21 July 2017

Mr V Ramaano
The Department of Justice and Constitutional Development
Private Bag X81
Pretoria
0001

Per email: vramaano@parliament.gov.za

Dear Mr Ramaano

RE: INTERNET SOLUTIONS SUBMISSION ON THE DRAFT CYBERCRIMES AND CYBERSECURITY BILL

Please find the attached submission from Internet Solutions in respect of the Draft Cybercrimes and Cybersecurity Bill, 2017.

Please do not hesitate to contact the writer hereof should you have any questions.

Yours sincerely,

PP

Adv. Mongezi Tshongweni
Regulatory Executive
Tel: +2711 575 6561
Fax: +2711 576 6561
Mobile: +2783 676 2135

1. INTRODUCTION

Internet Solutions thanks the Department of Justice and Constitutional Development (the Department) for the opportunity to make its written submission on the Draft Cybercrimes and Cybersecurity Bill ("the draft Cybercrimes Bill").

Internet Solutions, a division of Dimension Data, specialises in the provision of information technology and electronic communications related services. Internet Solutions is the leading South African communications service provider, which strives to offer a superior client service experience for client and partner organisations.

2. MAIN CONCERNS ON THE DRAFT CYBERCRIMES BILL

Internet Solutions submitted in 2015 its comments in respect of the first draft Cybercrimes Bill wherein we sought the Department to address the following: definitions (electronic communications service providers, national critical information infrastructures, cybercrime and cybersecurity); the criminalization of copyright infringement (section 20); electronic communications service providers obligations (section 64); penalties (personal information and financial information related offences- section 3); copyright infringement related penalties (section 20(2)); and jurisdiction (section 25). Internet Solutions commends the Department for addressing some of the definitions and uncertainties in the current draft Cybercrimes Bill.

While the current draft Cybercrimes Bill deals with a variety of topics relating to cybercrime and cybersecurity challenges, IS intends in its submission to only deal with certain topics which remain unaddressed by the current Cybercrimes Bill.

2.1 Cybercrimes

2.1.1 Unlawful Securing of Access: Section 2

The definition of cybercrimes in section 2(1)-(3) as provided in the draft Cybercrimes Bill is extremely broad as it attempts to criminalise every unlawful electronic access as a cybercrime. As such, it should be relooked. Firstly, the reference to "unlawful securing of access" is extremely confusing as it entails that an object (data, computer program, a computer, data storage medium or a computer system) has been unlawful accessed with the intention of safeguarding/protecting it. It should rather read "unlawful access or unauthorised access" as compared to "unlawful securing of access."

Second, in attempting to define cybercrime, the "unlawful securing of access" in itself is broadly defined to criminalise a mere wrongful conduct into a cybercrime. The entire

definition of “unlawful securing of access” in section 2(2)-(3) lacks the essential cyber ingredients, which are instrumental in the technically commission of a cybercrime. As such, the entire definition is a generalisation of the non-essential ingredients. While it is important to protect citizens against violation of their cyber interests, a mere unauthorised access to an object (data, computer program, a computer, data storage medium or a computer system) amounts to over criminalization of an unauthorised conduct as a cybercrime.

This is premise on the fact that an act of “altering, modifying, deleting, copying, relocating, accessing, storing, instructing, using or communicating with an object, such as data, computer program, storage medium or computer system, does not necessarily entail damage to an object. The draft Cybercrimes Bill does not link the conduct of unlawful access with any harm or damage, which may result in impairment or abnormal functioning of data, computer program, storage medium or computer system. As such, the means are devoid of the end.

In our view, unauthorised access should contain the necessary intent to cause serious harm or damage to a particular cyber-interest. Section 2(2)-(3) is problematic on the basis that the offence is committed even in the absence of serious damage. Further, Internet Solutions is also concerned that section 2(2)-(3) does not specify whether or not the unlawful securing of access as an unauthorised conduct is temporal or permanent. As such, the criminalisation of a mere unauthorised conduct without linking such unauthorised conduct with malicious intent to cause serious harm or damage is inadequate and it may result in prosecution of individuals for trivial alterations or modifications.

