Legal, Policy, Ethical and Technical implications of Zimbabwe's proposed Cyber Crime Law

By Arthur Gwagwa Esq.

14 December 2014

According to reports from Zimbabwean media activists, the Zimbabwean government is increasing its computer forensics investigation capabilities through a proposed cyber-crime law, which is still at draft bill stage. If passed, this law would allow the authorities to remotely install spying tools onto a person's device. A magistrate could authorize such actions if they are satisfied on the basis of an application by a police officer. The application would need to state that there are reasonable grounds to believe that applying non-invasive instruments listed in the bill cannot collect essential evidence, which is reasonably required for the purposes of a criminal investigation. In a related development, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is proposing compulsory sharing of base stations with local Internet Service Providers (ISPs), although the plans have been temporarily shelved due to technological incompatibility between government and ISPs base stations.

While computer forensics investigation is not a new field and is widely practiced in several jurisdictions, it raises a number of legal and ethical considerations and can potentially overreach into private lives of citizens. In the U.S.A, a number of decisions have been made on its implications on the Fourth Amendment, and this likely to also be the case in Zimbabwe where the twin rights to privacy and free expression are already embattled. This article examines some of the legal, policy and ethical considerations that the government, especially Parliament, ought to consider before passing the proposed bill into law. By drawing regional comparative case studies, the article also examines how the proliferation technologies, and laundering of policies and laws of is having a knock on impact on democracy on the African continent

Technological & Legal Implications: North American Comparative Experiences

Zimbabwe needs to carefully take into account the legal, technological, policy and ethical challenges that other jurisdictions have faced in implementing computer forensic investigation. Firstly, the volatile nature of electronic evidence may raise serious admissibility challenges, leading to proliferation of evidence suppression or interlocutory hearings. This is particularly the case since computer forensic data is amenable to manipulation through formatting and deletion.

Secondly, it is not clear whether the term "computer" will cover all mobile devices. If it does, it is not yet clear whether the government has considered both technological and practical challenges inherent in bugging mobile devices through the installation of a forensic device, given that mobile careers are usually in the possession of the user.

With regards to the first challenge generally applicable to all computer devices, it is important for the government to be aware that electronic data is very susceptible to alteration or deletion, whether through an intentional change or from the result of an invoked application in some computing process. David W. Bennett, in his article 'The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations' dated August 20, 2011, looks at some of the challenges. For example, 'as electronic data is created, modified or deleted through the normal operations of a computing system, therein lies the possibility of modifications arising from an incorrect or inappropriate digital forensics process.' Given that the results of such actions can be treated as critical evidence in a case, it is essential that every measure be taken to ensure the reliability and accuracy of the forensics process. A digital forensics process must be developed and applied with due regard to jurisprudence issues, such as the need for thorough examination.

While computer forensics in law enforcement can protect commercial and personal safety, the policy goals of law enforcement must be balanced with the goals of

maintaining personal liberty and privacy under the law. Computer forensic investigators invariably face ethical dilemmas and they must exercise their discretion wisely, balancing their prosecutorial zeal with respect for citizens' individual liberties.

The American Civil Liberties Union (ACLU) have raised concerns on whether the police can snoop through one's cellphone during an ordinary traffic stop in a letter dated 13 April 2014. `The letter was directed to the Director of the Michigan State Police, where forensic analyzers are routinely used in police investigations to recover data from computers and other digital devices. While this type of forensic device is nothing new in Michigan, the ACLU's concern is that such searches might violate constitutional guarantees against invasive and unreasonable search and seizure. Lately, one phone can include almost all of an individual's private communications (e.g., SMS, recently dialed numbers, email, Facebook and Twitter posts) as well as location data from the device's GPS unit.

The question of data forensically harvested from computers and mobile careers has been subject to contestation not only in the U.S Courts but other policy fora. It is therefore important to briefly look at some of these decisions and discussions. The court cases and discussions might be helpful in shaping the ongoing discussions in Zimbabwe. North American jurisprudence on the issues has developed in leaps and bounds.

In the case of *Smith v. Maryland,* 442 U.S. 735 (1979), the Supreme Court of the United States held that the installation and use of the pen register was not a "search" within the meaning of the Fourth Amendment, and hence no warrant was required. The pen register was installed on telephone company property at the telephone company's central offices.

