RIGHT2KNOW

NATIONAL & WESTERN CAPE
107 Community House
41 Salt River Rd
Salt River, Cape Town
Tel: 021 447 1000
Admin@r2k.org.za
WesternCape@r2k.org.za

KWA ZULU NATAL
101 Dinvir Centre,
121 Field (Joe Slovo) St
Central, Durban
Tel: 031 301 0914
KZN@r2k.org.za

GAUTENG
5th floor, Heerengracht Building
87 De Korte St
Braamfontein, Johannesburg
Tel: 011 339 1533
Gauteng@r2k.org.za

Cybercrimes, Cybersecurity, and Internet Freedom

Right2Know Campaign submission on the Cybercrimes and Cybersecurity Bill, 10 August 2017

About the Right2Know Campaign

The Right2Know Campaign (R2K) launched in August 2010 and has grown into a movement centred on freedom of expression and the free flow of information. We are a democratic, activist-driven campaign that strengthens and unites citizens to raise public awareness, mobilise communities and undertake research and advocacy that aims to ensure the free flow of information necessary to meet people's social, economic, political and ecological needs and live free from want, in equality and in dignity.

Our Vision

"We seek a country and a world where we all have the right to know – that is to be free to access and to share information. This right is fundamental to any democracy that is open, accountable, participatory and responsive; able to deliver the social, economic and environmental justice we need. On this foundation a society and an international community can be built in which we all live free from want, in equality and in dignity."

Our Mission

- To co-ordinate, unify, organise and activate those who share our principles to defend and advance the right to know.
- To struggle both for the widest possible recognition in law and policy of the right to know and for its implementation and practice in daily life.
- To root the struggle for the right to know in the struggles of communities demanding political, social, economic and environmental justice.
- To propagate our vision throughout society.
- To engage those with political and economic power where necessary.
- To act in concert and solidarity with like-minded people and organisations locally and internationally.

For more information about the Right2Know Campaign, please visit www.r2k.org.za.

1. Introduction

1.1 Background to the Bill

This is the Right2Know Campaign (R2K) submission on the Cybercrimes and Cybersecurity Bill (the "Cybercrimes Bill").

In 2015, the Department of Justice and Constitutional Development published a draft version of the Cybercrimes and Cybersecurity Bill for public comment. In its submission on the draft Bill, the Right2Know Campaign rejected the draft Bill in its entirety, citing "deep and fundamental flaws that threaten the democratic spirit of the internet."[1]

In that period, thousands of internet users signed a petition denouncing the draft Bill[2]. After taking consideration of the criticisms, the Department of Justice & Constitutional Development started a redrafting process, with input from an 'Expert Committee' which included human rights lawyer Alison Tilley, a longtime member of the Right2Know Campaign. Despite our concerns that this Expert Committee was not still not sufficiently inclusive of the range of perspectives and experiences that were necessary to redraft the Bill, we acknowledge several progressive amendments in the redrafting process.

1.2 Summary of R2K's submission

R2K's submission is prompted by our belief 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 both the very real threat of online crimes that target internet users (such as identity theft, financial crimes, and online harassment), and new laws and practices including censorship mechanisms to regulate online content, widespread state and corporate

[1] R2K submission on the draft Cybercrimes Bill, 30 November 2015: http://www.r2k.org.za/2015/11/30/cybercrimesbill/
[2] R2K petition to the Department of Justice, 'Stop the Cybercrimes Bill', 10 December 2015

surveillance, and the overreach of state security services. 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.

While we acknowledge the importance of the Bill's stated aims, to improve the state's capacities to fight actual cybercrime, and to put measures in place to upgrade security around all our cyber infrastructure to prevent further crime, the effect is to create a framework that undermines internet freedom overall, and enable state interference in our data, devices and networks.