Internet Solutions is strongly of the view that the criminalisation of an unauthorised conduct has to be cyber-specific and it should include an infringement of security measures to obtain computer data, such as circumventing password protection on a computer system. This is also premise on the fact that random tests without any authorisation from assigned users are conducted periodically by concerned businesses to guarantee data security and protect their cyber interests. The definition of unlawful securing of access criminalises, such random periodic security checks, which are effected for security reasons as a cybercrime.

Internet Solutions recommends that section 2 be deleted entirely given that unauthorised access is criminalised under sections 3(1), 4(2), 5 and 6, including other substantive offences, which may be committed by means of such unauthorised access with a view of circumventing security measures.

2.1.2 Unlawful Acquiring of Data: Section 3

Internet Solutions is of the view that section 3 (2)-(3) criminalises anyone who knowingly, unlawfully and intentionally possesses data which was acquired unlawfully. Internet Solutions notes that it is imperative that the government takes the necessary measures to protect sensitive information stored in computer systems considering the value of sensitive information. However, the manner in which this section is drafted fails to provide for public interest defences. As such, it could be interpreted to amount to an unjustified restriction and violation of the right of access to information as guaranteed by section 32 of the Bill of Rights, 1996 in that it does not include any protection for journalists and whistle-blowers.

Section 3 (2)-(3) is a restriction on the right of access to information on the basis that not all content, which is published in the public interest is acquired lawfully. As such, section 3 (2)-(3) is drafted in a manner that inadvertently restricts the role of the media and its contribution to the development of a democratic state by seeking to guarantee lawfulness by restricting a conduct altogether. The criminalisation of this offence fails to take into consideration public interest defences in instances where unauthorised access to data, computer programs, data storage mediums or computer systems may arise for legitimate purposes, such as investigative journalism.

Freedom of expression is vital as a necessary platform which sustains a healthy democracy, and guarantees free flow of opinions and ideas, which enable all citizens to participate in their systems of governance. It is for this reason that the government ought to provide special protection to the media in order to safeguard genuine investigative journalism and to enable the media to put in the open that which may have been concealed. It is on these basis that we strongly view the draft Cybercrimes Bill as having failed to promote the protection of freedom of expression.

The Constitutional Court in *Print Media South Africa and Another v Minister of Home Affairs and Another,* held that "the mainstay of the law is to encourage lawful conduct rather than to seek to guarantee lawfulness by restricting conduct altogether."[1] The Constitutional Court further noted that the law which guarantees lawfulness by restricting a conduct altogether "unjustifiably limits the right to freedom of expression."[2] As such, section 3 (2)-(3) has a negative impact on the right of freedom of expression. In as much as freedom of expression is not absolute in South Africa, measures encroaching upon this right should be reasonable

[1] *Print Media South Africa and Another v Minister of Home Affairs and Another* 2012 (6) SA 443 (CC).
[2] *Ibid.*

and justifiable in an open and democratic society in terms of section 36 of the Bill of Rights. Therefore, we are concerned that section 3(2)-(2) will not pass constitutional scrutiny.

Needless to say that South Africa is inundated with a myriad of court cases wherein the media was taken to court for publishing content, which was acquired unlawfully. Internet Solutions would like to particularly reflect on *SAA v BDFM Publishers and Others,* in which a confidential advisory opinion was leaked to Business Daily, Moneyweb and Media24 by unauthorised means.[3] Notwithstanding SAA's claim of a violation of their right to confidentiality, Business Daily, Moneyweb and Media24 sought to publish the advisory opinion as it was in the public interest to do so. The High Court duly held that it was not in the public interest to suppress the dissemination of information to protect SAA's right to confidentiality, which had already been lost when the advisory opinion was leaked, and which could not be remedied by a court interdict.[4] The court further held that the public interest in informing citizens on how SAA was spending tax revenue as a public company and an organ of state, outweighed SAA's right to confidentiality. [5]

