OPEN DEMOCRACY ADVICE CENTRE

TRANSPARENCY IN ACTION

Cybercrimes Bill Submission

Prepared by Alison Tilley of the Open Democracy Advice Centre.

Cybercrimes are simply crimes committed with computers. The problem with the law on such crimes is that it is out of date and running to catch up with the new and ingenious ways people have of committing crimes. So, we need a cybercrimes bill in order to make sure we can use the law effectively to stop cybercrime.

This is not only the responsibility of law enforcement and prosecutors. We all have a role to play in combatting cybercrimes, and need to stay alert for such things as phishing, and keeping our anti virus software updated. One way to think of cybercrime is to think of it exactly like a virus, like measles. If we all are vaccinated against measles, and stay home if we are infected, we can contain the disease. If many of us do not take these precautions we are all at risk.

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). Our rights to privacy, our right to freedom of expression and our right to access information must be protected. We should not be denied access to our own data by criminals holding our information hostage, or find our bank accounts emptied of their contents.

This legislation describes the role for the police and prosecutors in keeping us safe. It also hands significant powers to the Minister for State Security, and we will need to ask to what extent that is needed to keep us safe, or to what extent it creates a risk in and of itself.

Section 2 and 3

The most important part of the Bill is section 2 and 3. They create the crime of hacking. In the real world, trespassing on other people's property is a crime. However, it isn't that serious a crime. We know that people trespassing on your computer is a serious crime in and of itself, even if nothing is actually taken. So, this section creates that crime.

The section reads:

Unlawful securing of access
2. (1) Any person who unlawfully and intentionally secures access to—
(a) data;
(b) a computer program;
(c) a computer data storage medium; or
(d) a computer system,
is guilty of an offence.

(2) For purposes of this section a person secures access to—
(a) data when the person is in a position to—
(i) alter, modify or delete the data;
(ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;
(iii) obtain its output data; or
(iv) otherwise use the data;
(b) a computer program when the person is in a position to—
(i) alter, modify or delete the computer program;
(ii) copy or move the computer program to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;
(iii) cause the computer program to perform any function;
(iv) obtain its output; or
(v) otherwise use the computer program;
(c) a computer data storage medium when the person is in a position to—
(i) access data as contemplated in paragraph (a) or access a computer program as contemplated in paragraph (b), stored on the computer data storage medium;
(ii) store data or a computer program on a computer data storage medium; or
(iii) otherwise use the computer data storage medium; or
(d) a computer system when the person is in a position to—
(i) use any resources of;
(ii) instruct; or
(iii) communicate with, a computer system, and the access contemplated in paragraph (a), (b), (c) or (d) which the person secures is unauthorised.
(3) For purposes of subsection (2), ‘‘unauthorised’’ means that the person—
(a) is not himself or herself lawfully entitled to secure access;
(b) does not have the lawful consent of another person who is lawfully entitled to secure access; or
(c) exceeds his or her entitlement or consent, to secure access,
to data, a computer program, a computer data storage medium or a computer system.

The idea is that the actual crime is accessing your computer, without your permission. This section tries to say this:

(2) A person is guilty of an offence if—
(a) they secure access to any program or data held in any computer;
(b) the access they secure is unauthorised; and
(c) they know at the time when they causes the computer to access the program or data that that is the case.

We recommend redrafting thus. The section in the bill is much less clear. It firstly says the access must be unlawful. It doesn't say what unlawfully means. It clearly must mean when the access is unauthorised, but it says ‘unlawful’ instead. Now, unlawful is a lot of things, not just illegal access. Usually we use unlawful in relation to the state, where that state does things that are not authorised by law. The state, unlike individuals like you and me, must have a law to allow it to act. If it acts without a law, or in contravention of a law, that is unlawful. It is an odd word to use here.

You would normally expect a criminal law provision to say (this is just an example) –

If you murder anyone, the penalty is 20 years in jail.

This section says it the other way round – if you unlawfully kill someone, the penalty is 20 years in jail. But that is much, much wider than murder. So if I knock you over by mistake with my car, I am killing you unlawfully. But that is culpable homicide, not murder. If as a surgeon you die on my operating table because I make a mistake that is an unlawful killing. But not murder.

We are defining the crime in the negative, rather than describing the actual crime, which is accessing a computer without permission.

The section as redrafted here is much simpler and clearer as to the crime, and avoids the complication of acts, which are unlawful, and undefined, being made criminal.