Any cybercrimes legislation which defines potential offences must be as narrowly and clearly drafted as possible to prevent any possible misuse to enable online censorship, stifle online public participation or infringe on legitimate online activities. We believe the cybercrimes section of this legislation needs to be significantly redrafted to ensure this.

Any cybersecurity legislation needs to safeguard against state invasions of privacy, and over-reach by the state security structures. The current policy direction of the cybercrimes sections of this legislation is fundamentally flawed. It is inappropriate for the state security structures to be given primary stewardship over cybersecurity, as this makes cybersecurity initiatives inherently less transparent and subject to democratic control. While the state security structures have an obvious advisory role in these matters, it is more appropriate for overall stewardship to be transferred back to a 'civilian' department falling under the Ministry of Communications. We therefore recommend the complete withdrawal of at least Chapters 10 and 11, to be redrafted from scratch, with civilian agencies in the 'driving seat'.

1.3 Welcome changes

As stated above, we recognise several key positive changes since the draft version of this Bill. These include:

- The removal of the 'secrecy bill clauses' in the 2015 draft Bill, which would have criminalised journalists and whistleblowers for accessing classified information
- The removal of copyright offences in the 2015 draft Bill, which R2K identified as

outrageously broad and inappropriate.

1.4 Summary of the remaining problems

- This Bill still hands over a huge role to State Security in defining internet governance in South Africa. We believe that bringing cyber security under the domain of intelligence agencies makes cybersecurity initiatives less transparent and makes it harder for the public to have a say in them.
- The Bill tries to make internet users more secure from attacks. But the Bill's 'top-down' approach to cyber security could make us less secure. We will elaborate on this furthr in the submission.
- The Bill tries to reform RICA, South Africa's main surveillance law, but without addressing any of the serious problems with RICA that have led to massive surveillance abuses.
- The Bill tries to prevent online harassment, incitement and bullying by criminalising 'malicious communications', including the publishing of 'inherently false' information ('fake news') – but this raises huge freedom of expression problems.

R2K's submission covers our concerns in three areas: freedom of expression, freedom from surveillance, and cybersecurity.

2. Freedom of Expression

Chapter 3 of the Cybercrimes Bill seeks to regulate "Malicious Communications" – in other words, messages which could be harmful in various ways. Protecting freedom of expression online is a challenge in an environment where patriarchy, racism, hatred and toxicity thrive. However, these provisions create a legal framework that is wide open to abuse, especially viewing the full scope of how the Bill defines what messages are considered harmful.

This appears to be government's proposal to 'regulate' social media, a proposal often associated with State Security Minister David Mahlobo, whose comments on possible regulation led to social media users harshly criticising the proposal under the hashtag #HandsOffSocialMedia, as well as a widely circulated petition rejecting the proposal[3].

2.1 Inciting or threatening violence and property damage

Anti-incitement provisions that criminalise things which are already criminal, or that shouldn't be criminalised at all

Section 16 and 17(1)(a) and 17(1)(b) of the Bill would make it a crime to send or resend a message that:

- Incites violence or property damage
- Threatens a person with violence or property damage
- Threatens violence or property damage against a group of people, or any person who is associated with a group of people

Of course, it is desirable that people should not threaten each other with violence and property damage. But on principle we should reject laws that prohibit speech because it *could* do material harm, without any harm actually being done. Rather than create a chilling threat to freedom of speech, which could include hyperbolic or satirical speech, criminal penalties should only apply to demonstrable harm done.

[3] R2K petition, #HandsOffSocialMedia: https://awethu.amandla.mobi/petitions/handsoffoursocialmedia

A number of legal tools exist that potentially criminalises such message, including the apartheid-era Riotous Assemblies Act and Intimidation Act – laws whose constitutionality is under question exactly because they infringe on freedom of expression.

2.2 Online harassment to do harm

Anti-harassment provisions which should be dealt with by the Protection from Harassment Act

Section 17(1)(c) of the Bill makes it a crime to send or resend a message that "intimidates, encourages or harasses" a person to harm themselves or someone else.