However in *United States v. Jones*, 132 S. Ct. 945, 565 U.S. ___ (2012), the United States Supreme Court held that installing a Global Positioning System (GPS) tracking device on a vehicle and using the device to monitor the vehicle's movements constitutes a search under the Fourth Amendment.

In *R. v. Spencer, 2014 SCC 43,* the police identified the Internet Protocol (IP) address of a computer that someone had been using to access and store child pornography through an Internet file-sharing program. They then obtained from the Internet Service Provider (ISP), without prior judicial authorization, the subscriber information associated with that IP address. The Supreme Court of Canada, while condemning the act of child pornography, made a decision on the legality of the search without judicial authorisation and held that the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest that engages constitutional protection against unreasonable search and seizure.

Finally in *Riley v. California*, 573 U.S. ___ (2014), the United States Supreme Court unanimously held that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional.

The 2014 Cato Institute Surveillance Conference held on 12 December 2014 (CATO Conference) also explored the issue of mobile devices and how the law enforcement will deal with encryption, like the encryption built in the Apple's realtime iMessage, FaceTime and iCloud. Encryption certainly does affect criminal investigations and commercial encryption is protected under the U.S Patriot Act. In the circumstances, would the government ask service providers to provide either hardware or software backdoors, and what would be the ethical considerations for Apple, given that they explicitly promise their customers the right to privacy and never to decrypt? The other challenge posed by backdoors is the vulnerability to criminal elements; therefore backdoors are not only a moral threat but can harm economic interests. The backdoor challenge to the law enforcers might increase the risk of reliance on hacking by law enforcement, for example by infecting computer with malware. Apple, for example, might respond to this threat by helping their consumers to update their encryption software applications through iPlayer.

While cases relating to computers may be easy to deal with, this is not the case with mobile devices. If the government cannot legally compel service providers to decrypt, then they might be forced to compel someone to give up their password? In this case,

what are the individual rights under both the Fourth and Fifth amendments? Perhaps the law enforcement agencies would have to call the suspect and establish that the device they would like to access is linked to the suspect's cell phone number or track them and pounce on them when their phone is unlocked.

Technological and Legal Implications: Zimbabwean Experiences

The problem of keeping up step with technology is particularly acute in Zimbabwe. 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.' It is not clear what Zimbabwe's position is in relation to Apple products.

In 2013, forms of encryption and anonymity enabled a form of 'WikiLeaks' to take hold in Zimbabwe under the handle 'Baba Jukwa'. When the suspect behind the Baba Jukwa Facebook account was subsequently identified, the case against him partly failed because of the technological challenges, which were raised in the initial suppression of evidence hearing. During his bail hearing, the court ordered him to surrender the password to his Gmail account, which was connected to the mobile line, which was registered in his name. However, while he was still in detention, somebody continued to operate his account, raising new fears of the possibility of cellphone line mixtures. This subsequently prompted the state to send those who were investigating the case to the US to seek advice from social network and search engine providers, Facebook and Google respectively. Up to now, it is not clear what sort of support the Zimbabwean authorities got from the U.S where convictions on computer-related offences are very low due to both technological and legal barriers pointed out above.

Policy Implications: US Experiences

It is ironic that African governments are laundering policies and technologies from the developed world without a full appreciation of the challenges that these developed countries, such as the U.S, are facing. For instance, the CATO Conference explored

how even ordinary law enforcement agencies are increasingly employing sophisticated tracking technologies, from face recognition software to “Stingray” devices that can locate suspects by sniffing out their cellular phone signals. It further explored whether these tools are a vital weapon against criminals and terrorists — or a threat to privacy and freedom. It also explored how such tools should be regulated by the federal authorities so the secrecy that spying demands and the transparency that democratic accountability requires can be reconciled.

The CATO discussions raised very interesting views, which are very relevant to the current discussions in Zimbabwe. For example, the need to think of policy goals and objectives before passing laws was raised. Just like in Zimbabwe where the government has been proliferating surveillance-related legislation, some within the U.S. legal community are of the view that the Patriot Act was unnecessary. Most of the issues it addresses are either covered under The Foreign Intelligence Surveillance Act of 1978 ("FISA" or Executive Order 12333 United States Intelligence Activities (Executive Order 12333), therefore they feel that the Act was passed to solve a non-existing problem. The intelligence community had failed in that they didn't use information they had to avoid 9/11. There is therefore need to roll back the surveillance powers and focus them on where they are needed.

