ALL RISE SAY NO TO CYBER ABUSE

RESPONSE TO THE SOUTH AFRICAN CYBERCRIME AND CYBERSECUIRTY BILL 2017

13 August 2017

INTRODUCTION

ALL RISE – SAY NO TO CYBER ABUSE welcomes the Department of Justice's consultation on the Cybercrime and Cybersecurity Bill (the "Bill") and appreciates the focus of the Department on *effectively dealing with cybercrimes and addressing aspects relating to cybersecurity, which adversely affect individuals, businesses and Government alike* and *putting in place the required building blocks necessary to address cybercrime in South Africa*, as stated by your Deputy Minister for Justice and Constitutional Development, the Hon JH Jeffery, MP.

All Rise Say No to Cyber Abuse ('All Rise') is an international not for profit organisation with the purpose of bringing greater responsibility to the use of the internet, encompassing the eradication of the criminal activity labelled as cyber abuse on a global scale. This includes via research, education and better regulation wherever needed. This submission is therefore focused on the aspects of the Bill that pertain to cyber abuse, with the intention to provide a greater level input, rather than a simple comprehensive technical assessment.

We would like to support the Department's work in this area and would be happy to meet discuss and/or to participate in oral representations. In the meantime, please let us know if there are questions or clarifications we can address or further information we can provide in relation to this submission or otherwise.

CONTEXT

1. ALL RISE founded and established in the UK, has a global view and objective. The understanding that cyber abuse is a problem of epidemic proportions affecting humanity, not confined to particular countries within neat jurisdictional boundaries. Keeping in sight the needs of society as a whole should be the guiding light on how to move forward on these issues and South Africa can be a global leader in that regard, alongside countries like New Zealand, taking bold action on this subject.
2. 40% of the world population use the internet – equating to more than 3.5 billion people. Cyber abuse is a growing problem and press coverage, societal concern and extreme cases are on the rise, and seemingly being brushed aside as a "normal" part of everyday life. A 2015 ALL RISE global survey of 12,000 people showed that 72% of participants had witnessed cyber abuse and 1 in 3 had

witnessed it at least 6 times. 38% had suffered cyber abuse themselves. The Pew Research Centre shows similar findings. The imperative is clear.

3. There are evident concerns that cyber abuse, which encompasses cyber-bullying, cyber-trolling, cyber-harassment and cyber-stalking, are on the rise. Anyone can now use the internet as the modern day weapon of choice, a vehicle or a machine gun for hate and abusive conduct. This weapon can be fired in any capacity, with the present limited responsibility or accountability taking place. There needs to be a moment where the question is asked: when does the perpetrator stop harming their victim? Do they continue until there has been a life threating effect? This therefore presents serious physical and mental health[1] risk factor, that ultimately has an impact on each of us in the offline world, rippling into effects on to our national health services and global economy.
4. A societal reset on a major scale is needed and that can be precipitated by decisive legislative change, policing prioritisation and/or a dramatic change in policy on the part of the social media and blogging platform companies that host the relevant content. The standards of decency and respect need to be brought back to humanity's daily interaction no matter the medium that is used, online or offline. Responsibility for our behavior and understanding that the bar needs to be raised as to what is accepted on a societal level so we know the platform we set for the next generation is one that will encourage youth to have, as a minimum, decency and respect in all facets of life. The cohesive and emphatic work done by the Internet Watch Foundation on a global scale addressing online child sexual abuse shows what can be achieved when industry, government and law enforcement come together.

HEADLINE POINTS ON THE BILL

5. Many countries across the world are recognising the need to address cyber abuse related crime. Whilst much criminal conduct covered by the Bill was already unlawful under existing laws such as the Criminal Procedure Act 1977 and the Promotion of Equality and Prevention of Unfair Discrimination Act 2000, by bringing forward the Bill, South Africa is not only consolidating and strengthening the law in this area, but also sending a strong signal that tackling cybercrime is a priority for the country.
6. Cyber abuse is commonly cross-jurisdictional, either in respect of the perpetrator and victim being in different states or countries, or in respect of the location of the company hosting the content, versus the victim and law enforcement. We live in an increasingly borderless and globalized world

[1] As Paula Todd writes in her book Extreme Mean, 'My research revealed that the problem with cyberabuse is far, far bigger, that it is affecting adults, everybody. Not just being the target of cyberabuse but reading it and being exposed to it all the time is bad for us. We already have a mental health problem around the world… we are building a social and mental health crisis.'

which naturally is a challenge of our times to ensure we can adequately protect our global citizens in that context. This is the responsibility of all governments, globally.

