30 November 2015

Ministry of Justice and Correctional Services
SALU Building
28th Floor, 316 Thabo Sehume Street
Pretoria
South Africa

Access Now comments to the Department of Justice and Constitutional Development, Republic of South Africa, on the Cybercrimes and Cybersecurity Bill 2015

About Access Now

Access Now is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world – including presence in the African Union - Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.

Access Now advocates an approach to digital security that promotes good security policies that protect user rights, including privacy and freedom of expression. Access Now has previously commented on the establishment of the African Union Convention on Cyber Security and Personal Data Protection ("the Convention").[1] We now welcome the opportunity to provide feedback on the draft Cybercrimes and Cybersecurity Bill 2015 ("the Bill") to the Department of Justice and Constitutional Development.

[1] See blogs from June 2014, August 2014 and February 2015 where we have highlighted on potentially good, bad, and ugly clauses and have encouraged AU member states to attach reservations to their ratification documents, noting concerns about the specific provisions we outline in our comments: Ephraim Percy Kenyanito, 'Africa moves towards a common cyber security legal framework' (*Access Now*, 2 June 2014) <https://www.accessnow.org/blog/2014/06/02/africa-moves-towards-a-common-cyber-security-legal-framework > accessed 16 November 2015; Access Policy Team, 'African Union adopts framework on cyber security and data protection' (*Access Now*, 22 August 2014) <https://www.accessnow.org/blog/2014/08/22/african-union-adopts-framework-on-cyber-security-and-data-protection > accessed 16 November 2015; Ephraim Percy Kenyanito, 'Emerging threats in cybersecurity and data protection legislation in African Union countries' (*Access Now*, 13 February 2015) <https://www.accessnow.org/blog/2015/02/13/emerging-threats-in-cybersecurity-data-legislation-in-africa-union > accessed 16 November 2015

Background

In 2009, the African Union came up with the Oliver Tambo Declaration whereby the AU engaged in an effort to harmonize various information and communications technology (ICT) regimes in the region, particularly around cybersecurity laws.[2]

Following the declaration, The African Union (AU) approved the African Union Convention on Cyber Security and Personal Data Protection in June 2014 at the 23rd Ordinary Session in Malabo.[3] The Convention covers a wide range of online activities, including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cybersecurity. Once in effect, the Convention requires AU states to enact personal data protection laws and develop a national cybersecurity strategy, pass cybercrime laws, and ensure that e-commerce is "exercised freely." African countries have begun to enact laws in an attempt to conform with the Convention.[4]

Subsequently, on 28 August 2015, South Africa's Department of Justice and Constitutional Development invited the public to comment on the draft Cybercrimes and Cybersecurity Bill.

Passing data protection and digital security protections are critical steps to enabling greater user control over personal data, increasing protection for privacy, and securing the internet for users. We commend the South African government for consideration of its international commitments and awareness of the need to improve the security of the digital environment, particularly in Africa. However, the current draft Cybercrimes and Cybersecurity Bill contains several provisions that risk infringing human rights and chilling cybersecurity research in South Africa and beyond. We would like to take this opportunity to provide comments and suggested improvements to the South African law.

Applicable Human Rights Law

South Africa is a party to the International Covenant on Civil and Political Rights (hereinafter, the "ICCPR").[5] The ICCPR establishes certain international rights, including the right to privacy (Article 17), the right to freedom of expression (Article 19), and the right to freedom of association (Article 22). In addition, South Africa is a party to the African Charter on Human and Peoples' Rights (Banjul Charter), which establishes the

---

[2] Oliver Tambo Declaration (adopted 5 November 2009) <http://africainonespace.org/downloads/TheOliverTamboDeclaration.pdf> accessed 16 November 2015

[3] African Union, 'The 23rd Ordinary Session of the African Union ends in Malabo' (*African Union*, 30 June 2014) <http://summits.au.int/fr/22ndsummit/events/23rd-ordinary-session-african-union-ends-malabo> accessed 30 November 2015

