COMMENTS BY M-NET AND MULTICHOICE ON THE CYBERCRIMES AND CYBERSECURITY BILL, B06-2017

10 August 2017

1. Introduction

1.1 Electronic Media Network Proprietary Limited ("M-Net") and MultiChoice Proprietary Limited ("MultiChoice") are both licensed by the Independent Communications Authority of South Africa ("ICASA") to provide subscription broadcasting services.

1.2 We wish to thank the Portfolio Committee for Justice and Correctional Services ("the Committee") for this opportunity to comment on the Cybercrimes and Cybersecurity Bill, B06-2017 (“the Bill”).

1.3 The issues we will comment on are the following:

1.3.1 Concerns about cyber piracy and proposals on how it can be dealt with in the Bill; and

1.3.2 Concerns about the unintended consequences, in relation to section 2 (Unlawful securing of access), section 3 (Unlawful acquiring of data) and (section 4 (Unlawful acts in respect of software or hardware tool).

2. What is Piracy?

2.1 Piracy entails the unauthorised access, use and reproduction of another's work. It can take many forms. It involves, amongst others, the following:

2.1.1 Unauthorized interception, decryption and retransmission of encrypted broadcast signals to-

(a) multiple customers of commercial broadcasters (licensed or unlicensed) on cable, IPTV, or satellite networks; or

(b) multiple dwelling units by apartment building managers, as part of their building management business.

2.1.2 Unauthorized interception, decryption and public exhibition of encrypted broadcast signals, in public commercial venues such as restaurants, bars, hotels, and members' clubs.

2.1.3 Unauthorized distribution and retransmission of broadcast signals (whether encrypted or free-to-air) on other platforms on a commercial basis, for example on the open Internet to increase traffic to and through online websites to increase advertising revenue or for payment.

2.1.4 Selling, advertising, and distribution of illicit devices or software to circumvent encryption measures to access TV services without permission or payment

2.2 There are several types of online cyber-piracy, for example-

2.2.1 live Internet streaming of unauthorised content without downloading the illegal content;

2.2.2 live broadcast, via IPTV, of unauthorised content without downloading the illegal content;

2.2.3 delayed Internet streaming of unauthorised content without downloading the illegal content;

2.2.4 downloading of copied broadcasts (movies, series, documentaries or Sport); and

2.2.5 copying and distribution of movies and TV series;

which content is, in most instances, acquired through unauthorised access to the broadcast signals of legitimate licensed broadcasting service providers.

2.3 Different websites make use of the above types of online cyber-piracy, including –

2.3.1 streaming sites, which allow people to view unauthorised content on demand. These websites may stream directly or provide links to content hosted on other websites;

2.3.2 cyberlocker sites, which offer fast, convenient and anonymous storing and distribution of content which can be downloaded or streamed;

2.3.3 peer-to-peer sharing networks which allow the sharing of files among peers. Most peer-to-peer sharing networks are set up to ensure that files downloaded by individuals are also uploaded onto the sire, so that any downloading of content by a member automatically results in the distribution on that content to others;

2.3.4 linking websites, which collate thousands of links to pirated content often stored on external cyberlockers; and

2.3.5 torrent websites which make use of BitTorent technology to enable speedy distribution of large files (such as pirated movies and music) over the Internet.

3. Cost of Piracy

3.1 When broadcasting signals or audio-visual content is pirated, it results in revenue losses across the entire TV content distribution chain from the content producers to the TV platform companies.

3.2 Television content, whether on free-to-air or subscription platforms, is not free. Artists, performers, writers and producers of TV content earn their living by being creative and charging broadcasters for the right to show their content.

3.3 Licensed broadcasters make significant investments in the acquisition or licensing of programming from third parties, which they arrange and package with their own content in creating their programme schedule.

Licensed broadcasters also invest in the equipment and infrastructure required to transmit that schedule as an electronic signal. They also make significant investments in marketing their content to increase viewership of their content. If financial returns are diverted to signal and content pirates, then it becomes difficult for a licensed broadcaster to continue to make these significant investments.

3.4 The loss of licensing revenue for broadcast programming does not just hurt the broadcaster, but everyone else in the supply and distribution chain. Revenues to writers, screenwriters, artists, actors, musicians and other producers are reduced as a result of the decreased rivalry and demand for broadcasting content which piracy causes.

