Right2Know Campaign

Preliminary Position on the draft Cybercrimes and Cybersecurity Bill

30 November 2015

This document serves as the Right2Know Campaign's preliminary response to the draft Cybercrimes and Cybersecurity Bill ("the Cybercrimes Bill" or "the Bill"). The Department of Justice and Constitutional Development gazetted the draft Bill in August 2015, inviting public comments by 30 November 2015.

Given the Bill's complexity and far-reaching powers, R2K wrote to Mr Sarel Robbertse of the DoJCD to request that this deadline for public comments be extended at least to 11 December 2015. Mr Robbertse maintains that he cannot grant an outright public extension and informed us that the CyberCrimesBill@justice.gov.za email address would be deactivated by 15 December, but wrote that he "will consider" any submissions received until then.

While it is not exhaustive, we are posting this preliminary position online as a guide to members of the public who wish to engage with some of the problems with the draft Bill.

1. Introduction

1.1 About the Right2Know Campaign

The Right2Know Campaign (R2K) launched in August 2010. R2K is a democratic, activist-driven campaign that strengthens and unites citizens to raise public awareness, mobilise communities and undertake research and targeted advocacy that aims to defend and advance freedom of expression, access to information and the free flow of information. We view these rights as fundamental to any democracy that is open, accountable, participatory and responsive, and able to deliver the social, economic and environmental justice its people need.

1.2 Executive summary

R2K believes that a free and open internet is crucial to the full realisation of our constitutionally enshrined right to freedom of expression, which includes, but is not limited to, the freedom to impart or receive information or ideas, freedom of the press, freedom of artistic creativity, academic freedom, and freedom of scientific research.

The internet has the potential to democratise knowledge in unprecedented ways. In South Africa, we are witnessing the blossoming of the internet on a variety of ever improving platforms. The rapid development of internet technology and increasing internet access create new opportunities for ordinary South Africans to access and share information and engage critically with the world around them.

Yet this vision has yet to be fully realised. R2K notes with alarm events and developments around the world, and at home in South Africa, which threaten internet freedom. These include the overreach of state security services, widespread state and corporate surveillance, and new censorship mechanisms to regulate online content, often under the guise of security or 'moral' reasons.

These deeply troubling events underscore the need for the public to remain vigilant in defending internet rights and push back against reactionary legislation and policies that enable greater state and corporate control of the internet.

In this light, we reject the draft Cybercrimes and Cybersecurity Bill ("the Cybercrimes Bill") in its entirety. The need to combat genuine cybercrime is not contested. However, the Bill contains deep and fundamental flaws that threaten the fundamental democratic spirit of the internet.

This Bill creates a regime that is so broad and overarching that almost all possible crimes that could exist on the internet are dealt with using the same set of tools – from the risk of terrorist cyberattacks to the imagined crimes of an ordinary Facebook or BBM user. In attempting to police practically all of the internet, the Bill hands wide-ranging powers to state-security structures to secure vast parts of the internet as assets of state-security, rather than common spaces for the good of all. The Bill would put in place new offences which are over-broad and open to abuse. These would criminalise a range of lawful activities and place dangerous penalties on freedom of expression and access to information, while also giving the state new

invasive surveillance powers with little protection for ordinary people's privacy.

2. Key problems

2.1 Stewardship of the internet should not be a State Security function

At the heart of the Bill is a fundamental philosophical problem – it hands stewardship of the internet to the Ministry of State Security. The past few years have seen cybersecurity policy wrested from the organs of state responsible for promoting access to communication systems (the former Ministry of Communications), and handed to the Ministry of State Security. This is quite simply, a task for which the State Security structures are an inappropriate guardian. These structures lack the necessary transparency, accountability, mandate and organisational culture. As a convenient early example of the trouble ahead, it is worth noting that the Bill's forebear, a National Cybersecurity Policy Framework produced by the Ministry of State Security in 2012 – has been a classified state secret until last month.

More generally, the shift of internet governance responsibilities to State Security points to the broader problematic growth and influence of South Africa's state security structures, which has sometimes been described as a "rise of the securocrats". While the Constitution rightly envisages an extremely narrow and highly regulated role for South Africa's state security structures, we are seeing an ever-expanding mandate for these agencies that has resulted in them intruding in democratic spaces, with a tendency to conceptualise all manner of possible policy problems as a security threat.

This potentially dangerous view is certainly evident in the draft Cybercrimes Bill. The Bill would create a range of new agencies and structures with wide-ranging powers to shape standards and policies and protocols for the internet in South Africa – overwhelmingly these report to the Ministry of State Security.

