twesigye (Uganda) and Allan Maleche (Kenya) as part of the Global Surveillance & Safeguards Project*, 'Africa region privacy campaign'* by Privacy International, IDRC, Canada and their African partners. The paper was first published & first presented at the Africa Internet Governance Summit by Arthur Gwagwa, Djibouti on 31 May 2014.

## Abstract

The right to privacy, as guaranteed in Article 12 of the Universal Declaration of Human Rights and many other provisions - including Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 16 of the Convention in the Rights of the Child, and Article 14 of the Convention on the Protection of Migrants - is a core tenet of democratic societies. Its inclusion in such a variety of provisions demonstrates its significance in relation to the protection of a broad array of other fundamental human rights. Failure to protect this right has a knock-on effect on citizens' abilities to exercise other rights, thus undermining many of the principles upon which democracy is based. Although several African States have taken steps toward ensuring that individuals' right to privacy is protected, both online and offline, a number of challenges must still be addressed before adequate protection is afforded. This paper will provide an overview of the importance of protecting the right to privacy, before addressing why it is necessary for African States to adopt and enforce effective privacy protection policies, and the specific challenges that must be resolved in order for effective policies to be developed and implemented. Finally, it will propose a number of 'next steps' ttoward ensuring the adequate protection of this right.

**The Right to Privacy in a Digital Age**

As most African states seek to consolidate democratic gains and work on sustaining peace and stability, the continent is facing a variety of new threats, including those posed by cybercrime and terrorism. These security threats are real, some of them are new, and therefore legitimate national security considerations and the necessities of law enforcement may sometimes - in well-defined cases and under specific circumstances - justify limitations to the right to privacy. However, breaches of the right to privacy can only be justified when they are necessary to achieve a legitimate aim, prescribed by the law, and are proportionate to the aim pursued. It is not acceptable to use national security concerns as a blanket justification to excuse unwarranted privacy breaches.

Regardless, States worldwide have reacted to new threats by increasing both their legal and technical capabilities to closely monitor citizens, and introducing measures that enable the collection of personal data through surveillance, alongside invasive data retention modalities. Many of these measures, ostensibly taken in order to counter new and emerging national security threats, clearly interfere with the right to privacy set out in Article 12 of the Universal Declaration of Human Rights (UNDHR) and the many other covenants and declarations mentioned above. This interference affects not only the privacy of family, home and correspondence, but also in certain circumstances citizens' honour and reputation. In December 2013, the United Nations General Assembly noted and responded to the increasing prevalence of such invasive techniques by unanimously voting to adopt a resolution on the right to privacy in a digital age, which called for countries to take measures to ensure that the right to privacy is protected not only offline but also in the context of digital communications.

The advancement of technology in the digital age - particularly internet-based and mobile phone technology has had many positive developments on the way that people live and work. For instance, it has enabled real-time cash transfers, data sharing that improves industrial efficiency, and cross cultural communications that bring

communities together. It has also been instrumental in allowing individuals to enjoy rights such as freedom of association, freedom of expression, and the ability to access and share information. On the other hand, this technology has thrown up many challenges to citizens' right to privacy. In enabling the blanket collection of massive sets of data obtained through the surveillance and monitoring of telecommunication networks, for example, it has created a situation in which huge amounts of personal and intimate information, including about an individual or group's past or future actions, can be collected and stored. Increasingly, journalists, human rights defenders and political activists are subject to arbitrary and unlawful surveillance, either because they are being actively singled out for monitoring, or simply because the Internet, often their primary means of communication, is subject to extensive monitoring. In this sense, their main means of expression becomes the main means for repression. This represents a disturbing trend of the intentional suppression of legitimate dissent and curtailment of the right to free speech, as well as a restriction of other citizens' right to access information.

In addition, although technological developments themselves are relatively easily shared, the technical knowledge necessary to design legislative frameworks to keep pace with these developments remains in short supply, as does knowledge of how to arbitrate internet jurisdiction issues. Were effective privacy laws to be put in place, and correctly enforced and interpreted, this could provide a solid basis for protection against new, potentially invasive technologies without requiring new legislation to be adopted. However, international regulatory consensus has yet to emerge around issues of data protection, and regional agreements remain in flux. This deprives policymakers in countries lacking effective privacy protections of strong guidance and best practice upon which to base their own regulatory frameworks.

In this legislative void, countries worldwide are violating their citizens' privacy through activities ranging from conducting extensive surveillance without a legal basis and actively censoring the Internet to failing to protect the privacy of personal data and

digital communications. Such practices persistently violate the right to privacy whilst also threatening citizens' ability to exercise other basic human rights. As the right to privacy becomes more and more embattled across the developing world, there is an urgent need to educate citizens, policy-makers, legislators, members of the judiciary and law-enforcement officials about fortifying legal protections. Although technologies have the potential to be at their most transformative in developing countries, by providing individuals with the ability to access to information and justice, to express themselves, and to participate in local and global discussions in unprecedented ways, they have also contributed to a blurring of lines between the public and private spheres, and made possible unprecedented levels of interference with the right to privacy. This has prompted some to call for greater attention to be paid to the scope of the right to privacy.