[4] Ephraim Percy Kenyanito, Emerging threats in cybersecurity and data protection legislation in African Union countries' (*Access Now*, 13 February 2015) <https://www.accessnow.org/blog/2015/02/13/emerging-threats-in-cybersecurity-data-legislation-in-africa-union > accessed 16 November 2015

[5] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

rights to dignity (Article 5) and freedom of information and expression (Article 9), among other rights.[6]

The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") provide a framework for protection of human rights against communications surveillance.[7] The Principles "apply to surveillance conducted within a State or extraterritorially" and include, Necessity, Proportionality, Transparency, Public Oversight, and Safeguards Against Illegitimate Access and Right to Effective Remedy.

Privacy

1. Section 29 of the Bill creates the standard for issuance of search warrants for access or seizure of any data, computer device, computer network, database, critical database, electronic communications network, or National Critical Information Infrastructure connected to an offense under the Bill.[8] It permits magistrates or judges of the High Court to only issue a warrant on a written application by a member of a law enforcement agency if there appears to be reasonable grounds to believe the article is within the jurisdiction of the judge or magistrate or used or involved in the commission of an offence within South Africa if the authority is unclear of the jurisdiction of the article. Alternatively, a magistrate or judge presiding at a criminal proceeding can issue a warrant if it appears the article is required in evidence at the proceeding.

2. The current language fails to create a standard for law enforcement that satisfies human rights requirements for surveillance. The principle of Necessity requires "[s]urveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State."[9] Further, the principle of Proportionality places the onus on the state to establish, among others requirements, that "there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and; there is a high degree of probability that

[6] African (Banjul) Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M; *see also* African Union Department of Political Affairs, 'Human Righs Strategy for Africa' (14 December 2011) <http://pa.au.int/en/sites/default/files/HRSA-Final-table%20%28EN%29%5B3%5D.pdf> accessed 16 November 2015

[7] International Principles on the Application of Human Rights to Communications Surveillance (May 2014) <https://en.necessaryandproportionate.org/> accessed 16 November 2015

[8] Article 27 notes that Chapter 2 of the Criminal Procedure Act applies as well. The Criminal Procedure Act requires only that the state show there are "reasonable grounds believed to be concerned in the commission or suspected commission of an offense" or that the action "may afford evidence of the commission of an offense." Criminal Procedure Act 1977 s 2(20) <http://www.saflii.org/za/legis/consol_act/cpa1977188/ > accessed 16 November 2015

[9] See above n.6

evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought."[10]

3. Digital communications is increasingly prevalent and law enforcement can access such communication with increasing ease. Laws governing communications surveillance should ensure compliance with international standards. Guidance on conforming language can be found in the Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance ("Implementation Guide").[11] The Implementation Guide includes guidance on the government application for information, judicial consideration, the search, appeals and remedies, and international cooperation.[12]

Recommendation: The Bill should only permit the issuance of a warrant for communication surveillance if the request satisfies the standards of necessity and proportionality.

1. Section 64 requires electronic communications service providers that are aware or become aware that their computer networks or electronic communications networks are being used to commit an offense under the Bill immediately report the matters to the National Cybercrime Centre. The providers must also preserve any information which may be of assistance to the law enforcement agencies in investigating the offence, including information which shows the communication's origin, destination, route, time date, size, duration and the type of the underlying service. Electronic communications service providers which fail to comply are guilty of an offence and liable on conviction of a R10,000 per day fine.

2. This requirement outsources cybersecurity and communications surveillance to service to service providers, threatening both privacy and freedom of expression. The principle of Integrity of Communications Systems says that "States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes."[13]

3. The U.S. and EU governments are considering passage of legislation and a Directive, respectively, similarly designed to increase the flow of cybersecurity information from companies to the government by reducing disincentives or requiring sharing.[14] Security and privacy experts have criticized such approaches

[10] See above n.6
[11] Access Now, 'Universal Implemention Guide for the International Principles on the Application of Human Rights to Communications Surveillance' (May 2015) <https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf> accessed 16 November 2015.
[12] The Implementation Guide provides guidance on other sections relating to the issuance of warrants
[13] See above n.6
[14] Cybersecurity Information Sharing Act of 2015 <https://www.congress.gov/bill/114th-congress/senate-bill/754> accessed 16 November 2015; Network and Information Security Directive

for failing to protect user privacy while not doing enough to secure users.[15] The then UN Special Rapporteur on Freedom of Expression Frank La Rue has noted the right to private communication "gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties."[16]

Recommendation: The Bill should not include a mandate that electronic communications service providers report incidents to the National Cybercrime Centre. Participation should instead be optional, and incorporate strong safeguards to protect user security and privacy.