While we can appreciate the intention to protect vulnerable people from harassment online, this could have a chilling effect on freedom of expression, which includes robust political expression that is often crude, aggressive and unpleasant. For example, it is not uncommon for offended Twitter users to send messages to @realDonaldTrump (the President of the United States of America) to "go kill yourself". These rowdy rejections of the politics and policies of a deeply unpopular leader, would be criminal offences under this provision.

In any case, such communication should more properly be dealt with in the Protection from Harassment Act of 2011, which allows someone to get a protection order against their harasser – including for those who harass through the internet and telecommunications platforms. To harass in defiance of a protection order is a criminal offence. The Protection from Harassment Act has has not fully delivered its promised protections to victims of harassment – however, the remedy appears to be greater public awareness and better enforcement by the justice system. Additional criminal penalties imposed through the Cybercrimes Bill are not the answer.

2.3 "Fake news"

Seeking to police 'truthfulness' poses a huge threat to freedom of expression

Section 17(d) of the Bill criminalises "fake news" – defined as the sending or resending of any message that is "inherently false in nature and… aimed at causing mental, psychological, physical or economic harm".

This is, evidently, the state's response to 'fake news'.

Quite simply we reject this provision. We do not believe the prosecuting capacity of the state should concern itself with policing truthfulness.

Aside from the extraordinary waste of policing resources this could entail, freedom of expression is a human right, and it includes the freedom to be wrong, and the freedom to be dishonest. With due respect to the Honourable Members of the Committee, there are even some politicians who can be thankful for that.

Most importantly, in our current political climate, given a concerning trend of politically motivated and vexatious prosecutions, a 'fake news' clause would provide another avenue through which the state or political actors could harass and intimidate investigative journalists and voices of dissent.

2.4 Criminalising sending and resending

The Bill criminalises re-publishers of 'harmful' messages, regardless of intent

In addition to all the aforementioned problems, in each of its 'malicious communications' clauses, the Bill makes it a crime to re-send any message that is deemed 'harmful' – even if you were not originally the author. This could include forwarding an email or WhatsApp message, retweeting something on Twitter, or re-posting something on Facebook.

This does not take into account your intention for re-sending such a message. It would be very common for social media users to re-post an offensive or irresponsible or even criminal message in order to draw attention to it. In the case of 'false' messages ('fake news'), the best way to combat fake news is to do what social media users do – to repost it with a caption that says 'this is false'.

2.5 Prohibiting 'revenge porn'

Criminalising the sending of 'intimate images' without the subject's permission

Section 18 of the Bill would criminalise what is popularly known as 'revenge porn', which it defines as sending or resending a data message that has "an intimate image" of a person without their consent. The Bill defines "an intimate image" as one in which the person is nude, is exposing their genitals or "anal region" – or breasts, if the person is female.

We note that similar provisions seeking to criminalise 'revenge porn' are also contained in the Film and Publications Amendment Bill, also under consideration in Parliament. The R2K does not raise objection with this provision of the Cybercrimes Bill, except to reiterate the input made by Media Monitoring Africa (MMA) in its own submission on this clause. However, R2K reiterates its call for the full withdrawal of the Film and Publications Amendment Bill, on the basis that it chills freedom of expression.

2.6 Recommendations to protect freedom of expression

With the exception of the 'revenge porn' clauses, the Bill's entire section on 'Malicious Communications' should be rejected. There are already mechanisms to combat the ills of harmful and malicious communication. In many cases, these mechanisms have been weakened by poor implementation and a justice system that fails the poor and marginalised, especially women. – the solution is not to pile on new, heavy-handed criminal penalties, but to invest in creating a more just and responsive justice system.

3. Freedom from surveillance

In recent years the Right2Know Campaign has documented significant evidence of the abuse of the state's surveillance powers[4]. These abuses are enabled by loopholes in South Africa's main surveillance law, RICA -- both because of what RICA permits and what it fails to prohibit.