This includes, for example, the power to declare any data, database, device, network, infrastructure – publicly or privately owned – to be a "National Critical Information Infrastructure". This may be thought of as an attempt to create "national key points" of the internet. Effectively this allows a state-security structure to lay claim to any part of the internet and declare it to be a crucial asset to national security.

While a role surely exists for security structures in responding to legitimate threats, these

should be as narrowly defined as possible – however, the Bill envisages all manner of possible cyber-related crimes, including many that are utterly unrelated to even the broadest possible understanding of state security.

Stewardship of the internet should rest with a civilian agency with a mandate to promote freedom of and access to communications systems. Where a role for the security structures is necessary, it should be narrowly defined and subject to civilian oversight.

On these grounds alone, the draft Bill projects a fundamentally wrong vision of promoting cybersecurity and should be redrafted in its entirety.

2.2 Harsh, draconian penalties that would muzzle journalists, whistleblowers, and data activists

Any law that regulates the free flow of information must have appropriate safety mechanisms to balance ordinary people's rights of access to information and freedom of expression with the state's national security mandate, in the interest of open and accountable democracy.

Safety mechanisms appropriate to the values of our Constitution and hard-won democracy include:

- A public interest defence (the more so while the Bill criminalises the possession and disclosure of classified information by ordinary people);
- Appropriate whistleblower protection; and
- Appropriate access-to-information and declassification mechanisms.

There are simply too many examples to list of journalists, whistleblowers and data activists who have published classified state information in the public interest. In various jurisdictions, these acts have exposed human rights abuses, corruption, human rights abuses, unethical and illegal behaviour of elected officials, and a host of other information which should clearly have been exposed in the public interest. Overwhelmingly these acts have taken place over the internet and with the use of computers. Once published, this information is often accessed and shared by millions of people across the world.

Clause 16 of the draft Bill introduces a range of offences under the banner of "computer-related espionage" that replicate and deepen problems that still exist in the

Protection of State Information Bill ("the Secrecy Bill"), and which would seek to criminalise all of these acts with no regard for basic rights and freedoms.

These provisions make it an offence to "unlawfully and intentionally" possess, communicate, deliver, make available, or receive data "which is in possession of the State and which is classified".

These provisions clearly create penalties which could ensnare investigative journalists, whistleblowers or other civic actors who may need to access or publish classified information in the public interest. The penalties range from a maximum of 5 to 15 years in jail, depending on whether the information is classified confidential, secret or top secret.

There is no public interest defence and no whistleblower protection. Even the limited and flawed exemptions contained in the Protection of State Information Bill are missing. Effectively, even more so than the Secrecy Bill, the draft Cybercrimes Bill cannot tell the difference between an act of espionage and an act of journalism.

This duplication also meaning that a person may face penalties under the Secrecy Bill for possessing, delivering or receiving classified information *and* additional penalties under the Cybercrimes Bill for doing so with the aid of a computer. To make matters worse, while a journalist, whistleblower or other person may get limited protection for their actions under the Secrecy Bill, the Cybercrimes Bill offers no such protections.

Clause 16 also draws on clauses 3 to 10 to create *additional* offences around various steps that may be taken to gain access to such classified information, including unlawful access to any database, network or infrastructure; unlawful interception of data from any network, device or infrastructure; unlawful use or possession of software, and so on. While the deeper problems with these offences are dealt with elsewhere, their inclusion in the offences in clause 16 mean that journalists and whistleblowers may prosecuted both for exposing classified information in the public interest, and for a number of steps that may be taken in the lead-up to such an event.

Finally, the draft Bill also fails to distinguish between information which is solely in the possession of the state and information which is already in the public domain. In doing so, the Bill would criminalise not only the whistleblower or journalist who accesses and publishes the information, but also any member of the public that may access, possess or share the

information once it is in the public domain.

These provisions are another fatal flaw of the Bill, pointing to a fundamental failure to appreciate and safeguard basic information rights.

2.3 Makes a bad surveillance law (RICA) worse

Any law that regulates the interception, investigation, search and seizure of data or communication must contain the strictest possible protections for users' privacy, in line with the international Necessary and Proportionate principles.

The Bill provides for invasive surveillance powers with no adequate limits and few checks and balances. While South Africa's existing surveillance law, the Regulation of Interception of Communications and Communication-related Information Act (RICA), contains deep flaws and is likely unconstitutional, this Bill is significantly worse.

