Zimbabwe Human Rights NGO Forum

NORWEGIAN MINISTRY OF FOREIGN AFFAIRS

PRIVACY INTERNATIONAL

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

State Surveillance in the digital age: the implications for freedom of expression and the right to privacy

Are privacy and expression protected in Zimbabwe?

By Arthur Gwagwa and Charlie Blagbrough
Zimbabwe Human Rights NGO Forum
4 June 2013

Many Zimbabweans are used to living with their rights to free expression and privacy repressed. In many ways, surveillance in the digital age is simply an extension of the monitoring which political activists and Human Rights Defenders face in everyday life. This is despite the fact that, on paper, Zimbabwe has an extensive set of constitutional rights. In theory, the twin rights of privacy and freedom of expression are protected. Under Article 17 of the Lancaster House Constitution individuals were protected from arbitrary searches and entry onto their property. Article 20 protected a person's private correspondence, and also enshrined freedom of opinion and the free exchange of information. However, the widely-reported political violence which followed the 2005 election showed that, in practice, these rights are often not respected.

Still, the state's commitment to these rights was reasserted in 2008. The 'Global Political Agreement' (GPA), which the three main parties signed, largely brought an end to the violence. In the GPA the government recommitted itself to respect for free expression (Article XII) and association/assembly (Article XIX). But the GPA's veneer of reform merely hid a bigger problem. In Zimbabwe there are many pieces of legislation which actively encourage surveillance. In the GPA these laws were named. In practice constitutional rights are qualified by these laws so that privacy and free expression remain largely illusive and non-justiciable.

Perhaps the digital age can finally bring real change in Zimbabwe. As the esteemed delegates will be aware, on the 22nd May, Zimbabwe signed its new Constitution into law. The rights to expression, assembly and association are reaffirmed in articles 58 to 60. More significantly, the language of privacy has finally entered into constitutional discourse. Privacy stands as a right on its own through Article 57, which protects Zimbabweans against arbitrary searches

of their person and prevents unlawful entry into their homes, premises or property. It prevents disclosure of health conditions to third-parties and, most importantly for our purposes, it also seeks to the infringement of private communications.

Free expression boiled down to digital communications

In order for the new constitution to bring any real change, however, there must first be whole-scale reform of Zimbabwe's statute books. As mentioned, there are a number of laws which actively encourage surveillance and the repression of free expression. Most of these laws, however, cater towards traditional forms of human surveillance. The state uses its security forces to break into properties and search them, or to monitor and disrupt meetings. Informants are employed in order to keep track of the state's opponents. These forms of surveillance will have to change to meet the demands of the digital age. For, given the remote nature of internet usage, a traditional meeting could in future be conducted over a skype conference call instead.

Communications surveillance will become the main tool for cutting across the anonymity, rapid information sharing and cross-cultural dialogues of the digital age. Though old in the context of technological innovation, the 2007 Interception of Communications Act (ICA) has kept pace thanks to extremely wide drafting and the creation of blanket powers. Though designed primarily for post and telephone, ICA's long title states that it can still be applied to 'any other related service or system'. This provides broad powers to intercept any kind of communication, no matter how technologically advanced it is.

Just as post is intercepted or a phone line is monitored, the state also has the power to snoop on communications travelling by email or across a social network. Having set up a Monitoring of Interception of Communications Centre, manned by 'technical experts', and appointed by the Minister of Transport and Communications, the state has the legislative and institutional apparatus in place to subject Zimbabwean's digital communications to the same surveillance as any other. As the UN Special Rapporteur (A/HRC/23/40) notes, the inspection of emails prior to reaching the desired recipient is still a breach of the right to private communications.