Transparency

1. Section 38 says "[n]o person, investigator, member of a law enforcement agency, electronic communications service provider or an employee of an electronic communications service provider may disclose any information which he, she or it has obtained in the exercise of his, her or its powers or the performance of his, her or its duties" in the Bill. It provides exceptions for transferring if the individual or recipient are performing duties under the Bill, if the information is required in law or is evidence in court, constitutes information sharing under the Bill, or to a competent authority for the institution of criminal proceedings or an investigation. The penalty for a person, investigator, member of a law enforcement agency, electronic communications service provider, or an employee of an electronic communications service provider who contravenes Section 38 is guilty of an offence and liable upon conviction for a fine of no more than R5 million, imprisonment not exceeding 5 years, or both.

2. The principle of Transparency says that the state "should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each." Further, "States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State

---

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048> accessed 16 November 2015

[15] Letter of Civil Society Organizations, Security Experts, and Academics to Chairman Burr, Vice Chairman Feinstein, and Members of the Senate Select Committee on Intelligence on the Cybersecurity Information Sharing Act of 2015 (2 March 2015) <https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/03/CISA-2015-Sign-On-Letter.pdf> accessed 16 November 2015; 'Network and Information Security Directive' (*Open Rights Group*) <https://wiki.openrightsgroup.org/wiki/Network_and_Information_Security_Directive> accessed 16 November 2015

[16] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 7 (17 April 2013) A /HRC/23/40 <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf > accessed 16 November 2015

requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance."[17]

3. Service providers have a duty to respect human rights in their operations, including the right to privacy,[18] and their business models depend on gaining the trust of their customers. Barring them from disclosure of government requests impacting customer privacy prevents the providers from meeting their human rights responsibilities, and impedes them from transparently communicating with users.

4. Disclosure of public records of government requests issued under this Bill, even if in aggregated form, can bring useful transparency to the operation of the Bill. As written, this order would potentially interfere with the ability of law enforcement agencies and service providers to issue records of requests for communications surveillance and the text should be modified to permit such activity.

Recommendation: The Bill should require law enforcement to publish records of requests for communications surveillance, and clarify that service providers have the authority to publish such records.

Cybersecurity Research and Online Expression

1. Section 4 of the Bill makes it an offence for an person to "unlawful and intentional access to the whole or any part of" data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure. A person contravening through unlawful and intentional access to data, a computer device, a database, a database, or an electronic communications network, is liable on conviction for a fine not exceeding R5 million, imprisonment of a period not exceeding 5 years, or both. A person contravening through unlawful and intentional access to a critical database or a National Critical Information Infrastructure, is liable on conviction for a fine not exceeding R10 million, imprisonment of a period not exceeding 10 years, or both. For the section, "access" includes, to "make use of," "view," or communicate with," among other actions. Actions of a person are unlawful to the extent that they exceed lawful authority to access.[19]

2. Section 4 fails to offer guidance as to when access to such systems exceeds an individual's lawful authority. As written, this section is overbroad and will inevitably chill important security research, whistleblowing activities, and journalism. Harsh penalties and failure to offer protections for socially desirable activities will limit the use of information critical to the public interest.

[17] See above n.6
[18] United Nations Office of the High Commissioner, Guiding Principles on Business & Human Rights (2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> accessed 16 November 2015.
[19] Sections 4 through 10 similarly create offenses for unlawful activities. Protections for security research, whistleblowing, and journalism should similarly be addressed.