Harm to National Objectives

3.5 Piracy in Africa therefore leads to rising costs for independent producers all the way through the value chain to platform providers and the end-user. Piracy also damages the national objectives of governments, amongst others the:

3.5.1 *investment environment* – investors are reluctant to invest in countries if they cannot earn a decent return because of competition from pirates who have no costs;

3.5.2 *creative environment* – piracy impairs the development of indigenous content production and job creation in the sector;

3.5.3 *rule of law* – pirates are usually not licensed and are broadcasting or distributing content that has not been authorised for distribution in that country;

3.5.4 *government revenue* – pirates don't pay taxes, which can amount in some cases to millions of dollars. That's money that could be used by government for schools, housing, health care or even encouraging further growth in the communications sector; and

3.5.5 *growing the sector* - broadcasters and independent producers in developing countries are harmed the most by piracy as they don't have the economies of scale of international broadcasters or distributors and are heavily reliant on revenue generated by sale and the exploitation of their intellectual property rights.

3.6 In South Africa, piracy is damaging the South African creative industries and steps need to be taken to protect it. The Economic Contribution of Copyright-based Industries in South Africa Report[1] published jointly by the Department of Trade and Industry and WIPO in 2011, highlighted the importance of copyright-based industries as contributors to the South African economy and employment creation. Piracy that impacts on the growth of creative industries, thus also impacts on the economic growth of South Africa.

Harm to Sport's Contribution to South African Economy

3.7 It is important to note that piracy is also globally having a huge impact on sport. South Africa's economy and demographics differ from other BRICS members, but it does have something in common with Brazil, Russia and China – it has hosted major global sporting events over the years, such as the FIFA World Cup, the Cricket World Cup and the Rugby World Cup. This has had positive spin-offs in terms of new and refurbished infrastructure (stadiums, transport, accommodation), created jobs and developed world class expertise in hosting world sporting events. The FIFA World Cup alone contributed 55.7 billion rand to South Africa's economy.[2] Sport can thus have a significant direct impact on a country's economy and it also contributed to hospitality and tourism sector in South Africa.

3.8 It's very clear then that sports events are a critical part of the sports industry and form the backbone of their contribution to the economy. There

---

1 https://www.thedti.gov.za/industrial_development/docs/Economic_Contribution.pdf , accessed on 8 August 2017

2 http://venturesafrica.com/the-world-cup-was-great-for-our-economy-south-african-sports-minister/ , accessed on 8 August 2017

is tremendous economic activity around sports events ranging from, amongst others, licensing, sponsorships, broadcasting rights and advertising rights. Agreements are negotiated sometimes years in advance with Leagues, Sports Associations, Clubs, broadcasters and advertisers to secure investments. Digital piracy negatively impacts on all those businesses.

3.9 The sale of broadcast rights represents a substantial source of revenue to the sports rights owners who invest and distribute this revenue throughout their organisations, from grassroots to professional leagues and clubs. It is a core component of what makes them sustainable. The live unauthorised streams of sports events globally across the Internet is therefore one of the most critical threats facings sports rights owners currently. Sports associations and bodies receive no compensation from any pirated re-broadcast of their events, whereas those providing the pirated live data stream profit from advertising embedded in the website or the software client.

3.10 These free live streaming websites also cause harm to users and their devices. More than half of the streams provided by these free live streaming websites, according to research conducted in 2016, plant malicious software on users' machines through forced malicious ads and other deceptive techniques. The research also noted an increase in sites requiring the users to install browser plug-ins to watch the free steam, this software also allowed the hijacking or infection of normally safe websites that the user visits thereafter. For example, if a person installs an extension to watch a live stream of a sporting event and then visited government or news websites afterward the installed extension could change the contents of those websites as they appear in the user's web browser so that they include malicious links and advertising.[3]

---

[3] "Its Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services" https://zubairrafique.files.wordpress.com/2015/10/flis_ndss16.pdf , accessed on 8 August 2017

3.11 This clearly indicates that the cost and issue of free live streaming goes beyond the ability of copyright legislation to deal with. In fact, as the streaming is live and no download takes place to the hard drive of the user, in most cases the court would deem that no distribution of copies of works took place. Another aspect to consider is that as the main factor of a sport event is that as it is 'live' the damage is suffered immediately upon the illegal streaming commencing and current takedown processes in the Electronic Communications and Transactions Act, 2002 ("the ECT Act") do not address this harm as they do not offer immediate relief from damage.