Section 3 as drafted runs into the same problem, as do the other sections in Chapter 2.

Section 4.

Cybercrimes are like measles. How do we know if we are infected with something? That's easy – we have a temperature, a rash etc. With computers we equally need to take their temperature from time to time to see if they are going to get sick. Your doctor has a thermometer. They will check your temperature when you see them, and your blood pressure, because these are quick and cheap diagnostic tools which allow us to see if there is anything wrong.

IT engineers equally have such tools. They are a way of taking a system's temperature and seeing if there are any problems. In order to do that, you have to actually check the system from the outside. Like someone testing a security door, this is to secure the system. However, it looks exactly like the same tool that a hacker uses to test the system. These tools get better at testing security all time – as the attacks get more sophisticated the tools do too.

This section makes having such tools criminal if you are going to commit a crime (remember you can commit a crime by being a surgeon who makes a mistake or a driver who drives carelessly).

This is so broad and worrying that some IT engineers are saying that they would rather not have such tools. That's like doctors saying they are worried they will be held criminally liable if they have thermometers in their surgery, and saying they won't use them. Doctors can get by without thermometers – we are the ones who will be more at risk, because we wont get properly diagnosed.

Making people criminals because they have the tools of the trade, and might have the intention of misusing them, and then in addition make them liable if they

manufacture, assemble, obtain, sell, purchase, make available or advertises any such software or hardware tool is to make the law an ass.

Sections 16 – 17

These sections are unnecessary, overbroad, and an unreasonable and unjustifiable limitation of the right to freedom of expression in an open and democratic society.

In the first place, incitement to violence is already a crime.

Incitement to commit any crime is punishable by virtue of the provisions of section 18(2) of the Riotous Assemblies Act 17 of 1956, the relevant portions of which read as follows:

> "Any person who ... incites, instigates, commands or procures any other person to commit any offence, whether at common law or against a statute or statutory regulation, shall be guilty of an offence and liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable".

You do not have to prove that a crime actually took place, merely that incitement happened.

The Intimidation Act No 72 of 1982 remains in force wherein:

> (1) Any person who –
>
> a. . . .
> b. acts or conducts himself in such a manner or utters or publishes such words that it has or they have the effect, or that it might reasonably be expected that the natural and probable consequences thereof would be, that a person perceiving the act, conduct, utterance or publication-
> i. fears for his own safety or the safety of his property or the security of his livelihood, or for the safety of any other person or the safety of the property of any other person or the security of the livelihood of any other person; and
> ii. . . . [subsection 2 has been repealed]
>
> shall be guilty of an offence and liable on conviction to a fine not exceeding R40 000 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment."

This legislation has recently been upheld as constitutional in Moyo and Another v Minister of Justice and Constitutional Development and Others; Sonti and Another v Minister of Justice and Correctional Services and Others (28532/14; 41487/14) [2016] ZAGPPHC 1077; 2017 (1) SACR 659 (GP) (20 December 2016)

Sec 16 creates a yet another crime of cyber incitement, allowing you to be charged with cyber incitement as well as ordinary incitement, as well as the ordinary crime of intimidation. We would argue that to add more crimes here is to miss the point – if the social fabric is weak, adding another crime will not stop angry words.

The South African Constitution states that freedom of expression cannot extend to expression that expresses:
a. Propaganda for war;
b. Incitement of imminent violence; or
c. Advocacy of hatred that is based on race, ethnicity gender or religion and that constitutes incitement to cause harm.

Is this section consistent with the constitution? Not in our view. Again we have the problem of the use of the word “unlawfully” in the formulation of the crime, but put that to one side – the crime here is not to incite imminent harm, but the general incitement causing of damage to property or violence against people, which is clearly too broad. The act of forwarding posts on social media, for the purpose of comment on them, would become potentially criminal in terms of this law.

The intention, as we understand it, is to deal with this in any event the hate crimes legislation, which has been published for comment.

In section 17, we see distributing information, which is harmful is a crime. “Harmful” then includes threatening any damage or violence at all, even if trivial, and far in the future. The intention of the section was to deal with cyber bullying, hence the language around intimidating, encouraging or harassing people to harm themselves.