Secondly, while the goal to fight impunity is legitimate, it is not appropriate for local law enforcement to deploy heavy technologies ordinarily used by the military. These technologies can be highly invasive and with the current explosion big data, especially in the form of metadata, it is imperative that protection should be built into the law right now.

The third challenge in the U.S, which is also found in Africa, Zimbabwe in particular, is that law enforcement often use these technologies way before they are allowed to do so by Congress and keep their usage under wraps. The law usually steps in the game quite late, for instance, government often regularize the usage of these technologies either after lawyers have filed motion to suppress evidence obtained through surveillance or if the media has raised the issue. A recent example in the U.S relates to

a story reported in the Charlotte Observer on 18 October 2014. The Charlotte North Carolina Police's asserted that they had a court order to use the StingRay device but when the judge responsible for issuing warranties was asked if he issued a warrant for such a device, he responded that he had never heard of such a device. According to a story reported in the Baltimore Sun on 18 November 2014, a judge threatened a detective with contempt for declining to reveal cellphone tracking methods they use in criminal investigations. The future remains uncertain, since the legal system responds to technological developments very slowly and in a cumbersome way and when they do, court rulings are often very narrow which might prompt law enforcers to beg law makers to pass new laws to in response to new technologies.

Policy Implications: Zimbabwean Experiences

In the case of Zimbabwe, one needs to fully understand the background and context to the proposed law in order to make an informed conclusion.

Firstly, it is not very clear what the new proposed law will achieve that is not being achieved by the current Interception of Communications Act (ICA) 2007. This law gives the Zimbabwean Government significant powers of surveillance over the communications of its citizens. According to the long title of the ICA, the aim of this legislation is to allow both the "interception" and "monitoring" of communications. Of course, both "interception" and "monitoring" are acts of surveillance, which infringe on the rights of an individual to communicate with others without interference from the state.

The powers contained in the ICA are also extensive with regards to the kind of communications, which can be intercepted. Powers are given specifically for the authorities to intercept post and telecommunications. However, the ICA can also be used to intercept communications sent on "any other related service or system". This compounds the impression that in drafting the ICA the Government intended for it to cover, as much as possible, any modern technological developments like email, social media such as Twitter and Facebook; internet audio and visual telecoms like Skype; and computer forensic devices as contemplated under the proposed cyber law.

These worries are compounded by the complicity of Zimbabwean Internet Service Providers (ISPs). Under section 9 of ICA, ISPs are required to install, at their own expense, 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 Telecel – have complied with this requirement.

It appears the only difference between the ICA and the proposed Cyber-security law is that rather than installing the monitoring device with the complicity of the service providers, this law would allow the authorities to remotely install spying tools onto a person's device.

Secondly, while under the ICA, the minister is the arbiter under the proposed law; judicial authorization from a magistrate is required.

Thirdly, while the ICA implicitly deals with wide national security concerns, the proposed law deals with investigations of a criminal nature, which appears to distinguish national security from criminal activities.

The other nuanced difference between the two laws is a technological one. The term 'interception' in the ICA automatically implies that the Act deals with networked computers and data in transit although the term 'monitoring' can also cover data either in storage or at rest whether in an ICU or cloud. The monitoring element, could for example, cover situations contemplated in the Canadian Spencer decision cited above. On the other hand, the proposed law states that the authorities would install a remote spy tool. This also seems to imply usage of remote malware devices such as FinFisher, which can be covertly installed on targets' computers by exploiting security lapses in the update procedures of non-suspect software. It is yet to be seen if the proposed law will cover installation of hardware spy tool to non-networked computers to harvest, for example, data at rest. For reasons stated above, this would present practical challenges in respect of mobile phones.

Although the proposed law is a step further from the ICA insofar as it requires the police

to obtain a search warrant, it does not take into account the level of the offence in conferring blanket jurisdiction on a magistrate. Given the low level of policing in Zimbabwe and the low standards of training for magistrates, leaving such an important area of national security and personal liberty to the discretion of a police officer and magistrate does not meet the threshold of adequate judicial oversight in line with international standards and norms.

Both the proposed law and the ICA have to be viewed in light of the new constitution passed in May 2013. Section 57 of Zimbabwe's constitution guarantees every person the right to privacy, which includes the right not to have the privacy of their communications infringed, among other facets. However, article 86, entitled "limitation of rights and freedoms", allows privacy to be limited by a law of general application which is held to be "fair, reasonable, necessary and justifiable in an open, just and democratic society" in the interests of "defence of public safety, public order, public morality, public health, regional or town planning or the general public interest."