4. Electronic Communications and Transactions Act

4.1 We note that the Bill proposes to delete the cybercrimes provisions in the ECT Act, including sections 85, 86, 87, 88 and 90.

4.2 The cybercrime provisions in the ECT Act played a key role in the prosecution of cybercrime, including piracy of broadcasting services. The prosecuting authority has in the past successfully prosecuted pay TV pirates in terms of section 86 of the ECT Act. This section has been particularly useful in preventing the distribution of Internet TV boxes that facilitate piracy.[4] The current focus of the Bill on computer networks appears to be narrower than the sections being repealed in the ECT Act, which allow prosecution of a "person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item…" Therefore, subscription broadcasters and rights holders are

[4] https://mybroadband.co.za/news/internet/161750-multichoice-and-safact-nail-pirate-tv-box-seller-in-south-africa.html , accessed on 8 August 2017

concerned that they will lose some of the protections currently afforded them under the ECT Act.

4.3 This loss of protection is also happening at a time when digital technology has fundamentally changed the way in which content is created, manipulated and shared. Although digital technology has allowed broadcasting to evolve to the next level, it has also simplified the practice of broadcast signal piracy. Advancements in content protection and the development of new technologies and services available have caused most piracy to shift to the Internet. A pirate can now capture a broadcast signal with a simple tuner card or the station's signal streamed on line using a home personal computer or laptop. The pirate can then stream that broadcaster's signal on his or her own "channel," using one of the popular websites that enable live streaming of what is supposed to be user-generated content. These unauthorized live streams are then aggregated and distributed to a much larger global audience by websites that link to or embed them.

4.4 Some of the larger aggregation websites provide directories of the pirated signals. Sites that host and aggregate pirate broadcast signals can generate significant revenue by selling banner ads, pop-up ads, and pre-roll ads that appear before those streams, which are often placed by automated systems without regard to their legality. A local example of such piracy is that South Africa benefited from the World Cup in 2010, but so did online pirates. International research showed that during the World Cup in South Africa there were a total of 16,426 streams on 17 sites with pirated content.[5] Piracy is a growing problem in South Africa as broadband penetration increases. In 2016, when the first episode of Season 6 of Game of Thrones TV series aired in the United States, South Africa made the top

[5] NetResult. **Update on Digital Piracy of Sporting Events 2011**. Accessed: 8 August 2017. http://www.wipo.int/export/sites/www/ip-sport/en/pdf/piracy_report_2011.pdf

10 list of pirate downloaders globally for downloads within 12 hours of the episode being broadcast for the first time.[6]

Intermediary Liability

4.5 In South Africa, the ECT Act provides intermediaries with limited liability provided that they are a member of an industry representative body recognised by the Minister of Telecommunications and Postal Services (before the Presidential Proclamations in July and November 2014, this was the responsibility of the Minister of Communications), they conduct their operations as mere conduits without editorial control, they adhere to the industry representative body's code of conduct, and respond to court orders and take-down requests.[7]

4.6 This means that in terms of the ECT Act, a service provider is not liable for being a “mere conduit” of infringing information or data, or for the automatic caching of unlawful content. A service provider is also not liable for hosting unlawful content and for damages arising from data stored at the request of a user; Provided that the service provider did not have knowledge of the infringing activity or data, and that the data or activity relating to it infringes the rights of a third party. A service provider is also not liable for being an “information location tool” (providing links or references in an automatic manner) – like a search engine, or aggregator. When someone becomes aware of unlawful material or action taking place on the networks of intermediaries, they may notify the intermediary of the infringement and require it to remove or disable access to the unlawful material or activity.

4.7 The Copyright Review Commission of the Department of Trade and Industry in a report stated that the law of delict and copyright imposed liability for acts or omissions in a specific instance. So, an intermediary’s liability will also depend on the role it plays in a particular transaction. Where an Internet Service Provider (ISP) makes unauthorised

---

[6] http://www.channel24.co.za/TV/News/sa-in-top-10-pirate-list-of-game-of-thrones-20160510

[7] Chapter XI of the ECT Act

reproductions of a protected work (for example, for technical reasons such as caching) it may be liable for direct infringement of copyright. But where it merely transmits or facilitates access to copyright infringing material, it may be liable for 'contributory infringement' at common law." However, "the principle of 'contributory infringement' has not been established in any reported decision on South African copyright law.