Section 38 of the Cybercrimes Bill seeks to make some reforms of RICA. Unfortunately, the best that can be said for these reforms is that they do not make a terrible situation much worse, but stop short of the necessary reforms and continue to leave South Africans dangerously exposed as a result.

3.1 So what's wrong with RICA?

Lack of transparency, mass storage of data, and poor oversight have infringed privacy of millions.

The Right2Know Campaign has called for far-reaching reforms to RICA in the face of growing evidence of communication surveillance abuses in South Africa[5], co-signed by 40 social justice organisations in South Africa. This follows findings by the UN Human Rights Committee that South Africa's surveillance policies are out of step with human rights law[6]. Indeed, it is for these reasons that RICA is now facing constitutional challenge from the AmaBhungane Centre for Investigative Journalism, after that organisation confirmed that government agents had tapped the phone calls of one of its journalists[7].

For brevity the full programme to reform RICA will not be restated here. However, among the changes we have demanded:

1) An end to SIM card registration and mandatory user identification

2) An end to mass storage of users' communication data

3) Users must be notified if their communications information is intercepted

[4] R2K handbook on surveillance abuses, April 2017: http://www.r2k.org.za/ricaguide
[5] R2K memorandum on RICA, April 2016: http://r2k.org.za/rica-demands
[6] UNHCR, Concluding observations on the initial report of South Africa, CCPR/C/ZAF/CO/1 (April 2016), s43-44.
[7] AmaBhungane press statement, 20 April 2017:
http://amabhungane.co.za/article/2017-04-20-amab-challenges-snooping-law

4) Greater transparency in general on surveillance matters

5) Better judicial protection for metadata (which is as sensitive as content) and stronger judicial oversight in general

6) An end to mass surveillance

Each of these demands aims to bring South Africa's surveillance policies in line with international best practice (the International Principles on the Application of Human Rights to Communications Surveillance[8]), as well as research by the Media Policy and Democracy Project, a collaboration between Unisa and the University of Johannesburg. This research can be made available to the Committee at its request.

3.2 The Bill's modest changes to RICA

Expanding some surveillance (storing internet users' browsing history) while closing a major loophole

Frankly the lack of clarity, even from within state institutions and policymakers, about how the state's surveillance policies work, has made it extremely difficult to reach consensus on what Section 38 means. However, to our understanding after consultations with the Department's drafter, Section 38 of the Cybercrimes Bill aims to enact two changes to RICA.

3.2.1 The first reform: Storage of users' internet browsing information

The first is to operationalise existing provisions of RICA that require internet service providers to store customers' metadata for 3-5 years, such as IP addresses, browsing history, etc. While RICA's equivalent provisions for telecommunications providers were operationalised through regulations some years ago, these provisions relating to internet service providers appear have never been put into operation.

That these provisions, which were called for in legislation in 2002, have never been enacted, should already be a warning to drafters of this Bill about the gap between policy and practice.

However, from a human rights perspective the key point is that these provisions should *never*

[8] The "Necessary & Proportionate" Principles: https://necessaryandproportionate.org/

have been put into law, and may well be unconstitutional. That is to say, RICA calls for all communications providers to store *all* information about a person's communication for up to five years, irrespective of whether or not they are suspected of criminal activity. This will now be put into practice by the Cybercrimes Bill. This kind of data retention was struck down in the EU by the European Court of Justice because it led to a serious interference with fundamental rights.

Mass retention of a person's sensitive information violates their privacy in a way that we believe is unconstitutional.

We believe these provisions should be struck from the Bill, and removed from RICA.

3.2.2 The second reform: closing a loophole?

The second reform to RICA could be seen in a more positive light -- aiming to close the surveillance loophole in s205 of the Criminal Procedures Act, which has created a parallel procedure for law enforcement to access people's sensitive communications information outside of the RICA judge's oversight.

