CENTRE FOR LAW AND DEMOCRACY

Trinidad and Tobago

Note on the Cybercrime Bill, 2015

August 2015

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction[1]

The growth of the Internet, while providing unprecedented benefits to human rights, particularly freedom of expression, also poses novel challenges from a regulatory perspective. Legal frameworks governing issues such as communication, commerce and privacy need to be adapted to align with the changes wrought by the digital transition. To this end, in May 2015 the government of Trinidad and Tobago introduced the Cybercrime Bill, 2015 (the Bill), a legislative package which includes newly constituted cyber offences and rules for law enforcement investigations into online crimes.

Six weeks after it was introduced, the Bill lapsed.[2] However, given its similarities to a previous draft law, which was proposed in 2014, it is likely that this Bill, or a similar one, will be reintroduced in the near future. Although the Bill, as it was introduced in May 2015, had many positive features, such as its clear protections for online intermediaries, several of the newly created cybercrimes are of concern since they threaten to criminalise innocuous, commonplace or even beneficial online behaviour. Perhaps tellingly, the Bill itself acknowledges in its preamble that it is inconsistent with the rights guaranteed in the Constitution (which include freedom of expression), although Trinidad and Tobago's Constitution allows such a statute to be passed by a three-fifths vote of the legislature.

We recognise the need to modernise legislation to take into account the changes wrought by the digital transition. However, in drafting laws which impact online speech, it is important to bear in mind that a significant part of the Internet's value as an expressive medium flows from its open and borderless nature, qualities which can only be preserved through a light regulatory touch. In order to fully harness the power of the Internet, with all of its economic, cultural and human rights benefits, the people of Trinidad and Tobago must be allowed to communicate freely online.

This Note examines the major issues with the Bill from a freedom of expression perspective and provides concrete recommendations for how its language should be amended to bring it into line with international human rights standards. If and when the government of Trinidad and Tobago decides to reintroduce this legislation, we urge them to consider these amendments in order to ensure that the Bill respects

---

[2] The Bill's status is available on the Trinidad and Tobago Parliament website: http://www.ttparliament.org/publications.php?mid=28&id=722.

the right to freedom of expression and does not harm the country's burgeoning online culture.

1. Freedom of Expression and the Internet

As with all laws impacting speech, the Bill should be crafted in a manner which respects Article 19(3) of the *International Covenant on Civil and Political Rights* (ICCPR),[3] which Trinidad and Tobago ratified in December 1978, and which states:

> The exercise of the [freedom of expression] rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Restrictions on the right to freedom of expression are only legitimate if they are consistent with the test set out in Article 19(3) of the ICCPR. This means that restrictions must be clearly spelled out in law, must aim to protect one of the legitimate interests listed in Article 19(3) and must be necessary for the protection of that interest. The latter means, among other things, that any restrictions must be designed so as to impair freedom of expression as minimally as possible. The UN Human Rights Committee has summarised these conditions as follows:

> Restrictions must not be overbroad. The Committee observed in general comment No. 27 that "restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected . . . The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law". The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.
>
> When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat. [references omitted][4]

[3] UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.
[4] General Comment No. 34, 12 September 2011, CCPR/C/GC/34, paras. 34 and 35.

Trinidad and Tobago's online community is growing rapidly. From 2010 to 2013, Internet usage increased from 50% to 63.8%.[5] This means that many of its Internet users are still relative newcomers to the medium. Given that many local users are still discovering the Internet, it is particularly important to avoid criminalising normal online behaviours. The potential for a chilling effect, whereby individuals limit the ways in which they use new technologies out of fear of falling foul of the rules, even where they are not actually at risk of this, is magnified significantly given the novelty of the medium and the fact that its users are still discovering their voices online.

2. Overbroad Offences

The necessity requirement of Article 19(3) of the ICCPR, as noted above, means that any restrictions on freedom of expression must impair the right as little as possible. A well-crafted law will carefully carve out the area of limitation, forbidding only harmful speech. Anything which is not explicitly prohibited should be allowed.

