SUMMARY OF WRITTEN SUBMISSIONS AND RESPONSES THERETO: CYBERCRIMES AND CYBERSECURITY BILL [B 6 - 2017]

PART A

(CHAPTERS 1 TO 9 OF BILL)

Introduction

The Portfolio Committee on Justice and Constitutional Development (the DOJ &CD) invited stakeholders and interested persons to make written submissions on the Cybercrimes and Cybersecurity Bill [Bill 6 - 2017] (hereinafter referred to as "the Bill"). Written submissions have been received from the following persons or entities:

1. MediaMonitoring Africa
2. South African Communications Forum
3. Legal Aid SA
4. Cell C, Telkom and Vodacom
5. Michalsons Attorneys
6. Right2Know
7. Mr Jamie Brand
8. ISPA
9. MTN
10. Banking Association South Africa
11. Prof Basie von Solms
12. Deloitte Risk Advisory
13. DFIRLABS: Mr Jason Jordaan

14. Ms Zoelpha Carr
15. Centre for Constitutional Rights
16. Bowline
17. Minister of Finance
18. ENGEN
19. Tourism Business Council of South Africa
20. Western Cape
21. All Rise Say No to Cyber Abuse
22. Information Governance Consultancy: Mr M Heyink
23. South African Human Rights Commission
24. Johannesburg Stock Exchange
25. Southern Africa Federation Against Copyright Theft
26. Internet Solutions
27. Strate (Pty)Ltd
28. Snail Attorneys
29. Mr G Eatwell
30. Liquid Telecom
31. IM Governance (Pty) Limited: Mr P Hill
32. Digital Law Company
33. IAB South Africa
34. Open Democracy Advice Centre

35. International Federation of Film Producers Associations
36. Credit Bureau Association
37. Electronic Media Network Proprietary Limited (M-Net) and MultiChoice Proprietary Limited (MultiChoice)
38. Information Regulator
39. Freedom of Religion South Africa
40. Steven Cohen

SUBMISSIONS/RECOMMENDATIONS BY CLAUSE

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
1. GENERAL COMMENTS ON BILL			

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			In general, most commentators are of the view that the Bill is necessary to address the current gap in the substantive and procedural laws of South African relating to cybercrimes.
	1.1 DFIRLABS - page 1 (paragraph 1.1); R2K - pages 17 and 18	1.1 Cybercrime is a growing concern. The Bill is a credible attempt to address cybercrime. However, for the Bill to be implemented successfully, the standard and availability of digital forensic practitioners need to be addressed.	1.1 In terms of the National Cybercrimes Policy Framework (the NCPF) and the Bill, provision is made for the development of the necessary capacity to implement the Bill. The NCPF, among others, provide for initiatives to strengthen capacity building (see paragraph 12). Clause 54 of the Bill imposes obligations on various Departments to establish and maintain sufficient human and operational capacity to give effect to their various mandates. The clause further provides that these departments must develop and implement, in cooperation with institutes of higher education and training, accredited training programs to give effect to their obligations in terms of the Bill. It must be pointed out that this situation is not unique to South Africa. Even developed countries face a similar shortcoming in capacity to deal with cybercrime. In

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			order to ensure that suitably qualified persons are involved in the investigation of cybercrimes, the Bill provides for the appointment of investigators to assist the South African Police in the investigation of cybercrimes (see clauses 27(3), 30(3) and 31(4)) and paragraph 6.2.4),
	1.2 ODAC - page 1; R2K - page 3	1.2 Cybercrimes are simply crimes committed with computers. The problem with the law is that it is outdated and plays catch-up with the new and ingenious ways people have of committing crimes. So, we need the Cybercrimes Bill in order to make sure we can use the law effectively to stop cybercrime. This is not only the responsibility of law enforcement and prosecutors. We all have a role to play in combating cybercrimes. Cyber legislation should protect us on three levels, namely- * protecting our personal data; * protecting our device; and * protecting the networks we use. Our rights to privacy, our right to freedom of expression and our right to access information must be protected. We should not be denied access to our own data by criminals holding our information hostage, or find our bank accounts emptied of their contents. The Bill describes the role for the police and prosecutors in keeping us safe, but also hands significant powers to the	1.2 The perception that the Bill hands significant powers to the Cabinet member responsible for State security is fallacious. In terms of section 2(2)(*b*) of the National Strategic Intelligence Act, 1994 (Act 39 of 1994), the State Security Agency (SSA) already has the mandate to identify, protect and secure critical electronic communications and infrastructure against unauthorised access or technical, electronic or any other related threats. Chapter 11 of the Bill (that deals with the protection of critical information infrastructure), which is in line with international developments, further gives effect to this mandate. Although the Cabinet member responsible for State security was given the task to implement the NCPF, no powers are afforded to the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		Minister for State Security, and we will need to ask to what extent that is needed to keep us safe, or to what extent it creates a risk. These aspects are dealt with further on in the summary.	SSA to control the Internet or to obtain access to information to which the SSA would not be entitled to. In terms of clause 53 of the Bill, the Cyber Response Committee (the CRC) is established. Although the CRC is chaired by Director-General: State Security, various other Departments with different constitutional mandates are represented on the CRC, among others, the Department of Justice and Constitutional Development (DOJ&CD), the National Prosecuting Authority (NPA) and the Department of Telecommunications and Postal Services (DTPS). Any decision by the CRC needs to be supported by a majority of representatives. Furthermore, South Africa is a constitutional democracy and decisions or actions which are unconstitutional can be challenged.
	1.3 MediaMonitoring: Africa - page 4	1.3 There is a lack of an overarching Internet governance policy on how current and proposed legislation (including the Bill) that deals with how information and digital rights (freedom of expression, access to information, and privacy) regulation is to be managed. It is suggested that an interdepartmental	1.3 It is submitted that the National Integrated ICT Policy of the DTPS caters for the concerns raised by the commentator. The CRC is an intergovernmental forum consisting of the heads of various Departments.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		steering committee be established or other structure within Government be established to bring harmony to the Internet governance framework and to ensure effective state response to cyber irregularities. This interdepartmental steering committee may be structured similar to the Cyber Response Committee	
	1.4 International Federation of Film Producers Associations; Steve Cohen; SAFACT - page 4; MNET - page 10 to 11 (paragraph 4.5 to 4.7), page 11 to 12 (paragraphs 4.8 to 4.11), (pages 12 to 13, paragraphs 4.12 to 4.14) and (pages 13 to 20, paragraph 5)	1.4 A balanced approach to address the massive copyright infringement on the Internet is necessary. It is proposed that measures should be introduced to enable local internet service providers to act against copyright infringements. It is suggested that South Africa should consider adopting technology-neutral "no fault" enforcement legislation that would enable intermediaries to take action against online infringements, in line with Article 8.3 of the EU Copyright Directive (2001/29/EC), which addresses copyright infringement through site blocking. 1.37 * Legislation is necessary that would impose requirements on Internet Service Providers (ISPs) to co-operate with rights-holders and Government to police illegal file-sharing or streaming websites and to issue 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 Bill. * Obligations should be imposed on ISPs to co-operate with rights-holders and Government to police illegal file-sharing or streaming websites and to issue warnings to	1.4 The Bill does not deal with copyright infringements. These aspects must be dealt with in terms of copyright-related legislation. The Copyright Amendment Bill [B13-2017] is currently before Parliament. The suggested amendments fall outside the scope and application of the Bill.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		end-users identified as engaging in illegal file-sharing and to block infringing content. * The take down process in section 77 of the ECTA is time consuming and ineffective and adversely affect copyright infringements. This should be remedied in the Bill or the ECTA should be amended in the Schedule to the Bill. * Amendments are proposed to sections 1, 2 and 3 of the Bill to deal with cyber piracy.	
	1.5 MTN – pages 3, 10 to 11 (paragraph 4)	1.5 The Bill is a welcomed initiative in order to address cybercrime. However, the cost of compliance and expertise in Government to effectively establish and administrate the various structures should be assessed. The powers of law enforcement in terms of the Bill to investigate cybercrime must be measured against the privacy rights provided for in POPIA.	1.5 * Capacity to implement the Bill is discussed under 1.1, above. * The Bill will have cost implications for Government and the private sector. The cost implications of the Bill need to be measured against the cost of cybercrime in the Republic and the cost of measures that is currently being implemented to address cybercrime, which is substantial. Cybercrime is escalating and measures need to be put in place to address this escalation. From a compliance perspective, the Bill does not require the private sector to put in place or implement costly measures to comply with the Bill. * The constitutional right to privacy is not meant to shield criminal activity or to conceal evidence of crime from criminal