Another relevant and interesting case is *Tshabalala-Msimang v Makhanya,* which dealt with the theft of Tshabalala-Msimang's private and confidential medical records, which were leaked to the media. The private and confidential medical records were acquired illegally. However, it is interesting to note that the court refused to grant an interdict against their dissemination on the basis that they had already been leaked to the media and it was in the public interest to publish them.[6]

Based on the South African jurisprudence, it is clear that our courts have fostered constitutional and societal values, such as transparency, accountability, responsiveness and openness by promoting the dissemination of information irrespective of the manner in which it was acquired. The litmus test used by the court was whether or not the dissemination was in the public interest. In short, South African courts promote investigative journalism in the public interest as compared to weighing the manner in which data was acquired.

Internet Solutions also notes with interest that section 3(3) imposes the burden of proof on the right bearer who seeks to vindicate his right, whereas the onus should be on the state as the party seeking to restrain the expression of its citizens.

---

[3] *SAA v BDMF Publishers (Pty) Ltd and Others* 2016 (2) SA 561 (GJ).
[4] *Ibid, para. 49.*
[5] *Ibid, para. 63..*
[6] *Tshabalala-Msimang v Makhanya & Others 2008 (6) SA (W).*

We therefore recommend that section 3(2)-(3) be revised to safeguard unlawfully and intentionally acquired data in the public interest on the basis that unlawfully acquired data may have social value. The public interest served by an unlawful conduct should be weighed against the degree of criminality, which is the extent of the means employed through investigative journalism to justify the end as compared to absolute criminalization of the conduct concerned.

2.1.3 Unlawful Acts in Respect of Software or Hardware Tool: Section 4

Section 4(1) criminalises unlawful acts in respect of software or hardware tool, and it is defined by the draft Cybercrimes Bill as unlawful and intentional possession, manufacturing, assembling, obtaining, selling, purchasing, advertising or making available any software or hardware tool for purposes of contravening the provisions of sections 2(1), 3(1), 5(1), 6(1) or 7(1) (a) or (d).

Section 4(2) criminalises anyone who unlawfully and intentionally uses any software or hardware tool for purposes of contravening sections 2(1), 3(1), 5(1), 6(1) or 7(1) (a) or (d). Section 4(3) defines “software or hardware tool’’ as “any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component of such a device or a computer program, which is designed or adapted primarily for the purposes of securing access, acquiring data, interfering with data or a computer program, data storage medium or a computer system or acquiring, modifying, providing, making available, copying, using or cloning a password, access code or similar data or devices.”

Internet Solutions is concerned with the manner in which section 4(1) and (3) are drafted on the basis that they are defined too broadly in terms of their scope, influence, and impact, and as such, needs to be relooked. The scope of section 4(1) is broad in that it assumes that possession, manufacturing, assembling, obtaining, selling, purchasing or advertising of any software or hardware tool is a criminal activity and not the actual use of the tool or software.

Internet Solutions is strongly opposed to criminalizing these acts as unlawful. In our view, the Cybercrimes Bill should rather criminalize a conduct committed with a software or hardware tool, and not its mere possession, manufacturing, assembling, obtaining, selling, purchasing or advertising. In simple terms, the mere fact that knives are commonly used as tools to commit grievous crimes does not justify criminalising their possession, manufacturing, assembling, obtaining, selling, purchasing or advertising. As dangerous as knives are, it would be absurd to do so as possession, manufacturing, assembling, obtaining, selling, purchasing or advertising knives should not in itself be criminalised.