Using s205 of the CPA, law enforcement can approach any magistrate for a warrant that forces a telecoms company to give over a customer's call records and metadata if that person is under investigation. However, that person is never notified, even if the investigation is dropped or if if they are found to be innocent. A person's call records contains incredibly sensitive information, and needs high levels of protection to enforce the constitutional right to privacy.

It is good that the Bill aims to close this loophole. But how practical is it?

In May 2017, the Right2Know Campaign used the Promotion of Access to Information Act to obtain statistics from the network operators of how often they are compelled to hand over customer call records in terms of s205 of the CPA[9]. While inconsistent record keeping prevents us from determining an exact figure, at a minimum *71,731* phone records were

[9] R2K statement, 30 May 2017:
http://www.r2k.org.za/2017/05/30/mtn-vodacom-telkom-and-cell-c-30-days-to-provide-surveillance-stats/

intercepted in the 2016/2017 financial year.

This means the vast majority of surveillance warrants are issued using this loophole; tens of thousands of surveillance warrants are issued by magistrates every year, compared to just a few hundred a year by the RICA judge. And here lies the problem: the Bill will simply result expanding the RICA judge's oversight responsibilities by a factor of 100. This leads to poorer oversight, not better.

3.3 Falling short of full reforms

Urgent changes are needed to protect citizens' privacy

It is a greater point of concern that the Cybercrimes Bill fails to take any other meaningful steps to fix the many loopholes in RICA and other harmful provisions that have enabled the state to spy on its citizens and use surveillance as a tool for repression. R2K has put forward a comprehensive list of urgent reforms for RICA; this half job is unacceptable.

4. Cybersecurity

We can all agree on is that the internet does need to be more secure, but this can mean different things to different stakeholders. For government agencies, 'cyber security' can mean making sure the state knows what's happening on the internet and can intervene when someone does something wrong. But for ordinary people using their device or browsing the internet, cyber security can include being secure from government agencies interfering with their internet access or trying to spy on their communication – in other words, sometimes the government agency is the threat, not the protector.

4.1 Understanding the Bill from a digital rights perspective

We all have the right to cyber-security – when we use computers or phones, and send messages on WhatsApp or Facebook, or browse websites, we need protection for our right to privacy, our right to freedom of expression and our right to access information. To enforce those rights, we need cyber-security. Violations of our cyber security could be seen as a violation of our basic human rights.

A cyber-security law should protect us our three levels: protecting our personal data, protecting our device, and protecting the networks we use (the infrastructure that connects us to the internet and other people). There is a constant level of threat against our information – from criminals, private companies, and from state actors, both domestic and foreign.

Unfortunately, the Bill takes a fundamentally wrong approach cybersecurity, which is top down and state-centric. As a result, in key ways the Bill pursues strategies that would make cyberspace *less* secure for ordinary users.

4.2 Does it protect our information?

The Bill's cybercrimes provisions on "unauthorised access" inadvertently undermine POPI

The Bill tries to protect us from those people who want unauthorised access to our computers

and devices, but in doing so undermines and overlaps with the Protection of Personal Information Act (POPI), South Africa's data protection law. Section 2 creates a new crime in this regard, which is intended to criminalise those people who get access to your computer data or system without your permission.

These provisions criminalise anyone who "unlawfully", or contrary to law, secures access to data in a way that allows them to use it without permission. This includes "unlawfully" in terms of POPI. This would create many criminals of people who access data in breach of POPI - those who mishandle other people's personal data through carelessness, not through deliberate hacking attempts..This is not the intention of the Bill, and remedies for breach of POPI are extensive and set out in that Act.

As a result, the Bill will tread all over POPI's legal territory. The Protection of Personal Information Act, on which this Committee worked painstakingly, gives powerful protection (on paper) to our data and make sure companies and individuals who handle other people's personal data don't misuse that information or violate their privacy. It is a matter of great concern that POPI remains only partially implemented, with the Information Regulator's office not yet operational. Public efforts should be directed towards implementing POPI and fully funding it, rather than creating overlapping legislation that could undermine our new data protection law. This makes us less secure.