3. Security researchers find and demonstrate the existence and extent of systems vulnerabilities. Sometimes this is accomplished by employing equipment and software designed to penetrate and access computer and other digital networks.[20] Security research, such as penetration testing, is essential to ensuring the integrity of digital systems, and leads to stronger policy, protocol, and practice across all sectors online. In the course of this research those testing the systems often need to access information and systems in ways and to extents not envisioned or intended. As a result of security research, organisations, industry, and government branches have the opportunity to correct deficient and vulnerable cybersecurity systems and protocol prior to exploitation by malicious actors.

4. South Africa has repeatedly benefited from security research in recent years. For example, in 2013 a security researcher discovered a vulnerability in the province of Gauteng's E-Toll system that was easy to fix, but if left undiscovered could have compromised the personal details of a large number of motorists.[21] In another instance, concerned citizens discovered that the City of Johannesburg's online billing system had a security flaw that allowed invoices to be indexed by Google and therefore publically accessible over the internet.[22] Criminalizing security research would therefore undermine the Bill's primary purpose of enhancing cybersecurity in South Africa.

5. The existence of avenues for whistleblowers to publicize information of corporate and governmental malfeasance is an important and legally protected activity ensuring legal practices and combating corruption. The Protected Disclosures Act 26 of 2000 is intended to "create a culture which will facilitate the disclosure of information by employees relating to criminal and other irregular conduct in the workplace in a responsible manner."[23] The object of that law, however, is to protect employees from being subjected to occupation detriment, and not protection against criminal prosecution.[24] The Special Rapporteur for Freedom of Expression David Kaye released a report to the UN General Assembly on the Protection of Sources and Whistleblowers. It recommended that "[n]ational legal

---

[20] Collin Anderson, 'Considerations on Wassenaar Arrangement' (*Access Now* 9 March 2015)<https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf> accessed 16 November 2015

[21] Adam Oxford, 'Etoll web vulnerabilities expose Guateng Drivers' data' (*htxt.africa* 16 October 2013) <http://www.htxt.co.za/2013/10/16/etoll-web-vulnerability-exposes-gauteng-drivers-data/> accessed 16 November 2015

[22] Adam Oxford, 'Joburg wants to sue 'hacker' – so why don't we sue them back?' (*htxt.africa* 22 August 2013) <http://www.htxt.co.za/2013/08/22/joburg-wants-to-sue-hacker-so-why-dont-we-sue-them/> accessed 16 November 2015

[23] Protected Disclosures Act 26 of 2000 <http://www.justice.gov.za/legislation/acts/2000-026.pdf > accessed 16 November 2015

[24] Protection Disclosure Act 26 of 2000 s 2(1)

frameworks must protect the confidentiality of sources of journalists and others who may engage in the dissemination of information of public interest."[25]

Recommendation: The Bill should be modified to protect the work of security researchers, whistleblowers, and journalists by specifically excepting those activities in the public interest from prosecution under unlawful access and related crimes.

Recommendations

1. The Bill should only permit the issuance of a warrant for communication surveillance if the request satisfies the standards of necessity and proportionality;

2. The Bill should not include a mandate that electronic communications service providers report incidents to the National Cybercrime Centre. Participation should instead be optional;

3. The Bill should clarify that law enforcement and service providers have the authority to publish records of requests for communications surveillance; and

4. The Bill should protect the work of security researchers, whistleblowers, and journalists by specifically excepting those activities undertaken in the public interest from prosecution under unlawful access and related crimes.

Improving digital security means increasing the viability and usability of the internet as a platform for communications, and its effectiveness as a driver of commerce, education, health, and development generally. Security measures are an integral to the effort to expand global access to information and communications technologies.

Access Now commends the Department of Justice and Constitutional Development for approaching the challenging work of drafting cybersecurity and data protection policies. If you have any question or would like additional information, you can contact Ephraim Percy Kenyanito (ephraim@accessnow.org) and Drew Mitnick (drew@accessnow.org).

[25] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (8 September 2015) A/70/361 <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361> accessed 16 November 2015