No obligation to block infringing content

4.8 A flaw in the current law is that the ECT Act requires intermediaries to take down content on their servers when valid take-down requests are received, but it does not impose an obligation on them to block content on websites (local or international) that collect, index and host torrents to pirated movies and TV series or streaming websites.

4.9 Essentially, this means that South African law has failed to keep apace of rapid technological change on the Internet leaving gaps in the law that can be exploited to prevent prosecution. South Africa's copyright law requires a reproduction to have been made for violation to have occurred. In the case of steaming video where no content is physically stored on the hard drive and content is loaded directly to RAM and played from there in a buffered stream no reproduction or copy is made, making it difficult to enforce the rights of the copyright holder.

4.10 It could be argued that Virtual Private Network (VPN) service providers and suppliers of tunnelling software could be held liable for 'contributory infringement' for facilitating access to copyright infringing material, but once again in the context of streaming video, where there is no physical download to the end-users receiving device, it may prove difficult to demonstrate copyright infringement. This has resulted not only in the active provision or supply of technical methods to circumvent geo-blocking[8], but also the rise of companies who offer these services for a

[8] *Geo-blocking* is a form of technological protection measure where access to Internet content is restricted based upon the user's geographical location. https://en.wikipedia.org/wiki/Geo-blocking

fee. In South Africa, Global SA[9] has been operating since August 2013 offering Netflix and HULU packages which their website clearly indicates is "streamed straight out of the US to your home, office or wherever you are online".

4.11 There is dire need for legislation that would impose requirements on ISPs to co-operate with rights-holders and government to police illegal file-sharing or streaming websites and to issues warnings to end-users identified as engaging in illegal file-sharing. This is an aspect that is not currently covered in the ECT Act, or copyright law, and we believe it needs to be addressed in the Cybercrime and Cybersecurity Bill.

Flaws in takedown process

4.12 The ECT Act is also flawed in that s77 fails to address specific issues that may require immediate action, such as live streaming of a live sport event. The ECT Act, at s77, currently provides that a takedown notification must be in writing and must be addressed to the service provider and must include-

4.12.1 the full name and address of complainant;

4.12.2 written or electronic signature of complainant;

4.12.3 identification of the right that has allegedly been infringed;

4.12.4 identification of the material or activity that is claimed to be the subject of unlawful activity;

4.12.5 the remedial action required to be taken by the service provider in respect of the complaint;

4.12.6 telephonic and electronic contact details of the complainant;

4.12.7 a statement that the complainant is acting in good faith; and

[9] http://www.globalsa.co.za/onDemandTV.php

4.12.8 a statement by the complainant that the information in the take down notification is to his or her knowledge true and correct.

4.13 However, the ECT Act does not set time limits within which the intermediaries must take down or block access to illegal content or information. In practice, it can take anywhere from 24 hours to 3 days or even weeks before infringing content is taken down or deleted. As the window for live events is usually much shorter than 24 hours it is clear that the ECT Act takedown process cannot be the sole process available to deal with cyber piracy or cybersecurity issues.

4.14 It is proposed that the Bill should set out more specific notice-and-takedown laws either in the Bill or through the Schedule of the Bill amend the ECT Act to address specific conduct where immediate action is required, for example child pornography, terrorism related information and live streaming of sporting events all of which clearly require a faster more immediate process to reduce harm.

5. Proposal on Cyber Piracy Provisions

5.1 Piracy is ever evolving, and thus new approaches are required to fight illegal content distribution. As discussed above, the provisions of the ECT Act played a key role in addressing issues of cyber piracy, including as regards broadcast signal piracy. Given that the Bill is seeking to replace these provisions of the ECT Act, the provisions in the Bill ought to be strengthened to ensure that broadcasters and electronic communication service providers continue to have, and surpass, the protections currently afforded by the ECT Act.

Broaden focus to include all electronic communication networks

5.2 The current focus of the Bill on computer networks appears to be narrower than the sections being repealed in the ECT Act to the detriment of broadcasters, it should be kept in mind that data and the transfer of data is

not restricted to only computer networks. To protect data from interception and the circumvention of technological protection measures, the Bill should also apply to 'electronic communication networks' as defined in the Electronic Communications Act, 2005. In our view this would provide legal remedies to make illegal the circumvention of geo-blocking or technology protection measures employed by broadcasters and over-the-top video on demand (OTT VOD) services to protect their broadcast signal and content.