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			investigations. The powers of law enforcement to investigate crimes have been interpreted extensively in relation to the right to privacy and it is submitted that the Bill complies with these standards.
	1.6 Deloitte - page 1	1.6 Cyber risk has gained significant momentum. Cyber threats are a concern of most business executives, as no business is immune from cyber attacks, which can impact a company's reputation, threaten its bond with customers, and open it up to lawsuits and regulatory scrutiny.	1.6 Noted
	1.7 All Rise - page 1	1.7 The Initiative of Government to deal with cybercrime and cybersecurity is supported	1.7 Noted
	1.8 MediaMonitoring: Africa - page 4	1.8 The fact that the SEIAS relating to the Bill was not made available for public comments is criticised. It is submitted that, from the perspective of Internet governance and the complexities involved, the SEIAS should be made available for public comments and these comments should be considered by Parliament before the Bill is further processed.	1.8 The Bill was subject to a SEIAS assessment, and the required certificate of the DPME is attached as **Annexure A.** It is not a requirement that the SEIAS be subjected to a public consultation process. The Bill on the other hand was subject to an extensive consultation process and comments that were received during this consultation process were taken into account in the finalisation of the Bill.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	1.9 Western Cape - page 1 of Annexure to letter	1.9 The Bill is necessary to bring the South Law relating to cybercrime on par with the international community. However, the Bill may impose unnecessary onerous standards which may represent regulatory risk to businesses. An integrated approach would be necessary between the various Departments and structures in the Bill to develop the necessary capacity to deal with cybercrime. A regulatory impact assessment is necessary to identify any unintended consequences which may lead to unnecessary administrative burdens for businesses.	1.9 * It is submitted that the Bill does not impose unnecessary onerous standards on businesses. SEIAS was introduced to replace RIA and to assess policies, laws and regulations in line with NDP priorities. The Bill has been subjected to the SEIAS, which is intended to ensure that the regulatory burden is reduced. The only significant obligations that may arise for businesses is if they are declared critical information infrastructures as contemplated in Chapter 11 of the Bill. Such businesses will usually be well-established with significant assets and capital. The obligations that will be imposed on such businesses is necessary to secure their own customers or persons and entities with whom they do business and will be in line with the international trends that such businesses must comply with minimum set standards to secure information infrastructures. * The CRC will ensure an integrated approach between the various Departments and structures in the Bill. Aspects relating to capacity building are addressed under paragraph 1.1, above.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	1.10 All Rise - page 7	1.10 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.	1.10 Noted. Appropriate awareness campaigns will follow the implementation of the Bill.
	1.11 South African Communications Forum - page 1 (paragraph 6)	1.11 The Bill is welcomed due to the growing risk of cybercrimes and consequent necessity for cybersecurity. This is evidenced by the growing number of indiscriminate cybersecurity attacks globally. There is a need for a clear forward looking legislative framework that sets out the offences, penalties and powers and obligations of the relevant organs of state. The Bill in the main sets out this framework.	1.11 Noted
	1.12 South African Communications Forum - page 4 (paragraph 19)	1.12 It is pointed out that the Bill has many dependencies that reside across various Departments, which also have considerable risks. When a deliverable or milestone is dependent on an action the absence or delay of that action has a knock-on effect. Consequently it is proposed that the dependencies be reconsidered in order to ensure the	1.12 The Bill has three main focus areas, namely – (a) cybercrime (Chapters 2 to 9) (b) capacity building (Chapter 10); and (c) cybersecurity (Chapter 11). Although, Chapter 10 (paragraph (b), above) relates to both cybercrime and

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		effective implementation of the Bill.	cybersecurity, current resources can be used to implement the Chapters referred to in paragraph (a) and (c), above. * Chapters 2 to 9 of the Bill deals with cybercrime and can be implemented as soon as subordinate legislation that is required to give effect to certain provisions are finalised. * Chapter 11 relates to the declaration of critical information infrastructure, and can be implemented after the infrastructure in question has been identified and appropriate directives are finalised in respect of the different categories of infrastructures * Interdependencies that may delay the effective implementation of the Bill are therefore limited and steps are being taken to overcome delays. In terms of clause 63(2) the Bill may be implemented incrementally in order to cater for possible delays.
	1.13 South African Communications Forum - page 4 (paragraphs 20 to 21 and paragraphs 23 to	1.13 There is a need to expeditiously implement the Bill. The improved clarity in respect of standards is welcomed,	1.13 The Bill has limited cost implications for electronic communications service provider and as pointed out in paragraph 1.12, incremental implementation is possible.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	24)	however, the Bill should not be too prescriptive in the technical details. Instead, determination of the standards and desired requirements should be sufficient. The South African Communications Forum and its members support the Bill and its intentions, but are nevertheless concerned about the costs of compliance. This becomes a critical concern as the communications sector is required to continually provide services at higher speeds, better quality and at lower prices. As a result, it becomes imperative that their members keep a tight rein on input costs. Incremental implementation may be necessary from a cost perspective.	
	1.14 Legal Aid SA - page 3	1.14 (a) The Bill threatens digital rights in significant ways, especially the freedom of expression and association and the right to privacy. The Bill also lacks important checks and balances and increases state power over the Internet in concerning ways.	1.14 (a) Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. It is submitted that the Bill has the necessary checks and balances in place to ensure that rights are not infringed in an unconstitutional manner.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(b) The Bill provides for significant state involvement in the monitoring of business and private cyber activity.	(b) No monitoring can take place in terms of the Bill and no powers are afforded to the State to monitor business activities.
		(c) It appears that no social impact assessment was done for the Bill.	(c) See paragraph 1.8, above
		(d) This legislation will inevitably have a major impact on other legislation such as POPIA and Promotion of Access to Information Act (PAIA). It also seems that the Bill requires people to act contrary to their rights in terms of other legislation.	(d) The protection of personal information and the right to access to information are constitutionally guaranteed rights. The Bill does not infringe on those rights guaranteed in the PAIA or POPIA.
		(e) The Bill gives the police greater powers of arrest.	(e) Chapter 5 does not expand the powers of arrest. These powers already exist in terms of the Criminal Procedure Act, but did not provide for specific procedures to investigate cybercrimes and the resultant protection of information which the Bill addresses. On an evaluation of Chapter 5 of the Bill, provision is made for various checks and balances which strictly

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			controls the powers of the South African Police to investigate crimes with a cyber element.
	1.15 Cell C, Telkom and Vodacom - page 1 (paragraph 5)	1.15 The Bill as an important step in addressing the rising threat of cybercrime to our country. The Bill aims to rationalise the laws of South Africa that relate to cybercrime and cybersecurity into a single Bill, thus addressing the current fragmentary approach and also further aligning our legislative framework to international standards.	1.15 Noted.
	1.16 Cell C, Telkom and Vodacom - page 4 (paragraph 1.1.6); MTN - page 3	1.16 Laws dealing with the submission of electronic evidence in civil and criminal proceedings can be improved to cater for technological advances. The entities indicate that they are aware that the South African Law Reform Commission is currently conducting a review of the Law of Evidence and would advise that this be taken into account insofar as it applies to electronic evidence in criminal proceedings.	1.16 Chapter 3 of the Electronic Communications and Transactions Act, 2002, currently deals with electronic evidence. The investigation by the South African Law Reform Commission has been finalised. The recommendations of the South African Law Reform Commission with regard to digital evidence will be dealt with under the Electronic Communications and Transactions Act.
	1.17 R2K - page 3	1.17 The Bill creates a framework that undermines Internet freedom overall, and enables state interference with data, devices and networks. It is submitted that	1.17 The State is not given powers to undermine Internet freedom or to interfere with communications or devices. The power to investigate cybercrimes in terms of the Bill is similar to powers that are afforded to law

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		cybercrimes legislation which defines potential offences must be as narrowly and clearly drafted as possible to prevent any possible misuse by enabling online censorship, stifling online public participation or infringe on legitimate online activities. It is proposed that the cybercrimes Chapter of the Bill needs to be significantly redrafted to ensure this.	enforcement to investigate crimes outside cyber space. The offences in Chapter 2 of the Bill already existed on the Statute Book and the Bill aims to rationalise these offences and to bring the proscriptions in line with the international position. Malicious communications as contemplated in Chapter 3 also existed on the Statute Book, but a need was identified to specifically include those offences in the Bill. Other countries have followed this route. The criticism against Chapter 3 is comprehensively dealt with in paragraph 4.1.4 under Chapter 3 of this discussion document. The criminalisation of conduct that is primarily regarded as cybercrimes, among others, compares with the law of Canada, Australia, United Kingdom, and New Zealand, and laws that were recently enacted by various countries in Africa, Sri Lanka, Malaysia and the Philippines.
	1.18 R2K - pages 13 to 17; Freedom of Religion - paragraph	1.18 The Bill takes a wrong approach to cybersecurity which is top-down and state-centric and makes	1.18 All States have an obligation to protect its sovereignty and the citizens of such a country. Although cybersecurity initiatives differ from