Questions that demand attention have emerged, for instance, what is the meaning of 'privacy', or 'private communication', in the digital age? What are the privacy interests inherent in communications data transmitted over the internet or by mobile phone? How can privacy be adequately protected when the increasing convergence of civilian communications and intelligence collection is considered? This last question is particularly pressing considering States' growing focus on threats to national security, the scope of which has been repeatedly expanded to justify an increasing number of infringements upon citizens' rights.

**Why is it important for African States to adopt and enforce effective access to information and privacy protection policies?**

In order to address the issues outlined above, States must develop effective legislation and policies surrounding the issues of access to information and privacy. This is necessary, and would be beneficial, for a number of reasons.

**1 – To address the impact of surveillance on fundamental human rights**

In his report to the 23rd session of the Human Rights Council, the UN Special Rapporteur on the right to freedom of opinion and expression, Frank La Rue, explored the relationship between state surveillance, privacy and freedom of expression. La Rue's report highlighted the limitations that undue interferences with privacy can have on the free development and exchange of ideas, and noted in particular the importance of protecting correspondence – both online and offline – from unnecessary inspection by State organs or third parties. Examining the possible impact of surveillance on citizens' ability to exercise other basic human rights, La Rue pointed out that restrictions in anonymity of communications might, for example, make victims of abuse reluctant to report incidents for fear of double victimization. This is just one example of the many ways in which inadequate privacy protection can undermine the principles of democratic society. It is essential that citizens are protected from unnecessary, unjustified, disproportionate or illegal surveillance, online or otherwise, not only because of the importance of the right to privacy, but also in order to avoid inevitable infringements upon other rights.

**2 – To prevent data protection legislation from negatively affecting trade**

Africa's increased trade with Europe and the rest of the world has introduced pressure for States to ensure that their data protection laws and directives are in line with those required by countries with which they wish to conduct business. The development of the Internet, the operations of multinational corporations, and the transnational flow of data that these entailed, have led a growing number of countries to adopt legislation to govern the processing of personal data from which individuals can be identified – a process with clear implications for citizens' right to privacy.

Article 25(1) of the European Union's Directive on the Protection of the Individuals with regard to the Processing of Personal Data and the Free Movement of such data

Directive 95/46/EC specified that EU member states must prohibit the transfer of personal data to non-member states that cannot guarantee an adequate level of data protection. The processing of personal information must be undertaken in a manner that recognizes the rights of those outside States as well as within them.

It is clear, therefore, that the implementation of data protection legislation would be beneficial from the perspective of protecting individuals' privacy - legislation based on models used by countries complying with the EU Data Protection Directive would be likely to require individuals to consent to having their personal information processed; to introduce mandatory notifications of data breaches; and to limit the processing of information relating to religious beliefs, race or ethnicity, trade union membership, sexual orientation, and political opinions. Furthermore, the economic impacts of failing to meet EU data protection standards would be severe, prohibiting States that are unable to meet such standards from trading with countries within the EU.

**3. To safeguard honour and reputations**

The need to safeguard honour and reputation is expressed in Article 17, and the importance of ensuring that personal and private information is well protected is clear when the potential effects of leaked or misused information relating to political or governmental figures are considered. Particularly in the context of Africa, many parts of which face ongoing struggles to ensure free and fair elections and political representation, the possibility that personal data belonging to political opponents, or former or aspiring government figures will be obtained and misused with the intention of causing reputational damage is very real. This would threaten not only the honour of the individuals concerned, but also the development or establishment of democracy, as there is a chance that any information obtained will be used to punish political opponents, or to suppress legitimate criticism and dissent.

**4. To regulate the use of big data**

There are emerging developments in areas that increase availability of big data. This relates to big data that is both available from the public sector, such as national health statistics and infrastructure data, and that which is sourced from the private sector, such as information held by telephone network providers and Google search details. This has the potential to be beneficial in many African States in terms of facilitating socio-economic and political developments. However, they also pose a serious threat to personal privacy in countries that do not have strong legal frameworks in place to protect fundamental human rights.