Many cyber bullying behaviours already fall under existing criminal law (e.g., harassment, assault, certain acts of hate under Promotion of Equality and Prevention of Unfair Discrimination Act) or civil law (e.g., defamation.) In fact, an interdict in terms of the Harassment Act is contemplated in relations to cyberbullying: “harassment" means directly or indirectly engaging in conduct that the respondent knows or ought to know-

(a) causes harm or inspires the reasonable belief that harm may be caused to the complainant or a related person by unreasonably-

(i) following. watching. pursuing or accosting of the complainant or a related person, or loitering outside of or near the building or place where the complainant or a related person resides, works, carries on business, studies or happens to be;
(ii) engaging in verbal, electronic or any other communication aimed at the complainant or a related person, by any means, whether or not conversation ensues; or
(iii) sending, delivering or causing the delivery of letters, telegrams, packages, facsimiles, electronic mail or other objects to the complainant or a related person or leaving them where they will be found by, given to. or brought to the attention of, the complainant or a related person; or
(b) amounts to sexual harassment of the complainant or a related person;

In many American state jurisdictions, bullying is dealt with as a school level issue, and schools are required to have policies in place to deal with bullying as well as cyber bullying. There is American case law to the effect that such disciplining of children in term of the bullying policy does not amount to a first amendment violation. This is a potentially useful approach, but not one that should be contemplated in a cybercrime bill.

Sec 38

This section has a useful idea behind it. The idea is that there is a problem with the Regulation of Interception of Communications and Provision of Communication – related Information Act 2002, which is currently the subject of a constitutional court challenge, and is under review by the Department of Justice after adverse comments by the UNHRC.

The problem is essentially that there are two ways of getting evidence related to communications. The first is a sec 205 subpoena in terms of the Criminal Procedure Act. The second is RICA. RICA is more cumbersome and results in around 3000 subpoenas a year. Sec 205 is much easier to use, and results in many more warrants, in the order of 50 000. So we have an obvious concern – RICA is not being correctly applied.

This legislation requires in sec 38(1) and (2) that RICA must be used when getting evidence of metadata, so when a phone call is being made, where from, how long it is etc. There are at least three problems here. The first is the idea of passing a second law, asking that a first law be implemented. This is unusual. In future, to understand the relevant sections in RICA, you will have to read them with sec 38 of this law.

Secondly, it does not remedy the underlying issue of sec 205 being an alternative to RICA. 16(4) and 18(a) subpoenas in terms of RICA specifically allow for the application of any other law. The remedy might be to amend RICA, or it might be to Amend sec 205. It cannot be that the remedy is to pass another law, clarifying the first law.

We propose that this section be referred to the RICA review process.

Sec 57 - 58

We wish to draw the committee's attention to this section as being problematic in two ways. The first is that it is similar to the National Key Points Act, a controversial law, which is under review.

Why is this essentially the National Key Points Act for computers? In principle, there are people in the private sector who do things that we both value but also create a risk. Like an oil refinery, or a weapons manufacturing plant, we need to ensure that the security of such buildings is up to the right standard – high fences, properly trained guards etc. The National Key Points Act is a way of ensuring that such a private owner spends enough on the right security, in order to ensure we are all safe.

The parallel with the critical information infrastructure section of the Bill is obvious. We need to be able to ensure that where there are computers in the private sector, which create a large systemic security risk, the owners of those systems spend enough money on security. That is what these sections seek to do.

The Bill was significantly improved to create greater protections for those who might find themselves on the other end of being declared such infrastructure. However, there is a conceptual problem. The Bill allows the Minister of State Security to declare as critical information infrastructure computers that are controlled by a Municipality, or those entities as defined in the PFMA, being:

Schedule 1

1. The Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities
2. The Commission on Gender Equality
3. The Financial and Fiscal Commission
4. The Independent Communications Authority of South Africa
5. The Independent Electoral Commission
6. The Municipal Demarcation Board
7. The Pan South African Language Board

8. The Public Protector of South Africa
9. The South African Human Rights Commission

Schedule 2

1. Air Traffic and Navigation Services Company Limited
2. Airports Company of South Africa Limited
3. Alexkor Limited
4. Armaments Corporation of South Africa Limited
5. Broadband Infrastructure Company (Pty) Ltd
6. CEF (Pty) Ltd
7. DENEL (Pty) Ltd
8. Development Bank of Southern Africa
9. ESKOM
10. Independent Development Trust
11. Industrial Development Corporation of South Africa Limited
12. Land and Agricultural Development Bank of South Africa
13. South African Airways (Pty) Limited
14. South African Broadcasting Corporation Limited
15. South African Express (Pty) Limited
16. South African Forestry Company Limited
17. South African Nuclear Energy Corporation Limited
18. South African Post Office Limited
19. Telkom SA Limited
20. Trans-Caledon Tunnel Authority
21. Transnet Limited

and those institutions which form part of Schedule 3 of the PFMA, which I attach as Annexure 1.