4.3 Does it secure our devices?

The Bill's top-down approach to cybersecurity may criminalise independent security testing

The Bill tries to make sure that those people who have the technology to break into our devices are stopped – section 4 of the Bill, entitled "Unlawful acts in respect of software or hardware tool", makes it a crime to have any software that is used to overcome the security measures of a person's device.

This is the same as making it illegal to have a set of lockpicks or a crowbar, as a way of trying to stop burglaries. Unfortunately, this completely misunderstands the nature of providing internet security. The only way to test security is to use software to try and find ways into your system to make sure it is secure. It is the equivalent of making sure your house is locked,

by trying to open the front door.

The people who test the security of our systems – our devices, software and networks – do so by trying to break those systems from the outside, using software that would now be criminalised by this Bill. Many times, they do so without the authorisation of the owner of that network or software, because it's usually a company or government institution that thinks it knows better. This kind of security testing has made us safer, over many years, and prevented many acts of cybercrime before they ever happened. Because this Bill can't tell the difference between cybercriminals and security testers – it will discourage people from testing internet security systems, and ultimately make the internet less safe.

Recent examples of high profile public interest 'hacks' include:

- The latest iPhone 10.3.3 update fixes a flaw that was discovered by researchers at a private firm which allowed them break into an iPhone over wifi (ie. need to be within wifi range). It was disclosed to Apple, who fixed the bug.
- In 2017, a firm called Checkpoint discovered a bug in Whatsapp and Telegram whereby that sends their Whatsapp web session details to the attacker. It was disclosed to Whatsapp and fixed.
- In 2016, an analyst named Andrey Leonov discovered a flaw that allowed him to break into a Facebook server on the internet. He used a web browser, and a common harmless network diagnostics tool (called "netcat") to find and exploit this flaw. Though he was in no way affiliated to Facebook, he reported the bug.
- In 2015 two two independent researchers found a way to remotely influence the running of a Jeep Cherokee over the internet. They disclosed to Jeep, who in turn had to physically get cars into the workshops for firmware update,

These were all made possible by active attempts to overcome the security measures of devices, networks and systems, and used tools that were capable of doing so. None of these acts were authorised, but all of them made us safer. Though unintentional, the Bill would seriously undermine such efforts.

The act of breaching someone's security with bad intentions should be an offence, and

measured by the actual harm that is done. It should make no difference if the offender did it with a sharpened spoon or with a few lines of code. You can do a lot of damage with a sharpened spoon, but we do not outlaw sharpened spoons, and nor should we outlaw lines of code.

4.4 Does it secure our networks?

The Bill's provisions on declaration and protection of Critical Information Infrastructure are a nightmare for internet freedom

The Cybercrimes Bill seeks to ensure that the private sector secures its networks, and that where they don't, the state can step in to do so. One way the Bill tries to do this is by giving State Security structures the power to declare any device, network, database or other infrastructure as 'critical information infrastructure' and put legal obligations on these entities (including private companies) to meet government security standards and submit themselves to security audits.

These provisions seem to echo Section 2 of China's 2016 Cybersecurity Law[10], which provides for 'Critical Information Infrastructure' which must similarly be protected.

In the Bill, once an entity has been declared 'critical information infrastructure', the State Security Minister will issue directives on the classification of data held by that entity, the storing and archiving of that data, physical and technical security standards, and "any other relevant matter which is necessary or expedient in order to promote cybersecurity". There's a lot of devil in this detail. Among other things, it could mean that information held by a private company which helps you connect to the internet could now become classified as a national security secret. The "any other matter" provision could mask serious misdeeds that undermine privacy and internet freedom: most notably, the risk that State Security could grant itself backdoor access to private networks or give itself new surveillance and monitoring powers.