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	9.3 to 9.4 – (Bill is not necessary since Protection of Personal Information Act (POPIA) is adequate); Internet Solutions - pages 11 to 12 (paragraph 2.3) (overlap of Bill with POPIA)	cyberspace less secure to ordinary users. The Bill when evaluated against the three levels of protection have the following results: (a) Protection of information: Unlawful access (clause 2 of the Bill) undermines and overlaps with POPIA. Persons who, contra to the provision of POPIA access data, will be regarded as criminals in terms of the Bill. POPI contains its own remedies if a person contravenes its provisions. - Securing of devices: Clause 4 of the Bill, is the same as to make it illegal to have a set of lock picks or a crowbar, as a way of trying to stop burglaries. However, this is a misunderstanding of Internet security where the prohibited tools are used to test for security flaws in order to ensure that the systems are protected. The Bill criminalises these essential tools. Many times IT security experts would, without the authorisation of the owner of that network or software, use that tools to point out flaws in the security system. Because this Bill can't tell the difference between cybercriminals and security testers, it will discourage people from testing Internet security	country to country, the Governments of these countries are central to the implementation of cybersecurity initiatives and in the context of international developments around this area, are the leading role-players. (a) Unlawful access or any other cyber offence in Chapter 2 of the Bill must not be equated with non-compliance of the provisions of the POPIA. The POPIA, aims to promote the protection of personal information processed by public and private bodies by, among others, introducing certain conditions for the lawful processing of personal information. The offences contemplated in clause 2 are aimed at securing computer systems and data and this is an important step in the protection of computer systems and data. A hacker, for instance, that hacks into the Home Affairs database, is not a “responsible party” for purposes of the POPIA, and POPIA cannot be used to hold the hacker accountable, unless the personal information is an account

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		systems, and ultimately make the Internet less safe. Various instances are referred to where IT security experts discovered the flaws and reported it to the entity concerned. It is submitted that the act of breaching someone's security with bad intentions should be an offence, and measured by the actual harm that is done.	number. Section 59 of the POPIA, which criminalises a contravention of section 58 (1) or (2) (failure to notify the Regulator if processing is subject to prior authorisation); section 100 (obstruction of the Regulator); section 101(a contravention of section 54 which relates to a breach of confidentiality by a person acting on behalf or under the direction of the Regulator); section 102 (the obstruction of an execution warrant issued in terms of section 84); section 103(1) and (2) (non-compliance with an enforcement notice and false statements in purported compliance with an information notice); section 104(1) and (2) (offences by witnesses) must be regarded as "administrative offences" in order to ensure that there is compliance with the POPIA. In terms of section 105 of the POPIA, a responsible party, will commit an offence if an account number is processed in contravention of section 8 of the POPIA. Again this offence will not be applicable to a hacker. Section 106 of the POPIA may be used to hold any person accountable that obtains, discloses, procures the disclosure of, or sells an

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			account number. This offence is again not very helpful to criminalise the so called “gating offence” in cybercrime that give rise to most if not all crimes against a computer system. Without going into too much technical detail, most other countries that have personal information protections laws in place also criminalise unlawful access in their cyber laws. See among others also the African Union Convention on Cyber Security and Personal Data Protection.
		(b) Securing networks: A concern is raised against the declaration of critical information infrastructures by the Cabinet member responsible for State security. It is pointed out that there is a global trend in cybercrime policy of Governments seeking legal and technical 'backdoors' into networks and devices to bypass security measures for 'good' purposes and all have been resisted and decried by digital rights advocates and cybersecurity experts. It is submitted that it may be likely that the South African Government will use these provisions to seek to give itself access, direct or indirect, to the data held on 'critical information infrastructures'. It is pointed out that such backdoors may in general compromise the security of a computer system since it also allows others	(b) See paragraph 1.2, above. Furthermore, section 14(d) of the Constitution specifically guarantees the right to privacy of communications. Other legislation on the Statute Book also provides for the protection of information. The perception that Chapter 11 of the Bill gives any powers to the State to put measures in place that may give them access to information is clearly misconceived if the provisions of that chapter are considered. Chapter 11 authorises the Cabinet member responsible for State security to issue a directive to regulate, among others, minimum security

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		to access the systems in question.	standards that must be implemented on a critical information infrastructure to promote cyber security. The declaration of critical information infrastructures is subject to consideration by Heads of various Departments that have specific assigned constitutional obligations and a consultative process must be followed. The declaration of critical infrastructures can be challenged. Measures that must be implemented to secure such infrastructures must again be made in consultation with the executive authority of various Departments that have constitutionally assigned functions. The measures that must be implemented is in the form of subordinate legislation, which means that it cannot override the myriad of primary legislation that is on the Statute Book and which protect the confidentiality of communications. In any event these measures must be in line with the Constitution to be valid.
	1.19 Information		1.19 This suggestion is noted. The

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	Regulator - pages 3 and 4	1.19 The Bill was finalised before the Office of the Information Regulator was established. The Information Regulator indicates that the Bill is necessary to address current shortcomings in the substantive and procedural law of the Republic in so far as it relates to cybercrimes. According to the Information Regulator, various provisions of the Bill impacts on the mandate of the Regulator and there is a need to involve the Regulator in the various functions of the Departments involved in the Bill. The areas of involvement are discussed further in the summary.	proposals of the Regulator are dealt with in respect of the clauses where specific input was provided.
	1.20 SABRIC - page 2	1.20 Bill seems to comprehensively address cybercrime in line with international standards and address the current shortcomings in the South African law. Special necessary procedural measures are introduced to investigate cybercrime. Both the public sector and the private sector do not have the necessary skills to comprehensively address cybercrimes. The establishment of the various structures in the public and private sector may facilitate skills development.	1.20 Noted
	1.21 R2K - pages 18 to 19	1.21 It is submitted that: (a) The provisions of the Bill which deals with cybercrime should substantially be redrafted in order to prevent any possible misuse to enable online censorship, stifle online public participation or infringe on legitimate online activities.	1.21 These concerns are noted. (a) The criticism against the offences in the Bill is dealt with in paragraph 1.17. (b) See paragraph 1.18(b). It is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(b) It is inappropriate for the state security structures to be given primary stewardship over cybersecurity, as this makes cybersecurity initiatives inherently less transparent and subject to democratic control. It is recommended that cybersecurity should resort under the Department of Communications. (c) Chapters 10 and 11 of the Bill should be withdrawn	submitted that the role of the SSA is to facilitate the implementation of the cybersecurity initiative of Government as contained in the NCPF, in line with their constitutional and legislative mandate. The structure that is primarily responsible for the implementation of this initiative rests on the Cyber Response Committee as contemplated in clause 53 of the Bill. The CRC consists of various Departments with different constitutional mandates. The role of the SSA, in terms of the Bill, is in terms of Chapter 11, which deals with critical information infrastructure protection. This function is in terms of current legislation, already assigned to the SSA by the National Strategic Intelligence Act, 1994 (Act 39 of 1994). It is submitted that the Department of Communications does not have the necessary mandate, capacity and infrastructure to deal comprehensively with the implementation of the cyber initiative of the Republic. (c) Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	1.22 Centre for Constitutional Rights - pages 3 to 5, (paragraphs 7 and 8)	and redrafted with civilian agencies as controlling functionaries. 1.22 The Bill is welcomed to the extent that it addresses legitimate concerns regarding cybercrimes and breaches of cybersecurity. The Bill was redrafted and certain concerns were addressed. However, certain provisions of the Bill still infringes significantly on rights guaranteed under sections 14 (the right to privacy), 16 (freedom of expression) and 34 (access to courts) of the Constitution in so far as it aims to deal with malicious communications, powers to investigate search and seizure, interception of communications and information sharing between Government structures, respectively. These provisions are not in line with international principles.	1.22 It is submitted that the Bill is in line with international principles and norms. Information sharing between Government agencies need to be regulated by means of regulations that must be made in terms of clause 56 of the Bill. The purpose of the regulations, which will deal with the finer details of the implementation of this clause, is to ensure that an invasion of privacy does not take place. Other countries followed a similar route. The regulations will ensure that all information that is shared will be free of personal information (see among others the US Cybersecurity and Information Sharing Act of 2015 - section 104(d)(2)(A), (B) - A company intending to share a cyber threat indicator must remove—or implement a "technical capacity" configured to remove—any information "not directly related to a cybersecurity threat" that the company "knows" at the time of sharing to be "personal information of a specific individual or information that identifies a specific individual."). It must be noted that all rights in the Bill of Rights is subject to the limitation clause