The bill allows for declaring of critical information infrastructure even in relation to areas of exclusive provincial competence.

This would of course mean that if such infrastructure is declared ‘critical’ for the purposes of the Act, and the steps taken as arbitrated on are not complied with, the State Security Agency may then take those steps, recover the cost, and prosecute those who do not co operate. This is unnecessary in relation to those entities that form part of the state, which are governed by the Minimum Information Security Standards. These standards have not been updated since 1996, and it is evident that an update of MISS is urgent. However, again it is not necessary to re-legislate the MISS via this section of the Bill, which would in any event apply piecemeal. If it is the intention not to include these institutions as critical infrastructure, then they should be excluded from the Bill.

If municipalities find themselves on the end of such declarations they will struggle to find the funding for it. In the private sector there is a revenue stream, and security is paid for out of that. If you cannot afford to secure the risk, then the business is not

profitable and may be closed. If a municipality cannot afford computer security, it cannot simply be declared bankrupt. There is some argument for saying SOE's have an income and can logically included in the list of those who can be 'declared.' But any entity, which relies on taxes and is part of the state must be secured through the state, not by means of requiring them to take actions over an above those they have in their budget. That is in essence an unfunded mandate and should not be imposed.

This is a complex area and is the subject of an on-going process around the review of the National Key Points Act. This section might best be deferred to that process.

Annexure 1

Schedule 3

OTHER PUBLIC ENTITIES
Part A: National Public Entities
1. Accounting Standards Board
2. Africa Institute of South Africa
3. African Renaissance and International Cooperation Fund
4. Agricultural Research Council
5. Agricultural Sector Education and Training Authority
6. Artscape
7. Banking Sector Education and Training Authority
8. Boxing South Africa
9. Breede River Catchment Management Agency
10. Castle Control Board
11. Chemical Industries Education and Training Authority
12. Clothing, Textiles, Footwear and Leather Sector Education and Training Authority
13. Commission for Conciliation Mediation & Arbitration
14. Compensation Fund, including Reserve Fund
15. Competition Commission
16. Competition Tribunal
17. Construction Education and Training Authority
18. Construction Industry Development Board
19. Council for Geoscience
20. Council for Medical Schemes
21. Council for the Built Environment
22. Council on Higher Education
23. Cross-Border Road Transport Agency
24. Die Afrikaanse Taal Museum
25. EDI Holdings (Pty) Ltd
26. Education Labour Relations Council
27. Education, Training and Development Practices Sector Education and Training Authority
28. Electronic Communications Security (Pty) Ltd
29. Energy Sector Education and Training Authority
30. Estate Agency Affairs Board
31. Film and Publication Board
32. Financial Intelligence Centre
33. Financial Services Board
34. Food and Beverages Manufacturing Industry Sector Education and Training

Authority
35. Forest Industries Sector Education and Training Authority
36. Freedom Park Trust
37. Health and Welfare Sector Education and Training Authority
38. Housing Development Agency
39. Human Sciences Research Council
40. Independent Regulatory Board for Auditors
41. Information Systems, Electronics and Telecommunications Technologies Training Authority
42. Ingonyama Trust Board
43. Inkomati Catchment Management Agency
44. Insurance Sector Education and Training Authority
45. International Marketing Council
46. International Trade Administration Commission
47. iSimangaliso Wetland Park
48. Iziko Museums of Cape Town
49. Legal Aid Board
50. Local Government, Water and Other Related Services Sector Education and Training Authority
51. Luthuli Museum
52. Manufacturing, Engineering and Related Services Sector Education and Training Authority
53. Marine Living Resources Fund
54. Market Theatre Foundation
55. Media Development Diversity Agency
56. Media, Advertising, Publishing, Printing and Packaging Sector Education and Training Authority
57. Medical Research Council of South Africa
58. Mine Health and Safety Council
59. Mining Qualifications Authority
60. Municipal Infrastructure Investment Unit
61. Natal Museum
62. National Agricultural Marketing Council
63. National Arts Council of South Africa
64. National Consumer Commission
65. National Consumer Tribunal
66. National Credit Regulator
67. National Development Agency
68. National Economic Development and Labour Council
69. National Electronic Media Institute of South Africa
70. National Empowerment Fund
71. National Energy Regulator of South Africa
72. National Film and Video Foundation of South Africa
73. National Gambling Board of South Africa
74. National Health Laboratory Service
75. National Heritage Council of South Africa
76. National Home Builders Registration Council