Contrary to these principles, many of the offence definitions in the Bill create a reverse onus on users to justify their conduct, stating that particular actions should not be taken "without lawful excuse or justification." Many of these behaviours are defined very broadly and include not only potentially harmful activity but also innocuous or normal aspects of digital speech. For example, Section 5 makes it an offence to access a computer system for the purpose of securing access to data, while section 6 makes it an offence to remain logged into a computer system. These sorts of activities could be harmful, for example if the objective was to steal data, but they could also be innocuous, for example if the objective was to place cookies on the computer. They might even be deemed to cover employees who remained logged onto their work computers at the end of the day to check personal emails or browse the Internet, if that were not formally allowed by the terms of their employment.

This type of reverse onus runs entirely contrary to the freedom of expression protections in the ICCPR since, rather than carving out a limited area of prohibited conduct, the law applies a presumption of criminality to expressive digital behaviour, and then shifts the onus onto users to demonstrate that they are operating legitimately. Moreover, the meaning of "lawful excuse or justification" is incredibly vague, particularly when applied to actions as common as being logged into a computer system. Where the behaviour is inherently harmful, this sort of shift of onus can be seen as a defence and hence a way of mitigating the harshness of a rule. For example, section 9, makes it an offence to obtain data which is protected against unauthorised access and which is not intended for the person in question.

[5] Internet usage statistics are available at: http://www.itu.int/net4/itu-d/icteye/.

This is a legitimate (narrowly defined and inherently harmful) offence for which the inclusion of the phrase "without lawful excuse or justification" provides defendants with a possible avenue to justify their conduct.

Recommendation:

- The offences under sections 5, 6, 7, 8, 10, 13, 14 and 15 should be significantly narrowed, so that they only apply to inherently harmful conduct and the requirement to prove lawful justification should only apply in such cases.

3. Duplicate Offences

While cybercrimes may seem to be a new phenomenon, the vast majority of them are simply electronic versions of offences which have existed for decades or more. Many if not all aspects of computer fraud, for example, are already covered by garden-variety prohibitions on fraud. While it is important to update criminal rules to take into account the digital context – recognising that some criminal activities, such as the generation of computer viruses, are specific to a digital context – it is easy to overestimate the need to create new crimes or even adapt existing rules to address digital realities.

Several of the 'new' offences created by the Bill appear already to be covered under existing legislation. For example, the illegal interception offence in section 7 of the Bill duplicates existing offences in the Interception of Communications Act, which already carries maximum penalties of TTD 500,000 (approximately USD 79,000) and seven years' imprisonment.[6] Similarly, section 20(1)(a) of the Bill creates an offence of using a computer system to harass, intimidate or coerce someone, although these behaviours are already prohibited by the Offences Against the Person Act, including a maximum penalty of TT$5,000 (approximately US$790) and five years' imprisonment.[7] Section 20(2) of the Bill prohibits extortion using a computer, though extortion of any kind is already illegal under the Larceny Act.[8] In considering these duplicate offences, it is important to make clear that the mere use of a computer in the commission of a crime should not, by itself, justify an additional penalty. In a digitising world, it is natural that an increasing number of crimes will migrate online. This is not, of itself, a reason to increase criminal penalties.

---

[6] Interception of Communications Act § 6, Chapter 15:08 (2012), available at: http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/15.08.pdf.
[7] Offences Against the Person Act § 30A, Chapter 11:08 (2009), available at: http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.08.pdf.
[8] Larceny Act § 33, Chapter 11:12 (2009), available at: http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.12.pdf.

Recommendation:

- The draft Bill should be reviewed so as to eliminate offences which are already covered under existing legislation, including sections 7, 20(1)(a) and 20(2).

4. Cyberbullying

Section 20(1)(b) of the Bill, which criminalises cyberbullying, is also problematical. Trinidad and Tobago would not be the first jurisdiction to adopt a law against cyberbullying. As increasing numbers of people move online, the challenges associated with preventing abusive online activities have been increasing, particularly where they impact on vulnerable young people. The great megaphone that the digital realm grants to ordinary people can be used to whip up online mobs in the thousands or even millions, unleashing unprecedented vitriol against a single target. Clearly, laws need to provide victims of these campaigns, which may be distinguished from their offline counterparts by their scale, with a measure of protection in appropriate cases.