First, to recap some key grievances with RICA:

- While RICA provides that a designated judge must authorise communications surveillance in most cases, the grounds for authorisation are vague and have proven to be open to abuse.
- The 2008 report of the Ministerial Review Commission on Intelligence (the "Matthews Commission") found that RICA fails to regulate mass surveillance at all.
- RICA's surveillance regime also suffers from a general lack of transparency. Users are not notified of a warrant to intercept their data, even after the fact, and RICA gags telecommunications companies and internet service providers from disclosing any information about surveillance of their users, even in aggregate form.
- Despite providing for a designated judge to exercise oversight on interceptions, RICA also delegates power to authorise interception of *historical* data to all magistrates and High Court judges, who may have no special technical or legal expertise on communications surveillance and the right to privacy, and who are not subject to any oversight or reporting requirements.
- These failings have led to numerous abuses of the state's surveillance powers. In all of this, RICA is out of line with the Constitution, and the International Principles on the

Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate" Principles).

The Cybercrimes Bill would in fact make a bad surveillance law worse, by creating a parallel procedure to run alongside RICA with regard to investigation, search and seizure of electronic data communications. This goes beyond the mere interception of data that is an indirect communication and real-time communication , to apply to interception of practically any possible data that may exist. This procedure appears to have fewer checks and balances than the already deficient ones in RICA.

Among the most glaring problems:

- RICA provides that interception of communications should only be used in the investigation and prevention of serious offences. Section 26 of the draft Bill states that its invasive powers can be exercised to access information connected to any offence.
- Significant powers are handed to "investigators" who are not public officials, but private individuals with unspecified characteristics.
- While RICA's delegation of significant powers to magistrates has already been criticised, the draft Bill hands powers to authorise other forms of interception of communication to magistrates. This is undesirable as such authority should only be entrusted to judges with special expertise in the legality of communications surveillance, the technologies used and related human rights issues.
- Section 29 provides even broader grounds that RICA for issuing warrants – for example only requiring that that the information is believed to be in the jurisdiction of the relevant judicial authority, or relating to "any offence", or appearing to be "required in evidence" in trial.
- These invasive powers can be used not only on a person suspected of committing a crime, but any person who is believed to furnish any information related to the matter under investigation.
- Very broad powers can be given in the search warrant, including disclosure of password and decryption key, without additional safeguards as in RICA
- As with RICA, the draft Cybercrimes Bill places a gag order on any party – a state

agency or private company – disclosing to the user that their privacy has been violated.

In short, the draft Bill fails to provide even the most basic safeguards for the privacy of ordinary users against invasive state surveillance. It is completely out of step with Constitutional requirements to protect the right to privacy, as well as international principles of human rights law.

2.4 Broad, vague and generally open to abuse

Laws that may grant powers to restrict openness and freedom of expression should be as narrowly defined as possible.

There is a general, deeply worrying broadness to the Bill.

2.4.1 Potentially criminalises ordinary use

For example, clause 4 of the bill makes it an offense to "unlawfully and intentionally access the whole or any part of (a) data (b) a computer device; (c) a computer network; (d) a database; (e) a critical database; (f) an electronic communications network; or (g) a National Critical Information Infrastructure."

Similarly, clause 5 makes it an offence to unlawfully and intentionally intercept data from "(a) a computer device; (b) a computer network; (c) a database; (d) a critical database; (e) an electronic communications network; or (f) a National Critical Information Infrastructure."

Clause 7 makes it an offence to "unlawfully and intentionally" interfere with data or critical data – including, per 7(3)a, merely *altering* data.

The penalties for any of these offences are very severe – and yet many of the activities they describe are performed millions of times a day by ordinary users of the internet. The question is: how does the Bill define what makes these acts "unlawful"? The Bill is vague, except to say that such activities are only lawful if "written authority is granted by the person who has the lawful authority to consent to such an act".

Thus, even where there is no malicious intent and no harm done, an ordinary internet user who exceeds whatever "written authority" there may be to access, navigate, draw on or alter data that exists anywhere on the internet may be committing a crime.

2.4.2 Criminalising security analysts and 'white hat' activists

The draft Bill will make it illegal to use many software and hardware tools. The Bill's offences relating to malicious use of software and probing of security flaws is broad enough to criminalise the work of ICT professionals and a global community of security analysts and researchers who test these systems as a civic duty, in order to point out and fix security flaws that put the general public at risk. Many of them do these without the "written authority" of whoever owns or controls the system being tested - in some cases because the relevant authority refuses to acknowledge that their system may be unsafe or compromised. The Bill is drafted so that anyone who is accused of exceeding this written authority will be considered guilty, until proven innocent. Far from promoting users' security, these provisions would potentially make the internet a far more dangerous place, by criminalising the work of many individuals and organisations who seek to identify and fix the security flaws that endanger ordinary users.