77. National Housing Finance Corporation Limited
78. National Library of South Africa
79. National Lotteries Board
80. National Metrology Institute of South Africa
81. National Museum, Bloemfontein
82. National Nuclear Regulator
83. National Regulator for Compulsory Specifications
84. National Research Foundation
85. National Student Financial Aid Scheme
86. National Urban Reconstruction and Housing Agency
87. National Youth Commission
88. National Youth Development Agency
89. Nelson Mandela National Museum
90. Northern Flagship Institution
91. Office of the Ombud for Financial Service Providers
92. Office of the Pension Funds Adjudicator
93. Performing Arts Council of the Free State
94. Perishable Products Export Control Board
95. Ports Regulator of South Africa
96. Private Security Industry Regulatory Authority
97. Productivity SA
98. Public Sector Education and Training Authority
99. Railway Safety Regulator
100. Road Accident Fund
101. Road Traffic Management Corporation
102. Robben Island Museum
103. Rural Housing Loan Fund
104. Safety and Security Sector Education and Training
105. Servcon Housing Solutions (Pty) Ltd
106. Services Sector Education and Training Authority
107. SETA for Finance, Accounting, Management Consulting and Other Financial Services
108. Small Enterprise Development Agency
109. Social Housing Foundation
110. South African Civil Aviation Authority
111. South African Council for Educators
112. South African Diamond and Precious Metals Regulator
113. South African Heritage Resources Agency
114. South African Library for the Blind
115. South African Local Government Association
116. South African Maritime Safety Authority
117. South African National Accreditation System
118. South African National Biodiversity Institute
119. South African National Parks
120. South African National Space Agency
121. South African Qualifications Authority
122. South African Revenue Service

123. South African Social Security Agency
124. South African Tourism
125. South African Weather Service
126. Special Investigation Unit
127. State Information Technology Agency
128. Technology Innovation Agency
129. The Co-Operatives Banks Development Agency
130. The National English Literary Museum
131. The Playhouse Company
132. The South African Institute for Drug-free Sport
133. The South African National Roads Agency Limited
134. The South African State Theatre
135. Thubelisha Homes
136. Tourism, Hospitality & Sport Education and Training Authority
137. Transport Education and Training Authority
138. uMalusi Council for Quality Assurance in General and Further Education and Training
139. Unemployment Insurance Fund
140. Universal Service and Access Agency of South Africa
141. Universal Service and Access Fund
142. Urban Transport Fund
143. Voortrekker Museum
144. War Museum of the Boer Republics
145. Water Research Commission
146. Wholesale and Retail Sector Education and Training Authority
147. William Humphreys Art Gallery
148. Windybrow Theatre
All subsidiaries of the above national public entities

Part B: National Government Business Enterprises

1. Albany Coast Water Board
2. Amatola Water Board
3. Bloem Water
4. Botshelo Water
5. Bushbuckridge Water Board
6. Council for Mineral Technology
7. Council for Scientific and Industrial Research
8. Export Credit Insurance Corporation of South Africa Limited
9. Ikangala Water
10. Inala Farms (Pty) Ltd
11. Khula Enterprises Finance Limited
12. Lepelle Northern Water
13. Magalies Water
14. Mhlathuze Water
15. Namaqua Water Board
16. Ncera Farms (Pty) Ltd

17. Onderstepoort Biological Products Limited
18. Overberg Water
19. Passenger Rail Agency of South Africa
20. Pelladrift Water Board
21. Public Investment Corporation Limited
22. Rand Water
23. SA Bureau of Standards
24. SA Special Risk Insurance Association Limited
25. Sedibeng Water
26. Sentech Limited
27. State Diamond Trader
28. Umgeni Water
29. Umsobomvu Youth Fund

All subsidiaries of the above national government business enterprises