Involving ISPs

It must be noted however that, with an Opennet estimation of about 11% in 2009, internet penetration in Zimbabwe, though relatively high in Africa, is low by world standards. In 2007 Opennet found no evidence of the state filtering websites. However, a more recent 2012 report by Freedom House reports a huge increase in smart phone usage, especially amongst young people. Between 2006 and 2011 it is estimated that growth of mobile phone has gone from 6.8% to 72.1%. Many Zimbabweans use their phones and laptops to browse facebook, the country's most popular website, and to use whatsapp, a kind of internet text message service.

However, the worldwide trend of social media being used to express political opinions, and even to form campaigns online, has not been followed by most Zimbabweans. Freedom on the Net reports that, 'the lack of anonymity…and fear of repercussions limit politically-oriented statements which can be traced back to those expressing them'. Facebook is of course a largely public forum, and there have been instances of Zimbabweans being arrested because of their posts. Where facebook is concerned the state can still make use of human

surveillance techniques. Employing state agents to monitor the pages of human rights defenders and activists, in the form of what the UN Special Rapporteur calls 'mass communications surveillance', might still be an effective tool.

Case Study: The Facebook subversion trial

A supporter of the MDC-T opposition party reportedly put a post on facebook which drew parallels between the Arab Spring and the political situation in Zimbabwe. He was arrested and spent a month in jail. Eventually his trial collapsed because the post had been deleted and could not be offered as evidence.

These worries are compounded by the complicity of Zimbabwean Internet Service Providers (ISPs). ISPs are required, under section 9 of ICA, to put in place the hardware and software required for the state to carry out surveillance. Reports in Zimbabwe suggest that at least three of the main Internet Service Providers - Econet, TelOne and Telecontract – have complied with this requirement. Other reports, which cannot be confirmed, suggest that the state is buying surveillance technologies from a number of repressive regimes and even UK internet security companies. According to Freedom on the Net 2012 the Postal and Telecommunications Regulatory Authority of Zimbabwe banned the use of Blackberry Messenger because the service uses encrypted messages. This does not comply with the requirement in ICA that 'all telecommunication services should have the capability of being intercepted.'

Encryption and anonymity

On the other hand, there are questions regarding the state's ability to deal with other forms of encryption and anonymity. These technological developments have enabled a form of 'WikiLeaks' to take hold in Zimbabwe. Blogs and pseudonymous articles posted on internet newspapers also provide sources of media which are not controlled by state-dominated monopolies. On Facebook a source of reports about state corruption, published under the handle of 'Baba Jukwa', is followed by over 100,000 people. The accuracy of these reports is difficult to confirm or deny, because anonymity means that 'Baba Jukwa' is virtually unaccountable. However, the example shows the potential for technology to drive social change, to empower civil society, and to bring about greater state transparency.

Case Study: Baba Jukwa

Having emerged on Facebook in January 2013 Baba Jukwa has rapidly become established as a major source of online political news in Zimbabwe. It is thought to be run by a member of the ruling ZANU-PF party. Many of the posts centre on accusations of state corruption and violence. Reportedly, the government is undertaking an intense campaign to find the poster's identity. On May 31st the State Security Minister publicly announced his worries that 'Zimbabwe is under cyber attack'.

Rapid Information Sharing

Technological change has not only increased the speed of communications within Zimbabwe. It has also connected Zimbabwe to the rest of the world. Since many eminent Zimbabwean commentators are based abroad they are not under the same danger of arrest as those based domestically, and so can express themselves with more freedom. Furthermore, the news cycle now moves so quickly now that big news in one part of the world is big news all over. This was the case with the Arab Spring, videos of which made it into Zimbabwe and became a topic for discussion by opposition activists.

Case Study: Arab Spring videos

During a public lecture in Zimbabwe activists showed footage of the protests in Egypt. The police raided the lecture and arrested 45 people. Eventually charges were brought against six activists, who were convicted of inciting public violence in March and given community sentences.

The fact that the Arab Spring videos made it into the country shows the difficulty of preventing information sharing over the internet. However, equally the work of the police breaking up the lecture shows that human surveillance can still play a part in preventing the dissemination of information within Zimbabwe's borders.