However, experience suggests that cyberbullying laws have often been open to abuse. In 2013, the Canadian province of Nova Scotia passed the Cyber-safety Act in response to a high profile suicide of a young girl who has been bullied online.[9] Due to the law's broad scope, it was quickly subverted into a tool to enable politicians and other powerful interests to silence their critics.[10] Section 20(1)(b) of the Bill is even broader than Nova Scotia's law, since it covers offences which are just committed "recklessly".

Among the major problems with many cyberbullying laws, including the Cyber-safety Act and section 20(1)(b) of the Bill, is that they encompass legitimate speech on matters of public importance, the sort of speech which under defamation law would fall under a defence of fair comment. Politicians, particularly prominent ones, face a deluge of online criticism. But this should be par for the course in a democratic society. A person whose skin is too thin to deal with these attacks has no business in the political arena.

A related problem is that the current 20(1)(b) formulation – which includes any speech that might cause fear, intimidation, humiliation, distress, harm or detriment to a person's health, emotional well-being, self-esteem or reputation – is incredibly

[9] SNS 2013, c 2.
[10] David Fraser, "Nova Scotia's cyber bullying law is a disaster", Canadian Lawyer, 2 March 2015. Available at: www.canadianlawyermag.com/5493/Nova-Scotias-cyber-bullying-law-is-a-disaster.html.

broad. This could apply to all manner of perfectly legitimate speech, from a journalist who exposed corruption to a film critic publishing a scathing review.

Between section 20(1)(a), which prohibits harassment, and section 18, which prohibits non-consensual pornography, the tools to prevent legitimately harmful cyberbullying are already found in the Bill. So long as these are properly enforced, and the police are given adequate training to understand the intricacies of online speech, there is no need for an additional cyberbullying offence.

Recommendation:

- Sections 20(1)(b) and 20(4) should be deleted.

5. Other Problematical Offences

Another problematical offence in the Bill is section 13, which criminalises the unauthorised receiving or granting of access to computer data. Generally speaking, secrecy laws which criminalise the receipt of information by otherwise innocent third parties raise freedom of expression concerns. Leaks are an increasingly common part of the global discourse, and often perform a vital public function. Indeed, many of the biggest and most important news stories of recent years have come as a result of unauthorised leaks, which can contain information about corruption, environmental damage and threats to health and safety. While it may be reasonable to provide for penalties for breaching a computer system to obtain information, as are imposed by section 5, or sharing information beyond its authorised recipients, as is prohibited by section 9, the mere receipt of this information should not be an offence. In other words, when a journalist or blogger receives even illicitly obtained information, he or she should be able to report on the matter without fear of prosecution.

Section 14 also raises concerns insofar as it appears to prohibit any generation of inauthentic computer data. While ostensibly intended to prevent forgery, this would criminalise any inaccurate information. This is simply not appropriate and represents an online version of a prohibitions on the provision of false news, or false information, which is inconsistent with the right to freedom of expression. In accordance with Article 19(3) of the ICCPR, the list of legitimate reasons for restricting speech does not including promoting accurate speech simply for its own sake. Section 14 fails to link inaccuracy with some other harm to the public interest, such as the commission of fraud, or harm to the rights or reputations or others or to national security.

Furthermore, section 14 would apply to most privacy software, which depends on altering the user's information. While privacy tools can be used in the commission of crimes, the vast majority of their users simply do not like being watched and seek nothing more nefarious than basic online privacy. The United Nations Special Rapporteur on Freedom of Expression, David Kaye, made clear in a 2015 report that these tools are a key part of freedom of expression online:

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.[11]

Recommendations:

- Section 13 should be deleted.
- Section 14 should be deleted.

[11] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, UN Doc. A/HRC/29/32, para. 56.