In as much as section 4(3) attempts to validate section 4(1) in that the software or hardware tool in question ought to be primarily designed or adapted for the purposes of committing a cybercrime, Internet Solutions is concerned by such generalisation considering that a laptop which is a hardware tool can be adapted to commit crimes listed in sections 2(1), 3(1), 5(1), 6(1) or 7(1)(a) or (d). Linux.Wifatch, a form of malware, which was primarily designed to treat and prevent security threats against unsecured Wi-Fi routers could still be used primarily to commit cybercrimes. In essence, a tool which is primarily designed for one specific purpose, can be adapted to commit a crime. The cyber world should not be considered as an exception.

To avoid any unintended overlap, Internet Solutions humbly suggests that section 4(1) and (3) be deleted entirely since sections 5 and 6 deal specifically with interference, which creates a relationship between cause and effect in cyber criminality.

2.1.4 Unlawful Interference with Data or Computer Program: Section 5

Section 5 criminalises the unlawful interference with data or computer program, which is defined as permanent or temporal deletion, alteration, damage or deterioration or rendering data or a computer program meaningless, useless or ineffective; obstruction, interruption or interference with the lawful use of data or a computer program; or denial access to data or a computer program.

Internet Solutions recommends that section 5 should include an intent to cause harm.

2.1.5 Unlawful Interference with Computer Data Storage Medium or Computer System: Section 6

Section 6 criminalises the unlawful interference with data storage medium or computer systems, which is defined as “permanent or temporal alteration, interruption or impairment of the functioning, confidentiality, integrity, or the availability of a computer data storage medium or a computer system.”

Internet Solutions admits that computer systems are vital, and that malware attacks against computer systems can result in massive financial losses. However, it is recommended that unlawful interference with data storage medium or computer systems should cause serious impairment to its functioning, such as malware which is designed to damage, interfere, steal, delete data, hosts, or networks, and can also enable cyber criminals to install back-doors to circumvent security protections and remotely take possession of data or computer programs. As such, Internet Solutions recommends that section 5 be relooked.

2.1.6 Malicious Communications: Section 16 and 17

Internet Solutions is of the view that the criminalisation of speech relating to data messages in any legislation should be restricted to instances where intentional incitement or a direct call to cause damage to property or violence is apparent. To the extent that the government may wish to prohibit incitement to cause damage to property or violence, Internet Solutions is of the view that such offences should not form part of the draft Cybercrimes Bill as they are hate speech and common law offences. Notwithstanding that computer systems or networks can be used as a tool in the commission of hate speech and common law offences, the offences in question are not carried out specifically against data or computer systems.

Criminalisation of malicious communications distributed by means of a computer system amounts to online behaviour, which can also be effectively committed offline. It is common cause that with rapid technological advancement, there has been a growing trend in cyber related murders. However, this would not necessarily require the government to criminalise murder committed by means of a computer system as a cybercrime merely on the grounds that a computer system was used as a tool. Similarly, “malicious communications” in a broader sense could be considered a cybercrime. However, cybercrime in its narrow sense should be defined as any unlawful electronic behaviour committed by means of computer system, which violates the security of computer systems and processed data as already stated above on page 3. Narrowly defined, cybercrimes should only refer to offences committed by means of computer systems against data or computer systems as crime targets.

Needless to say that malicious communications distributed by means of a computer system could successfully be prosecuted under the Hate Speech Bill and applicable general criminal law. The scope of regulation should, therefore, be limited to areas, which are clearly a priority to enforce, and which can virtually be addressed with clear and desirable outcomes. As such, Internet Solutions is of the view that section 16 and 17 should not form part of the Cybercrimes Bill to avoid duplication as such provisions are more appropriate for the Hate Speech Bill.

2.1.7 Electronic Communications Service Providers Obligations: Section 52

Internet Solutions notes that electronic communications service provider obligations have been fairly amended in section 52(1). Section 52(1) of the draft Cybercrimes Bill requires the electronic communications service provider or financial institution to report any illegal activity to the South African Police Service as soon as it is “aware or become aware that its

computer network or electronic communications network is being used to commit an offence" provided for in Chapter 2.