5.3 Accordingly, we proposed the following amendments to sections of the Bill to deal with this issue and the inclusion of 'electronic communications network' as follows:

5.3.1 We propose the insertion of a definition of “electronic communications network” in section 1 of the Bill as follows:

> “electronic communications network” means an electronic communications network as defined in the Electronic Communications Act, Act 36 of 2005.”

5.3.2 We further propose the insertion of “electronic communications network” as sub-paragraph (e) in section 2(1) of the Bill to deal with content and data piracy of broadcasting and electronic communication services as follows:

> “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; or
>
> (e) an electronic communications network.”

5.3.3 To deal with cyber piracy which involves display or viewing of the broadcast signal and TV programming, we propose that access to data including viewing or displaying of data and that section 2(2)(a)(i) be amended to read as follows:

"(i) view, display, alter, modify or delete data;"

5.3.4 We propose the insertion of sub-paragraph (e) in section 2(2) of the Bill to explain what constitutes a person securing access to an "electronic communications network" as follows:

"2.(2) For the purposes of this section a person secures access to-

(a) data when the person…

(e) an electronic communications network when the person is in the position to-

(i) sell, offer for download, distribute, retransmit, store on a computer data storage medium or otherwise make available content or data transmitted through an electronic communications network

and the access contemplated in paragraph (a), (b), (c), **[or]** (d), or (e) which the person secures is unauthorised."

5.3.5 We propose the insertion of "electronic communications network" in section 2(3) of the Bill as follows:

"2.(3) For the purposes of subsection (2), "unauthorised" means that the person-

(a) …

(b) …

(c) …

to data, a computer program, a computer data storage medium, **[or]** a computer system or an electronic communications network."

5.3.6 We propose the insertion of "electronic communications network" in section 3(1)(b) as follows:

"(1) Any person who unlawfully and intentionally –

(a) overcomes any protection measure which is intended to prevent access to data; and

(b) acquires data, within or which is transmitted to or from a computer system or an electronic communications network, is guilty of an offence."

5.3.7 We propose the insertion of section 10A after section 10 in the Bill as follows:

"**Cyber Piracy**

10A Any person who unlawfully and intentionally commits any offence contemplated in sections 2(1), 3, 4(1), 5(1), 6(1) and 7, for the purpose of-

(a) infringing copyright in a work, or

(b) facilitating the infringement of copyright in a work by a third party, including by way of online locations and file sharing sites

is guilty of the offence of cyber piracy."

Advertisers who support illegal conduct

5.4 We propose that the Bill also deal with advertisers who directly fund illegal streaming data websites by advertising their goods and services on them, as well as other conduct which is an offence in terms of the Bill. This conduct can only be prevented making such conduct an offence.

5.5 We propose the insertion of a new section 7A after section 7 in the Bill as follows:

> "7A Any person who funds a website, computer network or an electronic communications network, including by purchasing of a product or service from or by advertising on that website or network, in circumstances where that person knows or ought reasonably to know that the website or network is used in the commission of conduct which constitutes an offence in terms of section 2(1), 3(1), 5(1), 6(1) or 7(1)(a) or (d), is guilty of an offence.

Takedown provisions and blocking

5.6 As mentioned in paragraph 4.11 above, the Bill can play a role in dealing with the damage that piracy has on local content industries and the economic contribution of sport events by putting in place necessary safeguards such as imposing requirements on ISPs to co-operate with government, law enforcement and rights-holders to block illegal streaming websites. A very recent UK High Court decision in July 2017 allowed the English Soccer's Premier League to pre-emptively require that ISPs in the United Kingdom (UK) block servers that are hosting illegal streams of its matches. The order was put in place for the entirety of the 2017-18 Premier League season which commences on 11 August 2017. A similar order was obtained for the final two months of the 2016-17 season allowing more than 5,000 server Internet Protocol (IP) addresses to be blocked that previously were streaming illegal Premier League content. In doing so the English Premier League is protecting the rights it sold to Sky and BT for more than £5bn to show live matches over three seasons. [10]

5.7 Accordingly, it is proposed that in order to allow pre-emptive blocking of servers hosting illegal streams prior to a live event the owners of the

[10] http://www.telegraph.co.uk/technology/2017/07/27/premier-league-lands-game-changing-court-order-war-illegal-streaming/

exclusive copyright may apply to the High Court for an injunction. We propose the insertion of a new section 19A after section 19 in the Bill as follows as follows:

"**Order against electronic communications service provider providing access to online location**