In our previous report titled Communications & Political Intelligence Surveillance on Human Rights Defenders in Zimbabwe published in December 2013, which can be accessed here, we raised concerns over the wide drafting of the section. Although international best practice shows that the right to privacy is often considered to be a qualified right, there is no precedent for allowing a limitation to be as broad as "the general public interest." There is no indication what this could mean, which fosters worries that the Government could again seek to make Zimbabwean constitutional rights non-justiciable.

In the same way, section 86 limits the right to privacy, its effect in respect of the proposed cyber law is to make evidence obtained through computer forensic investigation admissible and compliant with the provisions of section 70 (3) of the Constitution which otherwise excludes evidence obtained in violation of the Declaration of Rights and in violation of section 57, for example evidence acquired through illegal searches or monitoring of communications, which must be excluded in criminal trials. Allowing the evidence to be submitted would render the trials unfair or would be

detrimental to the administration of justice or the public interest.

From October 2013, the Zimbabwe Government, mainly through the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), has been taking several cyber related national security measures which, if viewed in their totality, brings into question the issue of transparency and accountability in Zimbabwe's policing, especially the role of the security sector in an increasingly digitalized world. If viewed in the larger context of the events preceding the 2013 elections, for example, the state's increased control of data, and reckless statements by politicians, it is easy to come to the conclusion that the politicization of the intelligence cluster is one of the greatest threats to democracy not only in Zimbabwe but in the African region.

Here is some background. In October 2013, POTRAZ promulgated a Statutory Instrument, which established a central database of information about all mobile telephone users in the country. The Statutory Instrument extended the Zimbabwean government's reach into the private lives of its citizens as it raised new challenges to the already embattled rights to privacy and free expression in Zimbabwe, increasing the potential that the state would spy on its citizens and further clamp down on free speech. However, following an adverse report on the regulations by parliament in November 2013, the government repealed the Statutory Instrument following a court ruling that the instrument was unconstitutional, as it allowed third parties to access personal data without a court search warrant. POTRAZ attempted to re-introduce an amended version, which contained provisions for a search warrant, but the amended version was again rejected by parliament.

Further, in September 2014, the writer learnt that POTRAZ was in the process of drafting new cyber laws to regulate the activities of social media. The writer's attempts to find out the status of the drafting process have been futile. According to media practitioners in Zimbabwe, the proposed social media law is simply a reaction to the swelling increase of Internet usage and merely critical comments expressed online. It is not grounded on any principle and lacks a sufficient policy framework to balance public interest and state security. It is likely going to become another tool for repressing free

expression and curtailing online debates and information sharing.

Although these laws appear legitimate for the purposes of national security and public order, one needs to understand the background to these developments. In August 2014, there was huge public outcry and a social media saga, which exposed public officials' disquiet over Baba Jukwa. In a related incident the outgoing presidential affairs minister Didymus Mutasa was recently quoted in reports as saying, 'Those who continue to criticize President Robert Mugabe will have the secrets of their bedrooms exposed to the public because the government "sees everything".' This is

Despite the arguments in favour of national security, the proposed spy and social media laws are clearly designed to facilitate greater State surveillance, in light of recent statements by public officials and prior developments. Didymus Mutasa's statement not only threatens Zimbabweans' right to privacy but also civil liberties contained in the new bill of rights. This assertion is further backed up by the clandestine nature of the drafting process, which is not open to public consultation and participation as mandated by section 141 of the constitution. It is not acceptable for the government to use national security concerns as a blanket justification to excuse unwarranted privacy breaches; for example, the state has been using its surveillance capabilities to suppress freedom of expression deemed to be an insult to the person of the president and the uniformed forces under section 31 (a) (iii) of the Criminal Law Codification Reform Act. In a step, which was widely viewed as a step forward for the freedom of the press, the Constitutional Court made a landmark ruling when it struck down the law, which had been used to prosecute many journalists in the past. However, Mutasa's latest statements demonstrate the government's indifference to the court ruling.

Human rights, democracy and economic implications: Regional & International experiences

In Zimbabwe and across Africa, digital surveillance has not only impacted the right to privacy - with a knock on effect on other rights such as freedom of expression and association - but has also had a far reaching harm on citizens and the realization of

democratic aspirations and national security objectives. The OHCHR Report the Right to Privacy in the Digital Age observes that 'Digital communications technologies, such as the Internet, mobile smartphones and Wi-Fi-enabled devices, have become part of everyday life. By dramatically improving access to information and real-time communication, innovations in communications technology have boosted freedom of expression, facilitated global debate and fostered democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights. As contemporary life is played out ever more online, the Internet has become both ubiquitous and increasingly intimate. In the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection'.