The personal data required for initiatives such as national identity systems or border control programmes, which often involve the use of biometrics technology like fingerprinting and iris recognition, is open to abuse. This is especially the case if such schemes are operated in a legislative void that fails to regulate the manner in which the data is processed, used or stored. This is the case in many countries that do not have data protection laws in place or designated information commissioners to provide avenues for redress in cases of negligence or abuse. Similarly, the highly sensitive data collected for the purposes of social protection programmes – for example, information that has been used for the World Bank's Cash Transfer for Orphans and Vulnerable Children project in Kenya or to enable healthcare fee waivers in Uganda – relates to the most intimate details of people's lives, and must be protected in order for the schemes to be fully beneficial.

**The Way Forward**

Several African countries and regions have already taken steps toward protecting the right to privacy, both online and offline. Nearly all African countries now recognize a specific right to privacy in their constitutions, and some States have introduced legislation to assist with the protection of this right. Several have also demonstrated

recognition of the importance of protecting the right, through their subscription to various international covenants and declarations. Nigeria, Tunisia and Ghana, for example, have supported the 2013 UN resolution on online privacy. Sub-regional entities such as the Economic Community of West African States (ECOWAS) have also created agreements that contribute to the protection of the right to privacy, such as a supplementary act on the protection of personal data in 2010, and a directive on fighting cyber-crime within the community in 2011.

These steps are encouraging, but a number of challenges and questions must still be explored before an effective legal framework to promote and protect the right to privacy in the digital age can be implemented.

***National Legal Frameworks:*** The first challenge relates to the manner in which respect for the right to privacy is guaranteed by legislative, administrative or judicial authorities. Effective national legal frameworks are critical to ensuring protection against unlawful or arbitrary interference. Yet in general, national legislation has not been adopted or adapted to match developments in communications technology and the surveillance measures these developments have facilitated. Where a framework has been created, it has frequently been geared towards legalising and abetting surveillance under the guise of national security protection, and tended to disregard the effect of such surveillance on citizens' other rights - particularly the right to privacy.

Further challenges are presented by the fact that in many jurisdictions there is a lack of independent oversight with the mandate to review surveillance measures in order to provide a safeguard against abuse. In other cases, a lack of regular judicial oversight allows intelligence services to operate entirely without constraints or accountability.

***National Security surveillance:*** A second, related difficulty concerns the definition of legitimate parameters for national security surveillance. 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 must be raised over the potential for national security overreach when adequate safeguards are not in place to protect against abuse. Several countries have already adopted draconian anti-terrorism laws that present serious challenges to the principles of the proportionality and necessity of surveillance. Notably, Kenya's Prevention of Terrorism Act 2012 explicitly allows for the limitation of the rights and fundamental freedoms provided in the Constitution for the purpose of investigating, detecting or preventing a terrorist act, stating that the right to privacy can be limited to allow communications to be 'investigated, intercepted or otherwise interfered with.'[1] The Act grants courts the right to require communications service providers to 'intercept and retain specified communication of a specified description received or transmitted, or about to be received or transmitted by that communications service provider',[2] and the right to permit police officers to 'enter any premises and to install on such premises, any device for the interception and retention of a specified communication and to remove and retain such device.'[3] Tanzania's Prevention of Terrorism Regulations 2012 are similarly concerning, so is Uganda.

***Enforcement:*** A third 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.

***Businesses:*** The final challenge relates to the responsibility of businesses themselves to respect privacy rights in the digital age. How do states ensure that corporations in the communications and technology industry respect the right to privacy and other related human rights? Responsibility for effective privacy protection cannot fall on governments

[1] Kenya Prevention of Terrorism Act 2012, 35.3.iii
[2] Kenya Prevention of Terrorism Act 2012, 36.3.a
[3] Kenya Prevention of Terrorism Act 2012, 36.3.b

alone, but must also be borne by relevant stakeholders and involved parties. In particular, vendors of surveillance technology facilitate intrusive ongoing surveillance, as do companies and corporations that fail to take adequate steps to protect their users from breaches of their privacy.

Again, States have an obligation to protect individuals against violations not only by their own agents, but also against breaches carried out by private persons or entities, including businesses. The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, set out a global standard for preventing and addressing adverse impacts on human rights linked to business activity. There have been important multi-stakeholder efforts to clarify their application to the communications and information technology industry. One of the challenges, of course, lies in the transnational nature of the communications and information technology industry, which can create legal and jurisdictional hurdles to the effective protection of the right to privacy.

**Suggested Steps**

**1. The strengthening of regional and sub-regional privacy and human rights protection mechanisms**

In order for privacy to be adequately protected, it is necessary for States to take advantage of existing regional and sub-regional protection bodies and mechanisms, such as the African Commission on Human and Peoples' Rights (ACHPR), and for relevant practices implemented by such over-arching bodies to then be adopted by individual States. Although several existing provisions have the potential to assist States ensuring the protection of various rights, including the right to privacy, their efficacy is dependent upon the full participation of member States. Notably, Article 62 of the ACHPR requires States to submit periodic reports detailing the legislative and other measures that they have adopted to give effect to the rights guaranteed by the Charter - including the right to privacy. Theoretically, this system provides an opportunity for the African Commission to monitor how effectively the rights are being protected, and to

identify factors that might be impeding the effective implementation of the Charter. However, the number of States regularly submitting reports is low, and prevents the article from reaching its full potential.