19A The High Court may, upon application by any person who has reasonable grounds to believe that copyright is being or may be infringed by any person situated inside or outside the Republic, grant any relief, including urgent relief, which it deems appropriate, including granting an order requiring –

(a) any person who enables or facilitates the infringement of copyright, or whose service is used by any other person to infringe copyright, to cease such enabling or facilitating activity or disable that person's access to its service for the infringing purpose;

(b) any person who hosts or provides an online location, service or facility situated inside or outside the Republic which is used by any person to infringe copyright or which enables or facilitates the infringement of copyright, to disable access to such online location, service or facility as replaced, amended or moved from time to time; or

(c) any service provider, as that term is defined in section 70 of the Electronic Communications and Transactions Act, 25 of 2002,[11] to prevent or impede the use of its service by any person in order to access an online location, service or facility situated inside or

[11] "Service provider" is defined in s70 of the ECT Act as meaning "any person providing information system services". "Information system services" is defined in s1 of the ECT Act as "includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service"

outside the Republic, as replaced, amended or moved from time to time, which is used to infringe copyright."

5.8 The implementation of the High Court Order in the UK was made possible by video monitoring technologies used by the Football Association Premier League and advances in the ISPs' blocking systems, which enable the blocking and unblocking of IP addresses during the course of a match, in some cases using automated technology systems.

5.9 It is counter-intuitive that one must go to court to order ISPs to block IP addresses that are currently infringing content by live streaming or providing access to terrorist information or malicious software or that facilitate cyber-extortion when in fact ISPs are already able to use blocking systems and can easily acquire systems that automate such a process. The protection of live content requires the takedown of the infringing content as rapidly as possible.

5.10 It is therefore proposed that the Bill require South African ISPs to put in place an online tool (such as a web form) that will automate the removal of content at a location specified in a notice filed on an urgent basis by a content rights owner or the South African Police Service. YouTube's Content ID system provides a model that allows verified copyright owners to remove material, rather than rely solely on YouTube to do so. Such a system would allow for fast-tracked processing of a takedown notice made under s77 of the ECT Act and/or the provisions of the Bill.

5.11 We propose the insertion of a new section 52A after section 52 in the Bill as follows:

"52A (1) An electronic communications service provider that provides information system services, as defined in section 70 of the Electronic Communications and Transactions Act, 25 of 2002, must implement automated takedown forms that allow-

(a) verified owners of exclusive copyrights the ability to remove infringing live streaming data immediately; or

(b) specifically designated police officials the ability to remove terrorist information or content that facilitates or incites cybercrime.

(2) The online automated takedown form must include, in addition to the Internet Protocol address of the allegedly infringing live streaming data, fields for the required information in s77 of the Electronic Communications and Transactions Act, 25 of 2002."

6. Unintended Consequences

6.1 There are several provisions in the Bill which are so broad that they may potentially criminalise ordinary use. These include section 2: Unlawful securing of access, section 3: Unlawful acquiring of data, and section 4: Unlawful acts in respect of software or hardware tool, which are very broad. Many of the activities described in these sections are performed daily by ordinary users. The Bill does not define what makes the conduct described in these sections "unlawful". As currently worded, software used for advertising, marketing purposes and for conducting research and analyses, may be unlawful. Similarly, there may be unintended consequences for the IT security industry due to the high potential for offences to be committed during every day investigations carried out to determine the level of security or otherwise of a client's system. Activities such as penetration testing and ethical attacks without authority will technically offend the provisions despite the intention behind them. For example, section 4 which is designed to catch people in possession of technology to be used for hacking activities, fails to recognise that similar or identical tools may be used for legitimate security purposes. Thus, even where there is no malicious intent and no harm done, ordinary Internet users may be committing a crime.

6.2 We propose that the unlawful access of data, etc. should be linked to an intention to commit a serious offence. An example of this approach is contained in the Australian Cybercrime Act, 2001, which provides:

"A person is guilty of an offence if –

(a) the person causes any unauthorised access to data;

(b) the unauthorised access is caused by means of a telecommunications service;

(c) the person knows the access is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence … by the access."

In our view, "serious offence" ought to be defined as "an offence that is punishable by imprisonment for five or more years".

7. Concluding Remarks

7.1 Once again M-Net and MultiChoice would like to thank the Committee for this opportunity to comment on the Bill, and we would like to indicate our interest in making oral representations on the Bill at the Public Hearings to be held at Parliament.