Cybercrimes Bill threatens our freedom

By Murray Hunter

28 Jul 2017

The Cybercrimes and Cybersecurity Bill will affect every internet user in South Africa - but at 139 pages long, there's a lot to go through. But if you haven't yet, now is the time! There's just two days left to give parliament your comments on the bill.

Friday 28 July is the final day to comment on the the Cybercrimes and Cybersecurity Bill. Image: Hypnobay on Pixabay (public domain)

UPDATE: Since this article was published the deadline has been extended to 10 August 2017.

Why has this bill been introduced? The government says it will help fight cybercrime and make South Africa's cyberspace more secure. In 2015, Right2Know criticised the draft version of the bill for threatening internet freedom, and thousands of internet users signed a petition denouncing it. The 2017 bill has some welcome changes from its 2015 draft version, but a lot of remaining concerns.

Good changes are:

- The "secrecy bill clauses" in the 2015 draft bill, which would have criminalised journalists and whistleblowers for accessing classified information, are gone.
- The copyright offences in the 2015 draft bill, which could have criminalised you for posting a meme, are gone.

But there's some bad stuff.

Section 17 of the bill makes it a criminal offence to send or resend "malicious communication", which includes messages that could be harmful in various ways. This part of the bill is new. This is what state security minister David Mahlobo was talking about when he proposed social media regulation – a proposal that has been widely rejected on social media under the hashtag #HandsOffSocialMedia. (You can add your name to that call here!)

Don't insult Mr Trump

Section 17(2)(c) of the bill makes it a crime to send or resend a message that "intimidate[s], encourages or harasses" a person to harm themselves or someone else.

While we 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 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 of an unpopular leader would be criminal offences under this provision.

In any case, genuine cyberbullying should be dealt with in the Protection from Harassment Act of 2011, which allows someone to get a protection order against their harasser – after which, continued harassment is a criminal offence. Unfortunately, the implementation of that Act has been extremely poor and has not delivered its promised protections to victims of harassment. But that is a failure of the justice system itself, not the existing law. The additional criminal penalties imposed by the Cybercrimes Bill give no further protections.

One positive thing: section 18 of this bill very rightly criminalises revenge porn.

Fake news

Section 17(2)(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”.

While this provision should have the programming manager of ANN7 feeling nervous, it is a bad idea. Even if the intention behind the Bill is noble, in practical legal terms it’s a mess. Who defines ”inherently false”? What is the borderline with “misleading”, “debatable”, or “unverifiable”? Would the law look at the intention of the message or the consequences? How is the “harm” measured?

Given the rise of politically motivated and vexatious prosecutions, a “fake news” clause would provide another avenue through which the state could intimidate investigative journalists and voices of dissent.

Criminalising retweeting

The bill also makes it a crime to resend a message of which 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.

If there is something in the message that could be seen as threatening or inciting violence or property damage, or intimidating someone to harm themselves, or if the message is “inherently false in nature”, you are as guilty of an offence as the person who originally wrote it.

This does not take into account your intention for re-sending such a message. It would be very common for social media users to repost an offensive or irresponsible or even criminal message in order to draw attention to it.

More surveillance

The bill tries to reform Rica, South Africa’s main surveillance law, but without addressing any of the problems with Rica that have led to serious surveillance abuses and pointless SIM card bureaucracy for all of us.

More power to State Security

This bill gives the Ministry of State Security a large role in governance in South Africa. Placing cyber security under the domain of the intelligence agencies makes cybersecurity initiatives less transparent and harder for the public to have a say in them.

The law threatens freedom and could be used to intimidate government critics. But does it make us more secure? In an article to be published tomorrow I will explain the law’s shortcomings when it comes to making the internet more secure.

P.S. If you're worried about how this bill will affect freedom of expression, add your name to our Awethu campaign: Hands Off Social Media!

You can also make your own submission to parliament by 10 August 2017.

Read part two of this article: Cybercrimes Bill make cyberspace less secure

---

Published originally on GroundUp.

ABOUT THE AUTHOR