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			in section 36 of the Constitution, that is , the test is whether the limitation is justifiable in an open and democratic society.
	1.23 TBCSA - pages 2 and 3 (paragraph 3.1) and page 4 (paragraph 4)	1.23 The Bill is discussed from a business perspective and the following remarks are made: * The Bill aims to address cybercrime in different industries as well as Government entities, which would imply that the South African Police Service (SAPS) would be able to deal with cybercrime and adequate sentences will be imposed for cybercrime. * Crime statistics would be available regarding specific categories of cybercrimes, which in turn will ensure that the SAPS to develop certain mechanisms and strategies to deal with it. * Ensure that specialised detectives and specialised prosecutors would be use in addressing cybercrimes. * The Bill needs to deal with issues of awareness of cybercrimes and fraud. * There is a need for highly trained information technology specialists within Government to protect critical networks – and not just state security officials such as the police and state security and defence members. * Partnership with the private sector is important and should be considered, especially as they are custodians	1.23 The remarks are noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		of information on cybercrimes. * South Africa has not yet ratified or entered into force, the Council of Europe's Convention on Cybercrime, which would serve as a deterrent for international cybercrime. The convention criminalises certain computer actions such as the interception of non-public transmission of computer data and recommends mutual assistance between countries during investigations. Alignment of the Bill with this convention is important as it relates to definitions and provisions. * Proper institutional arrangements without additional costs would enable Government to address cybercrime.	
	1.24 Mr Heyink - page 3 (paragraphs 13 and 15)	1.24 The Committee is urged in considering the structures proposed in the Bill and to investigate whether they are indeed practical and that the skills required to implement the Bill are available to Government. The Committee is also urged to clarify responsibilities and accountability for cyber security and policies supporting cybersecurity. The development of expertise and the capacity to deal with cybersecurity should be a National Imperative.	1.24 The structures in the Bill are set out in Chapter 7 (24/7 Point of Contact), clause 53 (the Cyber Response Committee), clause 54 (structures within Government to deal with cybersecurity), clause 55 (establishing of Nodal Points and CSIRT in the private sector). * The 24/7 is a structure in the SAPS that must facilitate international co-operation. The Interpol link in the SAPS currently fulfils this role in respect of international cooperation and provincial structures cater for local investigations. The establishment of a dedicated 24/7 will ensure that focused attention will be given to the investigation and

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			coordination of cybercrime investigations. It is submitted that there is start-up capacity to address the needs of the 24/7, which will be developed within available resources in due course. * The Cyber Response Committee has been established. * The Cyber Hub that has been established as is required in terms of the NCPF. * The NCPF requires that certain Government Departments must obtain institutional capacity to deal with cybercrimes and cybersecurity. In terms of the NCPF and also clause 54(1) of the Bill the SSA are responsible to establish a CSIRT for Government. This has been established. It is acknowledged that capacity building and the development of expertise is absolutely necessary for the Republic to come to terms with cybercrime and cybersecurity.
	1.25 Mr Heyink - page 4 (paragraphs 20 and 21)	1.25 During the development of the Bill there were calls	1.25 General objectives that must be adhered to in order to be cyber secure are:

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		to split the Bill in two Bills, the one to deal with cybercrime and the other with cybersecurity The Bill as it stands addresses cybersecurity responsibilities without addressing the proper coordination of a cybersecurity framework across both the public and private sectors. Co-operation and coordination of cybersecurity across all sectors of society is a characteristic of cybersecurity legislation in democracies globally.	* Emergency warning systems regarding cyber vulnerabilities. * Raising awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them. * The identification of critical infrastructure and enhanced protection of such infrastructures. * Tracing of attacks on information infrastructures and, where appropriate, the disclosure of tracing information. * Enhancement of response mechanisms to deal with attacks. * Continuity and contingency plans in the event of attacks on information infrastructure. * Adequate substantive and procedural laws, and trained personnel that can investigate and prosecute cyber offences and the ability to coordinate investigations with other countries. * International co-operation when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities,

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws. * The promotion of partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures. It is submitted that the Bill as a whole complies with these requirements. The coordination of the implementation of cybersecurity measures in Government will primarily be facilitated through co-operation in the CRC. The Cyber Hub and the DTPS plays an important role in involving the private sector in the cybersecurity initiative and to share information between Governments and the private sector. It is therefore submitted that it is not necessary to split the Bill in two separate Bills.
	1.26 Mr Heyink - page 4 (paragraph 22)	1.26 The normal research and consultative processes that would characterise legislation of such broad	1.26 The Bill was thoroughly researched and a broad and extensive consultation on the Bill took place. Various other commentaries have

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		application has not been followed. This failure has led to the Bill being heavily biased towards national security and law enforcement at the expense of civil liberties. Whoever may be in power may use this bias to abuse the civil liberties of citizens and lead to selective prosecution. This trap must be avoided in any democratic society.	attested to the amount of research that was done as well as the protracted and extensive consultation process taking into account that most offences in the Bill is already on the Statute Book and that the Criminal Procedure Act is used to investigate cybercrimes without the additional safeguards that is provided for in the Bill. Furthermore, the provisions of the Bill, in so far as it aims to address cybercrime, are on par with legislation of other constitutional democracies.
	1.27 Mr Heyink - page 4 (paragraph 23)	1.27 The broad wording used in the Bill is subject to many interpretations. As the Bill will affect all citizens across a wide spectrum of our society, the failure to draft the Bill in plain language and terms that is easily understandable by the many people that will be affected by the Bill, is highly undesirable and dangerous in a democracy. If skilled lawyers cannot understand the Bill what chance does the layman have?	1.27 The Bill is of a technical nature and substantially compares with the various model laws, the African Union (AU) Convention, the Budapest Convention, and legislation of Canada, the UK, New Zealand, the USA, various countries in Africa, Sri Lanka, Malaysia, and the Philippines among others. In any event, as pointed out above, most of these offences were already on the Statute Book.
	1.28 Liquid Telecom - pages 3 to 4		1.28 Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	(paragraphs 7 to 13) and page 8 (paragraphs 36 to 40)	1.28 The Development of the Bill was followed through its various stages, from the development of the National Cybersecurity Policy Framework (NCPF) in 2012, through the various stages of the Bill and the publication of the initial draft Bill in 2015. The author submits that the Bill is critical to address cybercrime but law enforcement must ensure that they can meet their obligations under the Bill. The author indicates that there may be concerns with the reach of the Bill and various definitions. The productive and cooperative manner in which the Bill was prepared is acknowledged. The Bill is necessary. Attention should be given to the wide powers that are afforded to law enforcement.	
	1.29 South African Human Rights Commission (SAHRC) - page 9 (paragraph 4)	1.1.29 The SAHRC recognises the need for a legislative framework to address cybercrimes and cybersecurity in South Africa. Freedom of expression and the right to privacy within the context of the Bill should be carefully balanced against the provision of the Bill. The crimes in the Bill should be defined as narrowly as possible. It is further suggested that the Bill will require extensive public education as well as training for officials who will be tasked with its implementation.	1.29 Noted.
	1.30 Mr Eatwell - pages 1 to 9 and 10 (paragraphs 45.5 and 46)	1.30 Mr Eatwell describes his experiences when he was unjustifiably prosecuted in relation to alleged cyber offences. In his submission he deals with various irregularities that took place during an investigation and points out the general lack of expertise in law	1.30 Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		enforcement and the courts to deal with computer-related crime.	
	1.31 Liquid Telecom - page 7 (paragraphs 31 to 33)	1.31 Various Departments are involved in the implementation of the Bill and substantial subordinate legislation needs to be enacted. The author points out that coordination is therefore absolutely necessary in order to ensure that the implementation of the Bill is not delayed.	1.31 Noted. See paragraph 1.12, above regarding implementation of the Bill.
	1.32 IAB - paragraphs 2.1 and 4.2	1.32 IAB appreciates the need for regulation of cybercrime in particular, and cybersecurity in general. Its members stand to benefit from several protections provided for in the Bill and the reform of outdated legislation limited in its scope of protection is welcomed. However a balanced approach should be followed.	1.32 Noted
	1.33 IAB - paragraph 2.3	1.33 The Bill amends various laws, and unintended consequences may result. The Bill does not give adequate attention to electronic evidence and does not consider the implications of information and data protection laws.	1.33 The Bill rationalises the cyber offences on the Statute Book in a single Bill and repeals other provisions on the Statute Book that criminalise similar conduct. The status of the Bill vis-a-vi the POPIA is discussed under paragraph 1.18(a), above.
	1.34 SAHRC - page 1 (paragraph 1)	1.34 More and more complaints that are investigated, by the SAHRC have a cyber dimension.	1.34 Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
2. CHAPTER 1: DEFINITIONS			
2.1 "access"	2.1 SAHRC - pages 2 and 3	The SAHRC refers to the definition of "access" and is of the opinion, that the word "without limitation" in the definition of access may be vague.	The phrase "without limitation" is to ensure that law enforcement officers are empowered during an investigation and not restricted to the actual "use" of data, a program, storage medium or computer system or peripherals. It is however submitted that the phrase "includes" and the phrase "to make use of", already ensure an extended interpretation of the definition. The Department is however of the view that the words "to the extent necessary to search for and seize and article", should be removed from the definition since it may lead to interpretation inconsistencies with the use of the word of "access" in Chapter 5.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
2.2 "article"	2.2.1 Western Cape - page 1 of Annexure to letter	2.2.1 The word article is used in the definition of "article", which is incorrect. It is suggested that the words "the same means" rather be used.	2.2.1 To address the linguistic concern the definition can be amended as follows: "**article**" means any data, computer program, computer data storage medium, or computer system which— (*a*) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission; (*b*) may afford evidence of the commission or suspected commission; or (*c*) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission, of an offence— (i) in terms of Chapter 2 or section 16, 17 or 18 of the Act; or (ii) any other offence, **[which may be committed by means of or facilitated through, the use of such an article,]** whether within the Republic or elsewhere;".