7. Electronic communications service providers are a critical part of the solution, with cybercrime happening via their networks. All Rise supports the introduction of formal obligations for all service providers including blogging and social networking service providers, to assist, rather than relying on goodwill.
8. With our citizens engaging electronically, access to electronic evidence in cybercrime cases is vital. Current processes for obtaining electronic evidence from companies outside the jurisdiction are not fit for purpose in terms of volume, speed or availability.
9. Save in certain situations, the companies on whose systems cyber abuse is commonly perpetrated are not under an obligation to verify the identity of their users or proactively to report to law enforcement and preserve data in the event of an issue arising.

SPECIFIC POINTS ON THE BILL

Electronic Communications Service Providers Definition

10. For the purposes of the malicious communications provisions, given the harm and harassment occurring on their networks and the electronic communications they facilitate e.g. via email or chat features, All Rise recommends providers of blogging and social networking services be clearly within scope of the Bill and not only service providers with an electronic communications licence.

Malicious Communications/Cyber Harassment

11. All Rise supports the addition of cyber harassment as a specific category of criminal conduct.
12. All Rise recommends the criminality be extended so that it covers not just a single form of abusive conduct (sending a harmful data message), but also covers harassment equal to the criminal offence of harassment offline. Sending a harmful data message is only one method or type of conduct and the law would benefit from future-proofing and from the certainty of providing for all cyber-abusive criminal conduct to be addressed in a consolidated way.
13. Section 17(d) prescribes a 2-step test for when a false data message will be considered harmful. The section requires (i) the message to be aimed at causing harm (intent) and (ii) that a reasonable person would regard the message to be harmful. The inclusion of an intent requirement introduces complexity and provides a route via which disingenuous perpetrators can argue they did not mean to cause harm. This then enables the modern day criminal to shoot down their victim under irresponsibility and walk away from the scene of the crime with blood on their hands whilst pleading

it wasn't their intent to pull the trigger. All Rise proposes the reasonable person test alone to be a well-established and understood concept that is more than sufficient to ensure fairness. To put simply, if a victim is stating their livelihood physically or mentally is being affected by the harassment and stalking nature of the criminal activity, it is our duty of care to ensure that all are free from harm in any capacity. All Rise recommends the deletion of the intent requirement.

Intimate Images

14. All Rise welcomes the inclusion of section 18 into the Bill.
15. Given the increasing prevalence of 'creep shots' and 'upskirt' images, All Rise recommends the Department considers extending the Bill to cover possession and distribution of such images and not just nude images.

Interim Protection Orders

16. The harm caused by cyber harassment and cyber stalking is significant. Therefore we have the responsibility to ensure all who use the vehicle of the internet are protected and cyber harassment is then actioned and eradicated, in turn protecting victims. Providing the ability to serve service providers with a formal call to action to help enforce interim protection orders for victims will be a critical part of the solution and removes the need to rely on goodwill to address cyber abuse.
17. Requiring service providers to enforce the terms of an interim protection order against a cyber harassment offender is a practical and welcome step. Presumably, this could take various forms, such as suspension of the service to an offender, removing messages/content or blocking contact with a particular contact so they cannot continue the harassment or stalk.
18. All Rise is interested to understand further how readily interim protection orders will be issued and how big a barrier the administration involved will be, particularly in light of the increasing volume of cyber harassment cases.
19. All Rise recommends the Department automates the process of applying for and issuing interim protection orders, to ensure they are easy to apply for and generously granted wherever needed. Once such orders become common for cases of cyber harassment and awareness of this increases with perpetrators or would-be perpetrators, this has the potential not only to protect victims, but also to provide a deterrent effect.
20. All Rise is again interested to understand how the Department will enforce cooperation on the part of the service providers and how readily fines, for example, will be utilisted and to what level.
21. Also how the issue of anonymity in cyber harassment will be addressed and managed, for example where blogging platforms and social networks are within scope of the provisions and the identity of the customer has not been validated, interim production orders may be available against 'persons

unknown'.

22. All Rise is also interested to understand what other mechanisms will be utilised to ensure 'low level' cyber harassment does not go un-addressed. It is the case in other countries that only the most extreme cases of cyber abuse are prosecuted, which sends a message to 'not so extreme' perpetrators or would-be perpetrators that they will be unlikely to be held to account for their actions.