In as much as electronic communications service providers and financial institutions are required to report cyber offences, where feasible and within 72 hours of becoming aware of the offence, this obligation is unreasonable considering that the draft Cybercrimes Bill does not define at what stage the electronic communications service provider or financial institution should be deemed as "being aware". Electronic communications service providers receive a number of complaints on a daily basis alleging that offences have been committed on their networks. An allegation does not determine whether or not an offence has indeed been committed.

For instance, in the case of an electronic communications service provider like Internet Solutions, is "being aware" a stage when our Abuse Desk has been notified of an illegal activity? If so, what about electronic communications service providers who do not have an Abuse Desk facility or any means of being constantly made aware of illegal activities? This raises another concern that there are no structures or regulatory bodies tasked with keeping the electronic communications service providers and financial institutions constantly aware of such illegal activities.

This also means that electronic communications service providers and financial institutions are required to police the internet and keep an inventory of all suspected activity. Further, the obligation requires electronic communications service providers and financial institutions to have the institutional and logistical capacity to detect and control all data stored in their servers.

Internet Solutions is of the view that electronic communications service providers and financial institutions should only be required to take down content following a takedown notification or a court order. As such, there should still be clarity with regard to when reporting in terms of section 52(1) must be done.

In terms of section 52(4), electronic communications service providers and financial institutions are not required to intercept or monitor data stored in their servers. They are also not required to actively seek facts or circumstances indicating any unlawful activity. It is extremely confusing as to how electronic communications service providers and financial institutions are required to achieve the intended obligation imposed in section 52 (1) without intercepting or monitoring the internet in respect of section 52(4).

Internet Solutions recommends that section 52 (1) be relooked as it is contradictory to section 52(4). Further, electronic communications service providers and financial institutions should only be required to take down content following a takedown notification or a court order as already stated above.

2.2 Critical Information Infrastructure: Section 57

Internet Solutions notes that the definition of **national critical information infrastructure** which was included in the 2015 version has now been removed, and replaced with **critical information infrastructure**. We also note that the current draft Cybercrimes Bill does not define critical information infrastructure, whereas the 2015 draft Cybercrimes Bill defined national critical information infrastructure too broadly to include "any computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof."

Not unless a definition is provided or an entity is identified and subsequently declared as a national critical information infrastructure according in terms of section 57(2) of the draft Cybercrimes Bill; the draft Cybercrimes Bill in its current form gives the Cabinet mandate for any entity, including Internet Solutions, to be declared a national critical information infrastructure. In terms of section 57 (2), the government has the mandate to declare any infrastructure as a critical information infrastructure, irrespective of the fact that the State Security Agency is required to declare such infrastructure in consultation with the Cyber Response Committee and the owner or the person in control of such information infrastructure. Internet Solutions is of the view that any information infrastructure which is declared critical by the State Security Agency should only be the infrastructure without which the state could not function.

We also note with concern the negative implications of section 57 (4) (a)-(g), which are far-reaching and could have a number of unintended consequences for any entity, which is declared a critical information infrastructure. Section 57 (4) (a)-(g) confers on government far-reaching powers to issue directives prescribing the manner in which data held by a critical information infrastructure ought to be classified, protected, stored and archived, including cybersecurity incident management, disaster contingency and recovery measures, physical and technical security measures, the period within which the owner ought to comply with directives; and any other relevant matter which is necessary or expedient to promote cybersecurity.

While we recognize that a critical information infrastructure is vital for a state's economic security, sustainability and stability, and that it could become susceptible to cyber-attacks, which could cause huge financial loss and damage, we are also of the view that the government's approach to preventing cyber-attacks against critical information infrastructure should not be far-reaching and overly obstructive.