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	2.2.2 Legal Aid SA - page 5	2.2.2 Paragraphs (*a*) and (*c*) of the definition of "article" requires the investigator to show that there were reasonable grounds that the article was connected with the commission of the offence, or intended to be used in the commission of the offence. The requirement for reasonable grounds is absent in paragraph (*b*) which in effect empowers investigators to search for articles without the need to prove that there are reasonable grounds that it will provide evidence for the commission of a crime.	2.2.2 Paragraph (*b*) of the definition is in line with section 20(*b*) of the Criminal Procedure Act, 1977.
	2.2.3 MTN - pages 4 to 5 (paragraph 2.5)	2.2.3 - "article" refers to "data, computer program, computer data storage medium, or computer system". This is not in line with international best practices.	2.2.3 This definition relates to Chapter 5 of the Bill that deals with the powers to search and seize. It is submitted that the definition contains a precise and comprehensive description of the different technological components that may be involved in cybercrime. Without going into technical detail most model laws and Conventions recognise a computer system, storage medium, data and computer program that is either the object of a cyber crime or used to commit a cybercrime. In many instances data includes a computer program (SADC Model Law, CW Model Law and HIPCAR Model Law). The

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			Budapest Convention and AU Convention merely deals with a computer system and computer data, which includes all the different aspects dealt with in this definition.
	2.2.4 IAB - paragraph 3.1	2.2.4 Article in the context of cybercrime offences means "data, computer program, computer data storage medium or computer system". The term is used in a catch-all manner that may lead to confusion in the interpretation of the Bill.	2.2.4 See paragraph 2.2.3

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	2.2.5 SAHRC - pages 2 and 3	2.2.5 With reference to the definition of "article", the SAHRC remarks that the persons who investigate an offence would be legally authorised to make use of data on the personal computer of a person, on the grounds that it is, 'concerned with'; 'connected with'; or has 'reasonable grounds' to believe that there is a connection with an offence. The SAHRC notes that there is no further clarity of these terms and that it may, from a practical perspective, lead to an inconsistent application of the provision. In addition, the Bill may impact the right to privacy on multiple grounds namely, i) 'person searched' if a mobile phone is on a person's body; ii) 'property searched' in terms of any device in a person's possession; and, iii) 'possessions seized' and 'communications infringed' in terms of 'data' being accessed indiscriminately. The SAHRC therefore notes that the Bill vests a disproportionate amount of discretion and power to the official for the purposes of searching and accessing any person's device. Furthermore, if 'access' entails unfettered access to data, and 'data implies electronic representations of information in any form,' then authorities can access any electronic information of any person and possible do so without retribution. In addition, it may be implied that in order to invoke its sweeping orders under the Bill, officials would only need to suspect that a particular piece of data, a computer or any computer system may afford evidence of the commission or suspected commission of an offence. The SAHRC recommends that Parliament	2.2.5 The Bill recognises the potential wide ranging infringements that can take place where digital devices are subject to criminal investigations. As a starting point, the Bill requires that investigations must take place in terms of a warrant as contemplated in clause 27. Clause 27 is substantially in line with section 20 of the Criminal Procedure Act and the same considerations will be applicable. See among others ZOECO SYSTEM MANAGERS CC v MINISTER OF SAFETY AND SECURITY NO AND OTHERS 2013 (2) SACR 545 (GNP) and POLONYFIS v MINISTER OF POLICE AND OTHERS NNO 2012 (1) SACR 57 (SCA) which clearly sets out the requirements for a search warrant. (These judgments are summarised in Annexure B and reference is made to other applicable judgments). In order to deal with exigent circumstances, the Bill provides for oral applications for warrants to counter the current position in terms of the Criminal Procedure Act that provides for search and seizures under narrow prescribed circumstances (clause 28). Although the Bill provides

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		consider amending the definition of 'access' to rather adopt the term which relates to a 'reasonable limitation' to make use of data.	for the arrest of suspects and seizure of computer equipment, these provisions require that judicial authorisation is necessary to access the content of such devices, unless the exceptional circumstances exist (clause 30 and 31).
2.3 "computer"	2.3.1 Cell C, Telkom and Vodacom - pages 7 to 8 (paragraph 2.1); TBCSA - page 2 (paragraph 3.1) – inclusion of cellular phones	2.3.1 (a) The definition of "computer" should be cognisant of the fact that computer can no longer commonly be described as a device but may otherwise also be a software image that in its entirety emulates all the functions of a computer by means of virtualisation and within such software image, programs, data and storage can be contained.	(a) The definition of the Bill is broad enough to deal with virtualisation. In virtualisation there is a primary computer device (computer or server) that implements software that creates virtual machines with their own operating systems, memory, storage capacity and other attributes. This virtualisation is still dependant on the program that was implemented on the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			original hardware device. Two scenarios is possible in terms of the definition of the Bill, namely – - interference with a virtual device may be regarded as interference with the device that implement the program, which creates the virtualisation; or - interference with the virtual device itself.
		(b) The question is raised whether or not the definitions of "computer" or "computer system" accounts for the concept of Network Function Virtualisation (NFV) where it may not be possible to discern where the computer or computer system was present at the precise time of the incident.	(b) NFV is relatively new technology, developed in 2013. The aim of this technology is, similar to computer virtualisation, to create various networks without the need of hardware devices which will be incorporated in the virtual network. From the perspective of criminalisation, the definitions of the Bill are adequate.
		(c) For reasons of consistency the Bill should not leave the classification of devices such as smartphones or tablets as computers or computer systems to police officials or possibly misconstrued public consensus. Such classification should at least be covered in training and be incorporated in Standard Operating Procedures.	(c) The definition of computer specifically provides that a computer must be regarded as "any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing, processing

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			or storage operations in accordance with set instructions". This definition is wide enough to include smartphones, tablets etc.
	2.3.2 Deloitte - page 1	2.3.2 It is suggested that the definition of "computer" must be amended to ensure adequate inclusion of operational technology such as medical devices, self-driving automobiles, automotive automation, aviation automation, Internet of Things devices, home-automation, building management systems and automation, industrial control systems, etc. The following amendment is proposed: "computer'' means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment or any part thereof to perform predetermined arithmetic, logical, routing, processing or storage operations <u>or physical actions</u> in accordance with set instructions and includes all—"	2.3.2 The definition of "computer" already caters for such an eventuality. However, it is submitted that the definition be amended as follows: ""computer" means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions **[and includes all—** **(*a*) input devices;** **(*b*) output devices;** **(*c*) processing devices;** **(*d*) computer data storage mediums; and** **(*e*) other equipment and devices, that are related to, connected with or used with such a device]**;" – This proposed definition is in line with international benchmarks. However, the offence of "access" in

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			clause 2, also aims to criminalise access to the resources (hardware) of a computer system. This is necessary to address, for instance the reconfiguration of hardware to commit other crimes or to deal with offences, similar to clause 3, where the data storage medium in a computer is taken with all data stored upon the storage medium.
	2.3.3 MTN - pages 4 to 5 (paragraph 2.5); IAB - paragraph 3.1	2.3.3 "computer" which also includes devices that are related to or connected or used with a computer. This is not in line with international best practices.	2.3.3 During the development of the Bill, suggestions were made to extend this definition to include peripherals, where the distinction between a programmable devices and the peripheral are blurred. To keep in line with international benchmarks, the changes to the definition are proposed in paragraph 2.3.2, above.
2.4 "computer data storage medium"	2.4.1 MTN - pages 4 to 5 (paragraph 2.5); IAB - paragraph 3.1	2.4.1 A computer storage medium includes a location from which data or a computer program is capable of being reproduced. This is vague and confusing and likely to result in vague search warrants and directions. This is also not in line with international best practices.	2.4.1 The inclusion of location was proposed during the development of the Bill. It was argued that location may cater for aspects such as cloud computing. In cloud computing all computational tasks take place within the cloud (a multitude of servers connected to each other and accessible

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			via the Internet, often through a Web interface, thus forming a "cloud" of computational power). The international benchmark for this definition varies. However, the most acceptable definition is as follows: "computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device;" – See CW Model Law, section 3; SADC Model Law section 3 (7): HIPCAR, section 3(7); Tanzania, section 3; Botswana, section 2. It is submitted that the definition need not be amended.
2.5 New definition proposed: "electronic communications identity number"	2.5.1 Banking Association SA - page 2	2.5.1 For purposes of clause 20, a definition of "electronic communications identity number" should be inserted.	2.5.1 Agree. It is proposed that the following definition be inserted: **"electronic communications identity number"** means a technical identification label which represents the origin or destination of electronic communications traffic, as a rule clearly identified by a logical or virtual identity number or address assigned to a customer of an electronic communications service provider (such as a telephone number, cellular phone