Preservation and Disclosure of Electronic Evidence

23. As regards preservation and collection of information necessary to investigate and prosecute cases, it is currently too difficult for victims to obtain (or law enforcement on their behalf) identifying data of their perpetrators. Contributing factors are:
    a. *anonymity*
    b. *the volume of abuse*
    c. *companies hosting relevant data being outside the jurisdiction*

24. *Anonymity*
    a. There has been much commentary on the problem of anonymity in respect of users of social networking services. The Pew Research Project cites 63% of internet users believe online environments allow for more anonymity than in their offline lives.
    b. Many blogging and social media platform providers are providing electronic communication-style services and do not validate identity when a user signs up to their service, which means only IP address, device ID and traffic data will often be available as evidence. This is insufficient and results in an inefficient and resource intensive breadcrumb-following exercise to establish the identity of the offender.
    c. This is an important issue that needs to be addressed to ensure the goals of the Bill are not undermined by insufficient availability of evidence or too narrow a remit over service providers.

25. *Volume of Abuse*
    a. With an already huge volume of cyber abuse statistics and cases on the increase, All Rise is interested to understand whether the Department is considering systems and procedures to streamline the process of evidence gathering and related activity, for example automating the court order and warrant application processes and service of data disclosure demands and other requests on service providers. It would be failing victims for the sheer volume of abuse to be a barrier to justice.

26. *Companies hosting relevant data being outside the jurisdiction*

a. Until countries come together and/or the platform and social media companies change their policies, it is hard to see how individual countries can adequately address cyber offences that take place across border jurisdictions, without seeking to enforce their own individual laws and scenarios. The most solid foundation for action is to ensure the relevant laws are expressed to have extra-territorial effect, as is set out in the Bill.
b. The Mutual Legal Assistance Treaty processes for obtaining evidence cross-border continue to be cumbersome and in dire need of an overhaul. All Rise is interested to understand whether the Department will be working on this alongside the implementation of the Bill.

27. All Rise also notes the concept of expedited preservation and access to electronic evidence relating to cyber harassment in section 39. Given the increasing number of cases of cyber abuse causing mental anguish and suicide, there would be value in the Department articulating the circumstances in which an expedited process would not be suitable for cyber harassment.

Obligations of Electronic Communications Service Providers

The obligations in chapter 9 on electronic communications service providers to report chapter 2 (cyber security) issues is understood, in light of the extensive harm to intangible property and infrastructure that can arise as a result of cybersecurity issues. Given the prevalence of cyber abuse and the devastating true human harm it causes, All Rise recommends the Department also establishes equivalent obligations in the Bill in relation to reporting and assistance on cyber harassment. The same goes for the establishment of a Cyber Response Committee in chapter 10 – there is a clear need for crisis management on cyber abuse.

Penalties

Given the extensive and enduring harm caused by cyber abuse, to individuals, businesses and communities, All Rise presents that a 2 or 3 year prison sentence is insufficient.

Could it be clarified further as to the level of fine proposed under the Bill for malicious communications.

Statistics of Prosecutions

All Rise supports the instruction to the Director of Public Prosecutions in section 60 of the Bill, to keep and disclose statistics relating to malicious prosecutions under sections 16, 17 and 18. Transparency and data insights will play a critical part in addressing cyber abuse worldwide.

However, the number of prosecutions sought will depend on the degree to which cyber abuse is a policing and prosecution priority. All Rise is interested to understand how the Department intends to address this.

CONCLUSION

The Bill is a welcome development in the area of cyber harassment. There are aspects that require strengthening if the devastation of cyber harassment is to be considered a priority.

The way the Bill is implemented and utilised will shape the next 5+ years in respect of cyber abuse in South Africa. The Department may already be considering how to maximise the potential for a societal shift here, for example via an awareness campaign on harassment, calling people back to principles of shared respect.

All Rise would like to support the work of the Department in addressing cyber abuse, including the implementation of the Bill, for example in addressing freedom of speech and other factors, providing research, awareness-raising initiatives, training for staff and beyond, and technical issues.

ALL RISE looks forward to seeing the Department's further work on this subject and is available to participate in further discussion and/or provide any additional information or clarification needed.

Website: http://www.allrisesaynotocyberabuse.com/
Email: contact@allrisesaynotocyberabuse.com
Twitter: AllRiseGlobal
Point of contact: Simone Benhayon