In terms of section 57 (8), the owner of a critical information infrastructure is required to take steps to comply with government directives at their own cost to the satisfaction of the government. Further, in terms of section 57 (10), failure to comply with a government directive is criminalised, and is punishable by a fine or imprisonment for a period not exceeding two years or both a fine and imprisonment. In instances where the owner of a critical information infrastructure fails or refuses to comply, the government, in terms of section 57 (11), may take steps to comply with the directive, and may recover costs of compliance from the owner on whose behalf compliance measures were taken, irrespective of whether or not the owner has been charged or convicted of the offence in terms of section 57 (10).

It is on this premise that Internet Solutions is seriously concerned with the manner in which section 57 is drafted, particularly obligations imposed on owners or persons in control of any critical information infrastructure in that electronic communications services providers could be held criminally liable for failing to implement such directives, which could possibly be considered non-executable on a practical level.

Furthermore, the draft Cybercrimes Bill criminalises the violation of directives, which are yet to be defined. It is our view that the government has exceeded its constitutionally conferred powers by criminalising the conduct of owners of information infrastructure for the violation of directives, which are yet to be well ascertained, and which may likely be unreasonable or restrictive. In our view, section 57 is overly ambitious and too cumbersome, and ought to be properly redrafted.

2.3 Regulatory Overlap

There is an overlap between the draft Cybercrimes Bill and the POPIA in terms of citizens' rights to privacy and national security (interception of personal information). This is a reality which poses a serious challenge for privacy and cybersecurity.

Internet Solutions is of the view that there is an urgency to commence the enforcement of POPIA's remaining provisions considering that the POPIA sections, which have commenced are insignificant to protect data subjects. Sections of POPIA which prescribe compliance

requirements on the part of data handlers to implement appropriate technical and organizational measures to process personal information securely to prevent data breaches are yet to commence. Data protection laws are closely interlinked with cybercrime in terms of data security, data handling and the obligation to notify authorities and data subjects of security incidents. As such, Internet Solutions is of the view that privacy protections have to be enhanced to prevent cybersecurity threats as a matter of urgency.

3. CONCLUSION AND RECOMMENDATIONS

We note that the current draft Cybercrimes Bill has been improved in terms of drafting as compared to the 2015 version of the draft Cybercrimes Bill. However, as it stands, the draft Cybercrimes Bill may fail constitutional scrutiny. Internet Solutions strongly recommends that a number of provisions be relooked, including amongst others, the definition of cybercrime, (in particular the unlawful securing of access, unlawful acquiring of data, unlawful interference with data or computer program, and malicious communications), and the extremely onerous obligations imposed on critical information infrastructure.

In respect of unlawful securing of access, Internet Solutions recommends that section 2 (1)-(3) be deleted since the definition excludes an infringement of security measures to access computer systems or data. In respect of unlawfully and intentionally acquired data, Internet Solutions recommends that section 3 (2)-(3) be revised to safeguard unlawfully and intentionally acquired data in the public interest. In our view, the draft Cybercrimes Bill should promote a progressive and a revolutionary approach to the protection of freedom of expression, particularly investigative journalism.

Further, Internet Solutions is concerned that the draft Cybercrimes Bill unnecessarily addresses electronic activity which may be committed online and offline, such as incitement of violence and damage to property. In as much as these offences are committed in relation to information systems, they are beyond the cybercrime landscape. As such, Internet Solutions is of the view that the government should address such conduct by way of general provisions of the criminal law as compared to the cybercrimes legislation.

In respect to critical information infrastructure, Internet Solutions is concerned that the draft Cybercrimes Bill gives broad powers to the government to issue directives to critical information infrastructure owners, which prescribe the manner in which data ought to be classified, protected, stored and archived by critical information infrastructure owners. The directives may well result in restrictive and arbitrary interference. In our view, this is

detrimental to constitutionally guaranteed freedoms. The potential for misuse of government powers is extremely high, and such potential should be avoided.

Internet Solutions thanks the Department for the opportunity to make a submission on the draft Cybercrimes Bill. Internet Solutions would welcome the opportunity to make an oral presentation should public hearings be held.