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			number, email address with or without a corresponding IP address, Web address with or without a corresponding IP address or other subscriber number);".
2.6 "electronic communications service provider"	2.6.1 All Rise - page 3 (paragraph 10)	2.6.1 For the purposes of the malicious communications provisions, given the fact that harm and harassment occurs on their networks and the electronic communications they facilitate e.g. via email or chat features, it is recommended that providers of blogging and social networking services be included and not only service providers with an electronic communications license	2.6.1 The Department does not agree with this proposal. Clauses 19, 20 and 21 of the Bill, provides that "persons in control of a computer system" must in terms of an order – * in terms of clause 19, ensure that access is not granted to the malicious content; * in terms of clause 20, furnish particulars to the court to identify the perpetrator; and * in terms of clause 21, destroy or render inaccessible the malicious content. The phrase "persons in control of a computer system" can be used to bring blogging and social network providers within the web of those provisions. It must, however, be pointed out that the provisions may not necessarily offer protection from malicious communications outside the jurisdiction

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			of the Republic.
	2.6.2 SAFACT - page 3 (reference is made to a previous version of the Bill)	2.6.2 The definition of electronic communications service provider includes "anyone" (including an entity) who processes or stores data for someone else – an ESCP is thus essentially "everyone".	2.6.2 This comment is not applicable to the Bill since reference is made to a previous version of the Bill that was made available in the development of the Bill.
2.7 "financial institution"	2.7.1 Minister of Finance paragraph (a)) (Also see the comments of the JSE in respect of the definitions of "financial institution" (clause 1), "financial sector regulator" and "regulatory body" (as used in Chapter 11 of the Bill), which should be amended to be in line with the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017)	2.7.1 The definition of "financial institution" refers to the Financial Service Board Act, 1990. In June 2017 the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017), was passed, and which repeals the Financial Service Board Act. This definition should therefore be amended to refer to the definition in the Financial Sector Regulation Act.	2.7.1 Agree. The definition will be amended in consultation with the legal division of the National Treasury. A proposed definition is as follows: "**financial institution**" have the meaning of a 'financial institution' as defined in section 1 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017);
2.8 New definition"	2.8.1 Western Cape - page 2 of Annexure	2.8.1 A definition of National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), should be inserted.	2.8.1 Agree. It is proposed that the following definition be inserted after the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
"National Strategic Intelligence Act, 1994 (Act No. 39 of 1994)"	to letter		definition of "NPA Act, 1998": "National Strategic Intelligence Act, 1994" means the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994);".
2.9 "output of data"	2.9.1 MTN - pages 4 to 5 (paragraph 2.5); IAB - paragraph 3.1	2.8.1 "output of data" means by having it displayed or in any other manner. This definition is not in line with international best practices. It is proposed that a complete definition be inserted of what constitutes "output of data" and "display of data".	2.9.1 This definition relates to the offence contemplated in clause 2 dealing with unlawful access and is based of section 1(*b*) of the UK Computer Misuse Act, 2013. The definition is in line with section 17 of the UK Act. Output of data may be obtained through having it displayed on a computer screen, by printing it or among others obtaining electromagnetic emissions from the screen or from the system over which it is transferred. The word "in any other manner" ensures that the definition is not limited in any way. The Department, is of the view that the definitions of "output of a computer program" and "output of data", should be moved to clause 2, since it is mainly relates to that clause.
2.10 "person"	2.10.1 Banking Association SA -	2.10.1 The definition of "person" should include an organ of state. Reference is made to the Financial Sector	2.10.1 It is not necessary for purposes of the Bill to extend the definition by

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	pages 1 and 2	Regulation Bill, which contains such a definition.	also including the "State". The aim of the definition in the Bill is to ensure that a person must be interpreted to as to include a natural and legal *persona*.
2.11 "Public available data"	2.11.1 Deloitte - page 2	2.11.1 Grammatically, data that is available in the public domain is "publicly available data" and the opposite is "non-publicly available data".	2.11.1 Agree. It is proposed that the definition be amended accordingly: "'**[public] publicly available data'** means data which is accessible in the public domain without restriction;". Consequential amendments need to effected to clause 43 of the Bill.
2.12 "seize"	2.12.1 Banking Association SA - page 2	2.12.1 In the definition of "seize", a comma should appear after the words 'render inaccessible' in paragraph (*b*), to ensure consistent legal interpretation that the "render inaccessible" applies to the whole of paragraph (*b*): render inaccessible, data, …..".	2.12.1 Agree. It is proposed that paragraph (*b*) be amended accordingly: "(*b*) render inaccessible, data, a computer program, computer data storage medium or any part of a computer system in order to preserve evidence;"
2.13 "traffic data"	2.13.1 MTN - pages 4 to 5 (paragraph 2.5)	2.13.1 "traffic data" is broadly defined to include the format of communications, duration or type of underlying service. The definition is not in line with international best practices.	2.13.1 The definition in the Bill is in line with international benchmarks, see among other Article 1(d) of the Budapest Convention; section 3(22) of the SADC Model Law; section 3 of the CW Model Law; section 3(18) of the HIPCAR Model Law. It is not necessary to indicate that this is data generated by

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			a computer system that is part of the chain of communication as is suggested by the referred authorities.
2.14 General	2.14.1 TBCSA - page 3 Item 1	2.14.1 There is no definition of cybercrimes or cyber fraud, which are dealt with later in the Bill. Examples of cybercrimes could also be offered in a definition that is explicit, such as data espionage, illegal interception, hacking, phishing, system interference, identity theft, website defacement, cybersquatting, etc.	2.14.1 It is not necessary to insert a definition of “cybercrime” in the Bill. This may have unintended consequences by being restrictive. There is no general, universally recognised definition of cybercrimes and the approach of other countries is not to define cybercrimes in their cyber crime laws.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
3. CHAPTER 2: CYBERCRIMES			
3.1 General	3.1.1 IAB - paragraph 3.3	3.1.1 The Bill does not recognise the use of digital tracking and analytical software to collect, monitor and analyze data traffic and digital communication channels in connection with marketing and advertising intelligence. With the current wording, such legitimate uses would potentially be classified as unlawful. Any potential for strict liability for the possession or use of the above software would put digital content industries to substantial legal risk. The Bill should include a clear exception from liability for legitimate use of digital rights management and analytics software.	3.1.1 These aspects do not fall within the ambit of the objects of the Bill and should be dealt with in the Copyright Amendment Bill. As long as the procedures do not fall within the proscriptions of the offences of Chapter 2 of the Bill or amount to a contravention of the RICA, criminal liability would not follow.
	3.1.2 South African Communications Forum - page 2 (paragraph 7 to 11)	3.1.2 Chapter 2 of the Bill sets out the offences or cybercrimes, which is largely aligned to international best practice. However, the view is held that the Bill inadvertently omits two key cybercrimes which should be included due to the significance and magnitude of its consequences – these are identity theft and phishing. We therefore, propose that these are included in Chapter 2.	3.1.2 The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. In a real life example a person will receive a document from SARS, indicating that he or she received a tax rebate and the person is requested to provide his or her bank account number to the sender of the email. Clause 9 of the Bill deals with cyber forgery and uttering, which makes a specific offence of “phishing”, superfluous. Identity theft is discussed under paragraph 3.1.5, below

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	3.1.3 MTN - page 3	3.1.3 The Bill should consider the implications of POPI, specifically concerning the lawful processing and the offences stipulated in that Act. According to MTN where other legislation allows for offences, those will prevail	3.1.3 POPIA, with the exception of sections 105 and 106, creates various administrative offences that cannot be used to address the conduct which is criminalised in terms of the Bill. Other offences on the Statute Book prevail unless they are amended or repealed by the Bill and the Bill does not deal with the offences in terms of the POPIA.
	3.1.4 Cell C, Telkom and Vodacom - pages 3 to 4 (paragraphs 1.1.3 to 1.1.5)	3.1.4 The provisions dealing with cybercrime do away with the fragmentary approach relating to the criminalisation of cyber offences and repeal other laws that deal with these aspects. Where a person is prosecuted for an offence in terms of the Bill, the State must still prove the elements of an offence beyond reasonable doubt as is required in terms of the adversarial criminal justice system of the South African law. Save where otherwise cautioned, the provisions of the Bill is not in contradiction with the presumption of innocence that has been emphasised by our courts: acts have to be criminalised and have to be committed with a criminal intent.	3.1.4 Noted
	3.1.5 Cell C, Telkom and Vodacom - pages 4 to 7 (paragraph 1.2)	3.1.5 It is proposed that the offence which criminalises various forms of identity theft and which was contained in the initial draft of the Bill in 2015 and the subsequent proposed amendment to the POPIA should again be considered for inclusion in the Bill. Identity theft is a “key	3.1.5 The POPIA does not deal with identity theft which is also one of the shortcomings of the POPIA. Account numbers as contemplated in sections 105 and 106 of the POPIA, only