Technologies, in particular those that enable states to conduct mass surveillance, though perhaps not to the same level as the US, have been flooding the developing world, especially Africa, as these are relatively easily shared. However, the technical knowledge necessary to design legislative frameworks to keep pace with these developments remain in short supply. African surveillance modalities do vary, are diversified, and do not always involve mass data retention but range from wire taping, data retention, filtering, spying technology, denial of service attacks and suppression of encryption technologies such as Blackberry messenger. Some modalities are being carried out from within but some from outside. African governments are constantly seeking for ways to enhance their surveillance technical capabilities and passing laws to justify such practices.

The main types of technologies fall into two categories: those developed by tech companies and state-sponsored spyware. The discussion of these is beyond this article's purview. Whatever form these assume, their impact on personal liberty is huge, especially in countries such as Ethiopia, where in February 2013, Citizen Lab research found that a finSpy campaign in Ethiopia uses Ginbot 7 as bait to infect users. When security researchers of Rapid7, a security firm scanned the Internet in 2012 for finFisher

– an internet surveillance software, only 11 countries IP addresses are found including Ethiopia's.

In a paper that the writer recently presented at a side event during the 27th Session of the Human Rights Council, titled *Impact of digital surveillance on journalists, HRDs and lawyers in Africa: Harm caused by surveillance beyond right to privacy*, the writer listed some of the harms that state surveillance can cause beyond the right to privacy including harm to democracy, electoral integrity and national security.

In the case of Zimbabwe's ICA, In addition to concerns about the wide drafting of the powers of the law, there is also concern about the lack of separation between the judicial and political roles in the Act. In particular, the main decision-maker arbitrating on whether to issue warrants is a Government Minister. This raises serious concerns of partisanship, the politicization of the intelligence services and the extent of state control over surveillance operations.

Apparently this is a regional phenomenon. According to Glenn Ashton, in his article South Africa: Watching the Watchers - the Case for the Moral Superiority of Hackers, Leakers and Citizen Watchdogs dated 3 December 2013, says that a direct result of this politicization of the intelligence cluster both in South Africa and in other developing states like Zimbabwe, Angola, Morocco and Egypt, is to shift the focus of intelligence agencies from their primary role toward support of the status quo within the dominant political infrastructure. This has left criminal networks increased freedom to operate and entrench their activities, says Ashton. In Zimbabwe, instances of invasive state surveillance on civil society were uncovered on almost a daily basis especially before the 2013 elections, with a knock on effect for the entire democratic process. It would seem a reasonable hypothesis to suggest that surveillance in Zimbabwe tends to increase during periods of high political activity. In fact, the evidence of surveillance surrounding the 2013 elections neatly supports this conclusion. In weeks during August 2013, several human rights and independent media organisations were hit by internet-based attacks, disabling their websites and preventing their users from accessing information. Among the sites that were immobilised were www.electionride.com which

was in the process of monitoring the election results. While it remains beyond the capabilities of such organisations to establish the true sources of these highly sophisticated attacks, their convenient timing so as to coincide with the allegedly irregular elections of that month led many observers to draw their own conclusions.

For the above reasons and other reasons, which the writer mentioned in the previous Article, Africa clearly needs to take urgent steps to protect the right to privacy. We recommend that the Zimbabwean Government should take measures to engage in broad based consultations before passing laws that impact civil liberties. Such laws must balance national security concerns and civil liberties by restraining political power in the cyberspace. Legislating away social problems and political dissent has far reaching impact on civil liberties, democracy and economic development. Some of most compelling arguments on this issue can be accessed here. In line with emerging best practice, in particular, the critical study by Ben Emmerson QC, the UN's special rapporteur on counter-terrorism, Mass Surveillance, Counterterrorism and Privacy: The Way Forward there is a need to differentiate between targeted surveillance, which follows a belief that its subject is involved in a specific act of wrongdoing, and bulk surveillance, which indiscriminately swallows up digital or telephonic communications data. This amounts to a systematic interference with the right to privacy of communications, and requires a correspondingly compelling justification. Zimbabwe's laws currently fail this test and require a wholesale revision.