2.4.3 Extra offences for using a computer

Many of the offences contained in this Bill relate to acts which are already prohibited in other laws such as fraud, forgery, extortion, and terrorism – as well as common-law offences such as aiding or inciting someone to commit a crime.

Under the Bill, it would be an extra offence to undertake such crimes with the aid of a computer. The practical effect of this is to promote a technophobic policy agenda that is out of step with the 21st century.

2.4.4 Over-broad definition of "terrorism"

The Bill seeks to criminalise "computer-related terrorist activity", but widens the existing definition of terrorism contained in existing statutes. The Protection of Constitutional Democracy against Terrorist and Related Activities Act provides that legitimate struggles for self-determination should not be considered terrorists acts, nor should advocacy, protest, dissent or industrial action which do not intend to cause harm that would otherwise be criminalised under the Act. (i.e. if harm occurs through such acts it was not an intentional outcome). The Cybercrimes Bill fails to distinguish between cyberterrorism and cyber-dissent, when people use digital networks for activism and civil disobedience.

2.5 Over-broad restrictions on disseminating information

2.5.1 Hate speech

Section 17 of the Bill creates criminal offences for anyone who "makes available, broadcasts or distributes... a data message which advocates, promotes or incites hate, discrimination or violence against a person or a group of persons". This may be a message to a specific person or to the general public.

The Bill further provides that this should be understood as:

> any data message representing ideas or theories, which advocate, promote or incite hatred, discrimination or violence, against a person or a group of persons, based on (a) national or social origin; (b) race; (c) colour; (d) ethnicity; (e) religious beliefs; (f) gender; (g) gender identity; (h) sexual orientation; (i) caste; or (j) mental or physical disability.

As deeply distasteful and undesirable as such messages may be, these restrictions go beyond the limitations on freedom of expression envisaged in section 16(2) of the Constitution, which states that freedom of expression does not extend to "advocacy of hatred that is based on race, ethnicity, gender or religion, *and that constitutes incitement to cause harm*."

From this reading, it is clear that a message is only hate speech if it contains an incitement to cause harm, and only on the grounds of race, ethnicity, gender or religion. The provisions of the Cybercrimes Bill go beyond these restrictions, and thus infringe on constitutionally protected free speech, however distasteful.

2.5.2 Incitement to violence

The Bill, through Section 18, also makes it an offence for anyone to makes available, broadcasts or distributes:

> a data message which is reasonably likely to incite (i) violence against (ii) damage to the property belong to a person or a group of persons.

Again, this extends to any message to a single person or to the general public.

As above, these provisions go further than the constitutional restrictions on freedom of speech, which prohibit the incitement of ***imminent*** violence (not violence in general) and do not explicitly restrict damage to property at all.

These provisions could well lead to constitutionally indefensible censorship of internet

content.

2.6. Copyright provisions

Section 20 provides criminal penalties for a wide range of offences related to copyright infringement. These are outrageously broad and inappropriate – and R2K aligns itself with the Electronic Frontier Foundation's submission on the full extent to which the Bill's anti-copyright provisions go far beyond international norms – but crucially, copyright matters should not fall within this Bill's remit at all. The Department of Trade and Industry is already undertaking amendments to South Africa's copyright law and this Bill threatens, once again, to create a parallel process with significantly worse provisions.

2.7 Undermining POPI

Section 3 of this Bill has 'data protection' clauses that compete with South Africa's existing data protection law, the Protection of Personal Information Act (POPI). POPI provides excellent safeguards to protect all personal and financial information, in line with international best practice. The unseemly delay in implementing POPI, including appointing an independent and fully staffed Information Regulator, greatly undermines the protection of ordinary people's privacy in South Africa. Clearly the solution is to put all possible effort into implementing POPI fully and immediately, rather than drafting a new Bill that attempts to compete with POPI's provisions.

3. Conclusion

This submission is by no means exhaustive. The Bill suffers from over-arching structural problems and many clause-by-clause defects that cannot be accounted for in this brief submission.

While R2K does not contest the need for policy that regulates and combats legitimate and malicious cybercrimes, this draft Bill fundamentally threatens the democratic character of the internet. We do not believe it can be tweaked or salvaged – it should be withdrawn and redrafted in its entirety.

#ENDS