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		offence" that facilitates other cybercrimes. References are made to the three stages of the offence namely, the obtaining of identity information, the possession and disposal of identity information and as a third stage the use of identity information for the purposes of committing an offence. Reference is also made to a study which deals with identity theft conducted by the EU in December 2012, which demonstrates the impact of identity theft in the EU. It is proposed that the following clause should be inserted in the Bill to deal with the various identified stages of identity theft: "**Personal and financial information or data related offences** … **.** (1) Any person who intentionally and unlawfully— (*a*) acquires by any means; (*b*) possesses; or (*c*) provides to another person, the personal information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence. (2) Any person who intentionally and unlawfully— (*a*) acquires by any means; (*b*) possesses; or (*c*) provides to another person, the financial information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence. (3) Any person who intentionally and unlawfully uses the personal information or financial information of another person to commit an offence under this	addresses a narrow range of essential information that is needed to commit cybercrimes. In any event POPIA is only applicable to a "responsible party" and a hacker cannot be regarded as a responsible party. The proposed offences was removed from the Bill, due to the fact that some persons were of the opinion that the offences may have unintended consequences. Many other countries have offences on their statute books that deal with identity theft, specifically. This aspect also received international attention.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		Act or any other law is guilty of an offence. (4) Any person who is found in possession of personal information or financial information of another person in regard to which there is a reasonable suspicion that such personal information or financial information– (a) was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under this Act or any other law; or (b) was used or may be used to commit an offence under this Act or any other law, and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence. 5. ……. (7) For purposes of this section— (a) "personal information" means any 'personal information' as defined in section 1 of the POPIA, 2013 (Act No. 4 of 2013); and (b) "financial information" means any information or data which can be used to facilitate a financial transaction.".	
	3.1.6 Cell C, Telkom and Vodacom - page 20 (paragraph 2.5.12)	3.1.6 In light of the fact that electronic communications service providers are mere conduits of information or data, it is proposed that a "mere conduit clause", specifying that electronic communications service provider's shall not be criminally liable for criminal actions committed on its network unless they (electronic communications service provider's) have intentionally and unlawfully committed an offence under the Act, be included in the Bill.	3.1.6 The offences in Chapters 2 and 3 (in so far as it criminalises malicious communications), does not impose any form of criminal liability on electronic communications service providers where their networks were involved in the commission of these offences. The "mere conduit" provision is already on the Statute Book (section 73 of the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			Electronic Communications and Transactions Act, 2002).
	3.1.7 Michalsons Attorneys - pages 1 and 2 and 5 to 6	3.1.7 (a) Offences in Chapter 2 of the Bill require "unlawfulness". Unlawfulness means conduct (or a consequence) that is prohibited by law. Broadly speaking, law is made up of common law and statute. What makes something unlawful is determined by a standard of objective reasonableness based on the legal convictions of society. In the post Constitutional era, the legal convictions of society are informed by constitutional values. It is essentially a conduct that is allowed and not prohibited by any law. Unlawfulness means conduct that is prohibited by the law and some unlawful conduct are deemed to be a crime or an offence in certain cases, thus making that unlawful conduct illegal. In terms of the wording in the Bill, and the way the offences are drafted in Chapter 2, something is an offence only when you 'unlawfully' and intentionally do x. Essentially what this means is that if your unlawful conduct is unlawful, you are committing an offence in terms of the Bill. This understanding is circular and on the face of it, does not make sense. As an example clause 2 provides that if x unlawfully and intentionally secure access to data, x is guilty of an offence. But for something to be an offence, the conduct must already be unlawful, and this conduct is unlawful as it is prohibited by this Bill. Another unfortunate effect	3.1.7 (a) In general, criminal liability recognises four separate and distinct elements or requirements, namely: (i) an act (actus reus); (ii) which is unlawful (unlawfulness); (iii) causing the crime (causation); and (iv) committed with the necessary intent or culpa (mens rea). The basic principle in criminal matters is that the *onus* is on the State to prove all the elements. The mere fact that an act corresponds to the definitional elements of a crime does not mean that a person who performs the act is criminally liable. Two other elements is further necessary, namely – * unlawfulness; and * culpability (also known as fault or *mens rea*). These elements do in many instances not form part of a statutory criminalising provision. However, the Bill includes both. Even if the Bill did not include these elements, courts will read the requirements in the proscriptions (see among other S v SELEBI 2012 (1)

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		of this broad wording is that unlawful conduct that was previously not a crime, is now a crime in terms of the Bill. For example, in section 9 of the POPIA you are required to lawfully process personal information. To lawfully process personal information, you must comply with the conditions set by POPIA. If you do not comply with those conditions, you are processing personal information unlawfully, but you are not committing a crime. POPIA defines processing to essentially mean doing anything with personal information. Considering the broad wording of the Bill however, your unlawful conduct of not complying with POPIA, could result in you committing a crime in terms of the Bill. POPIA was never intended to criminalise such conduct, otherwise Parliament would have made unlawful processing a crime in POPIA. It is suggested that the word "unlawful" should be removed from the offences in Chapter 2 of the Bill which will bring the Bill into line with the Budapest Convention and other regional instruments. (b) There is a relationship between unlawfulness and	SACR 209 (SCA), paragraphs [8] and [9]). Unlawfulness, in short means the absence of any ground of justification or defence which would justify the act that complies with the proscription. There is no *numerous clauses* of defences in the South African Criminal law, however, in the context of cybercrime, necessity and consent is probably the defences that will in most instances be used to justify an act that falls within a criminalising provision. The State must prove the absence of any defence before conduct can be regarded as unlawful. Culpability is comprised of two elements, namely fault and criminal capacity. The fault requirement in terms of the Bill is intention in the form of *dolus directus, dolus indirectus or dolus eventualis*. Criminal capacity requires that at the time of the act, the perpetrator had the ability to appreciate the wrongfulness (in other words that he or she acts unlawfully) and to conduct him or her in accordance with this appreciation of the wrongfulness. (b) The words "'without authorisation" or

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		defences that exclude unlawfulness. Essentially, a person might have done the act prohibited by law but may escape liability by raising a defence that excludes unlawfulness. The existence of these defences is based on the theory that the same society that deems the conduct to be in contravention to their values but also deemed it justified conduct in certain circumstance. In order to deal with this aspect it is suggested that the words "'without authorisation' or 'without any justification' be added to the criminalising provisions.	"without any justification" or "without colour of right" are used in foreign legal systems and fulfil the same role as concept of unlawfulness in the SA Criminal law.
	3.1.8 Michalsons Attorneys - pages 3, 4 and 5; Engen Petroleum - page 2 (paragraphs 7 and 8) – where the commentator deals with unlawfulness	3.1.8 Most of the crimes in the Bill are too broadly defined, and the result is most if not all conduct is deemed to be criminal. Reference is made to clauses 2, 3, 5 and 7 of the Bill. In respect of clauses 2 and 3, it is submitted that the clauses in question include use of data in their definition. Both include moving and copying in their definition. Further, 'interference with data or a computer program' and 'securing access' both include deleting or altering in their definition. There it is unclear what is different and distinct in the clauses, and what specific conduct the clauses deal with. Essentially what this means is that if you do anything with data or a computer program that is deemed to be unlawful, is committing an offence. The basic principle of legality is that a crime must be clearly defined. The principles of legality were common law principles (and remain so) but they are also in the Constitution s 35(3)(l) to (n). It is	3.1.8 The offences in clause 2, criminalise the act of securing access and define when a person secures access to data. The offences in clause 3 aim to deal with the acquiring of data (person takes possession of the data). The objective of clause 5 is to criminalise the interference with data (for instance where a person sends a virus to a computer to encrypt data on a computer). These offences are clearly defined substantially in line with legislation of other countries. It is submitted that these offences are not vague or overly broad and are aimed to criminalise specific different acts.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		submitted that the crimes in the Bill are not worded with reasonable precision. As shown above by the quoted clauses, there is significant overlap in the definitions of the crime because the crimes are drafted so broadly, and vaguely. One could be charged for multiple crimes simply based on the overlaps.	
	3.1.9 Zoelpha Carr - pages 1 to 3 (also see discussion under Chapter 11)	3.1.9 Biometric images as a security tool is discussed and the questions are asked as to whether the Bill - * criminalise certain conduct in relation to the use of biometric images for criminal purposes; and * enables Government to effectively deal with biometrics as an identity management tool. It is submitted that mismanagement of biometrics may give rise to crime.	3.1.9. Misuse of biometric images as a security tool are criminalised in terms of clause 7(1) and (2), read with clause 7(3)(*f*) of the Bill. The clauses in question criminalise conduct relating to the acquisition, possession, provision, receipt or use of password, access codes or similar data or devices.
	3.1.10 Engen Petroleum - pages 1 and 2 (paragraphs 4 to 6)	3.1.10 The Bill is inconsistent in the manner it deals with the element of intention as part of the conduct criminalised. Clauses 2 to 7 of the Bill requires the conduct to be intentional as part of the other elements of the offence. However clauses 8 to 10 specifically link intention to the nature of the offences in question. The latter approach is preferable since it clarifies the nature of the test that should be used to determine intention. The proposed manner will ensure that persons who potentially engage in conduct which is unlawful without the required criminal intent cannot be held accountable. As an example reference is made to clause 3, which according to the author imposes strict liability in the	3.1.10 The offences of cyber fraud (clause 8) and cyber forgery and uttering (clause 9), were drafted in accordance with the elements of the offences in terms of the common law which require a specific intent in relation to the misrepresentation that was made, namely to induce somebody to embark on a course of action prejudicial to him or herself as a result of the misrepresentation. In clauses 2 to 7, the intention requirement relates to the prescribed elements of the offences in