The ACHPR must itself also be more vocal on the issue of privacy protection, and take steps to ensure that the right is protected according to national and international standards. It would also be beneficial for organs like the ACHPR to promote collaboration between States on such issues, in order to facilitate the development of regionally appropriate best practice. This could then be used at a national level to strengthen existing protections through the introduction of optional protocols. ECOWAS provides an example of an existing sub-regional framework with the ability to implement policies and protocols addressing issues affecting its fifteen member States.

**2. The strengthening of domestic national systems for protecting privacy.**

Alongside strengthening and increasing the use of regional and sub-regional systems for privacy protection, individual States must put in place effective domestic judicial oversight mechanisms, and must also ensure that effective methods by which to redress breaches of privacy exist. Laws must be put in place to protect privacy, but legislation is insufficient without means of enforcing it. The creation of independent committees – separate from political roles – that are responsible for investigating and addressing breaches of human rights may help in this regard, and would also help to address the lack of transparency and accountability that currently facilitates violations of human rights in many States. Ensuring that citizens have secure and confidential avenues through which to report privacy-related concerns is also essential.

Furthermore, it is important to ensure that those responsible for overseeing issues relating to digital and online privacy have expertise in this field; the pace of technological developments demands that those operating in this area have the up-to-date knowledge necessary to effectively deal with problems arising from new technology, whether or not legislation is in place to specifically address the issues

faced.

A significant step towards strengthening domestic systems, as well as regional systems to an extent, would be the adoption of the 13 International Principles on the Application of Human Rights to Communications Surveillance, which provide a framework by which States, and organisations operating within them, can evaluate whether surveillance laws and procedures protect international human rights including those to privacy and freedom of expression. They govern surveillance activity conducted within States and extraterritorial activity, and serve to provide a check against activities conducted by the State or non-State actors that infringe upon fundamental human rights.

The principles set out the need for limitations to privacy to be prescribed by law, conducted to achieve a legitimate aim, necessary to achieve that aim, proportionate to the aim pursued, and adequate to fulfil the intended purpose. They call for decisions relating to communications surveillance to be made by an impartial and independent judicial authority, for such decisions to follow due process, and for the individuals concerned to be notified of the authorisation of communications surveillance and given adequate time to appeal against the decision. They state the need for transparency about the scope and use of surveillance techniques and powers, and for independent mechanisms of public oversight to be put in place to ensure transparency and accountability. Regarding cooperation with foreign service providers, they call for safeguards for international cooperation to be established to ensure that in cases of mutual assistance, the highest level of protection for individuals' rights is applied, and also call for safeguards against illegitimate access to be implemented, criminalising illegal communications surveillance. Finally, the principles clarify that the integrity of communications and systems must be protected, and that service providers or software or hardware vendors should not be compelled to build surveillance capabilities into their systems.

A commitment to adhere to these principles, which have now been co-signed by over 400 organisations from around the world, would be a significant step towards

acknowledging the importance of protecting human rights in the face of technological developments that make more personal information than ever before accessible through surveillance, and would provide guidance to States as they consider the reform of their agencies' polices, practices and structures to align themselves with human rights standards. These principles embody, but go beyond the safeguards laid out in international treaties including article 17 of ICCPR and Human Rights Committee General Comment 16 on the Interpretation of article 17 and General Comment 31 on the nature of the general legal obligation imposed on State Parties, other developments at the Human Rights Council, e.g. Frank Larue's Report to the Human Rights Council as well as other international discussions and recommendations on best practice. The 13 Principles have completely changed the debate around communications surveillance. By providing a detailed, clear interpretation of human rights standards that is relevant and meaningful in the digital age, the 13 Principles have done what so many national legislatures have failed to do - update long-standing legal protections of the right to privacy in the light of new technologies that challenge traditional distinctions such as content vs. metadata, nationals vs. non-nationals, intelligence vs. law enforcement.

**3. The training of officials and sensitization of civil society to know their rights and to demand protection of such rights.**

Finally, at a fundamental level it is important that individuals are aware of the rights, both online and offline; that they are able and willing to demand that these rights be protected; and that in cases of violation they can seek redress. Steps toward achieving this may include public information campaigns about the impact of breaches of privacy, alongside the aforementioned development or strengthening of avenues by which breaches can be reported. Furthermore, the adoption of the International Principles mentioned above would provide individuals and civil society groups with a benchmark that could be used to evaluate State practices and advocate change at a national level.