The fear of a government 'backdoor' is not an idle fantasy, but a legitimate concern that policymakers need to address.

[10] An unofficial English translation of the Law:http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en

Why is it a legitimate concern? There is a global trend in cybercrime policy of governments seeking legal and technical 'backdoors' into networks and devices to bypass security measures for 'good' purposes, and all have been resisted ad decried by digital rights advocates and cybersecurity experts. It is highly likely that the South African government will use these provisions to seek to give itself access, direct or indirect, to the data held on 'critical information infrastructure'. How better to monitor and detect acts of cybercrime?

Aside from the very serious risk this poses for surveillance abuses, security 'backdoors represent a serious risk to cybersecurity overall and make the users of technology more vulnerable, not more safe. This is because any 'backdoor' security vulnerability in a network, device or database that lets in the government, can also let in cyber-criminals and foreign governments. In other words, a system is either secure from *everyone* (including government agencies) or it is vulnerable to *everyone*.

The Bill's 'Critical Information Infrastructure' could be characterised as 'National Key Points of the Internet', yielding many of the same concerns that have arisen through the National Key Points Act. Whether the intentions are good or not, there is a great risk that efforts to lock down institutions will result in making them less accountable and transparent, and give the state too much power to impose itself on internet infrastructure.

4.5 Finding capacity to fight genuine cybercrime and make cyberspace more secure

What the Cybercrimes Bill doesn't do, and can't do, is develop the expertise inside the police to detect and solve cybercrimes, and the expertise in the state to create better defenses against cybercrime.

This is a point of concern for several reasons. The first is because genuine cybercrime is a serious and burning problem of which many people in South Africa are the victim every year. Thus far the ability of the state to detect, investigate and prosecute such crimes, using many existing legal mechanisms, leaves a lot to be desired. A cybercrimes law that in many way over-reaches will not solve this incapacity -- if anything it could stretch policing capacity even further.

We are aware of the submission by Mr Graeme Eatwell, who has been seriously victimised as a result of the police and prosecuting authority's low levels of capacity in matters of cybercrime. There is no way of knowing how many others have had this experience, but it offers a serious cautionary to policymakers: new legislation, which makes matters more complex, will only compound the serious capacity issues we face in the realm of cybercrime.

5. Conclusion

It has already been said that the Bill is significantly improved from its draft version, but clearly there are several serious defects in it which undermine internet freedom, and may indeed undermine cybersecurity imperatives as well.

It is worth remembering that the Bill is two different policies that have been married together. The first policy is a cybercrimes Bill, that tries to improve the state's ability to fight actual cybercrime (but creatings problematic offences along the way) and the second policy is a cybersecurity bill that tries to put measures in place to upgrade security around all our cyber infrastructure to prevent further crime.

While we acknowledge the importance of the Bill's stated aims, the effect is to create a framework that undermines internet freedom overall, and enable state interference in our data, devices and networks. We are therefore proposing to *split* the Bill into two.

We believe the cybercrimes section of this legislation needs to be significantly redrafted to ensure it is narrowly and clearly drafted as possible to prevent any possible misuse to enable online censorship, stifle online public participation or infringe on legitimate online activities

Any cybersecurity legislation needs to safeguard against state invasions of privacy, and over-reach by the state security structures. The current policy direction of the cybercrimes sections of this legislation is fundamentally flawed. It is inappropriate for the state security structures to be given primary stewardship over cybersecurity, as this makes cybersecurity initiatives inherently less transparent and subject to democratic control. While the state security structures have an obvious advisory role in these matters, it is more appropriate for

overall stewardship to be transferred back to a 'civilian' department falling under the Ministry of Communications. We therefore recommend the complete withdrawal of at least Chapters 10 and 11, to be redrafted from scratch, with civilian agencies in the 'driving seat'.

#Ends