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		sense that an entity may intentionally acquire data from a third party in terms of a valid contract without the knowledge that the data was acquired unlawfully and will have the result that the acquiring party may be held liable without any intention to contravene the provision in question	question. * Clause 3(2) does not impose strict liability and specifically requires that the State has to prove that the person who possesses the data has "knowledge that the data was acquired unlawfully".
	3.1.11 Engen Petroleum - page 2 (paragraphs 7 and 8)	3.1.11 The Bill should deal with all cyber-related criminal conduct and repeal other similar offences on the Statute Book.	3.1.11 All other similar offences are repealed in terms of 61 of the Bill (see the Schedule to the Bill).
	3.1.12 Legal Aid SA - page 3	3.1.12 There is no public interest defence under this Bill - (this is raised in respect of clauses 2 and 3 of the Bill dealing with unlawful access and unlawful acquiring of data). According to the author, the mere fact that data is protected by a password should not give rise to criminal liability especially where journalists are involved. According to the author journalists may be held liable for obtaining information illegally and then for distributing the information.	3.1.12 The role of journalists in a democratic society was recognised in KHUMALO AND OTHERS v HOLOMISA 2002 (5) SA 401 (CC) (2002 (8) BCLR 771; JOHNCOM MEDIA INVESTMENTS LTD v M AND OTHERS 2009 (4) SA 7 (CC); and HOLOMISA v ARGUS NEWSPAPERS LTD 1996 (2) SA 588 (W). The crux of these judgments is that journalists should not have special protection not available to others. In the discussion of unlawfulness in Criminal law, in paragraph 3.1.7, it was pointed out that there is no close category of defences that may exclude unlawfulness.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			Necessity may be used as a defence where a person, in the public interest, commits an offence. A public interest defence in relation to criminal offences has not yet been recognised by our courts. It is however, submitted that the Bill cannot deal with such a defence since it must apply to all criminal conduct and in a variety of circumstances and need to be considered carefully.
	3.1.13 Mr Snail – (last two pages)	3.1.13 An evaluation of clauses 2, 3, 5 and 12 of the Bill is made with reference to Chapter 13 of the Electronic Communications and Transactions Act, 2002, in order to determine whether the Bill has bettered the current provisions that criminalise cybercrime. The opinions of various academic and other persons pertaining to the Bill are discussed during this evaluation, where various opinions and concerns were raised against the Bill. According to the author "any study of cybercrime offences must take into account the Criminal Procedure Act as this is law that deals with issues applicable to all offences" and secondly "when analysing the functions of cybercrime legislation, there are several aspects which needs to be taken into account, namely; setting clear standards of behaviour for the use of computer devices; deterring perpetrators and protecting citizens; enabling	3.1.13 Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		law enforcement investigations while protecting individual privacy; providing fair and effective criminal justice procedures; requiring minimum protection standards in areas such as data handling and retention and enabling co-operation between countries in criminal matters involving cybercrime and electronic evidence", should be taken into account in evaluating the Bill. The author is of the opinion that the Bill addressed the shortcomings in the Electronic Communications and Transactions Act but he also points out that the Bill has shortcomings with reference to the powers which it affords to the State in respect of private communications over the Internet.	
3.2 Clause 2: Unlawful access	3.2.1 Cell C, Telkom and Vodacom - pages 8 to 9 (paragraph 2.2.1) and oral submissions to JPC	3.2.1 The offence is in line with the international position and necessary in view of the rise of this type of offence. However, during oral submissions it was recommended that the offence be brought in line with the Budapest Convention on Cybercrime. (Overcoming security measures and the access a computer system)	3.2.1The offence is loosely based on section 1(*b*) of the UK Computer Misuse Act, 2013, and came about as a result of recommendations during the review of the Bill during the consultation phase. If the Committee accepts this proposal, the following clause may be used: "**2.** (1) Any person who unlawfully and intentionally— *(a)* overcomes any protection measure which is intended to prevent access to; and *(b)* thereafter accesses, data, a computer program, a computer

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			data storage medium, a computer system, is guilty of an offence. (2) For purposes of this section— (*a*) "**protection measures**" means any measure that restricts access to data, a computer program, a computer data storage medium and a computer system; and (*b*) "**access**" means to make use of data, a computer program, a computer data storage medium or a computer system.".
	3.2.2 Deloitte - page 2	3.2.2 The clause does not provide for instances where an individual may gain access and misuse another individual's data or device negligently versus the intentional misuse by an unauthorised person.	3.2.2 Only intentional conduct is criminalised in terms of the Bill. Where a person foresees the possibility of the result occurring and the person reconcile himself or herself with this possibility even if he or she hopes that the result will not follow, intention in the form of *dolus eventualis* will be present.
	3.2.3 SAHRC - pages 3 and 4 (paragraph 3.2)	3.2.3 The SAHRC notes with concern the use of the term 'intentionally' in the clause 2(1) and highlights instances where the draft provision may have unintended consequences, among others, in respect of	3.2.3 The position of journalists is discussed under paragraph 3.1.12, above. Whistleblowers are protected to the extent provided for in the Protected

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		impact on investigative journalism and whistleblowers..	Disclosures Act, 2000 (Act 26 of 2000).
	3.2.4 Internet solutions - page 2 to 3 (paragraph 2.1.1)	3.2.4 The offence is extremely broad as it attempts to criminalise every unlawful electronic access as a cybercrime. As such, it should be relooked. (a) 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 unlawfully accessed with the intention of safeguarding/protecting it. It should rather read "unlawful access or unauthorised access" as compared to "unlawful securing of access." (b) Secondly, in attempting to define cybercrime, the "unlawful securing of access" in itself is broadly defined to criminalise a mere wrongful conduct into a cybercrime. It is submitted that the offences in clauses 2(2) to (3) lacks the essential cyber ingredients, which are instrumental in the technical 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 criminalisation of an unauthorised conduct as a cybercrime.	3.2.4 (a) The word "securing", must not be confused with the act of making safe. Securing access is defined as a state of affairs where the person will be in a position to use data, programs or devices. The clause is Based on the UK Computer Misuse Act that uses similar wording. (b) Most countries criminalise unlawful access as part of their cybercrime laws. It is submitted that the clause sets out the essential elements of this offence. The remark that wrongful conduct is elevated to a cybercrime is discussed under paragraph 3.1.7, above. The essential ingredient that is overlooked by the commentator is that such access must be unauthorised as is contemplated at the end of clause 2(2).

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(c) The clause is further criticised since it does not – (i) 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; and	(c)(i) The harm that the offence intends to address is unauthorised accessing. Similar to the common law offence of house breaking, which is in itself an offence" no further harm is required. If a person gains access to a computer that person is in a position to commit various further offences, similar to house breaking.
		(ii) specify whether unlawful securing of access should be temporary or permanent.	(ii) It is not necessary to specify that access must be permanent or temporary, since the mere act of obtaining access is criminalised.
		(iii) It is recommended that clause 2 should be deleted since 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.	(iii) The offences in clauses 3(1) (theft of data), 4(2) (possession of software and hardware tools to commit an offence), 5 (interference with data or programs) and 6 (system interference), does not address the gating offence of access, which opens the gate to commit the offences to which those clauses relate.
	3.2.5 ODAC - pages 1 to 3	3.2.5 The most important offences in the Bill is clauses 2 and 3. These offences relate to hacking. It is however recommended that these clauses be redrafted. The problem is the use of the phrase "unlawful" which is not	3.2.5 See discussion under paragraph 3.1.7, above, for a discussion of unlawfulness.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		defined. Unlawfulness has the connotation of contravening a proscription that prohibits something.	
	3.2.6 MNet - page 20 and 21 – (also see comment under clause 4)	3.2.6 (a) Clause 2, 3 and 4 may include daily actions by ordinary users. The problem is that the Bill does not define what constitute unlawfulness.	3.2.6 (a) Regarding unlawfulness, see discussion under paragraph 3.1.7, above. It is further submitted that unlawfulness cannot be defined for purposes of the Bill since new defences may be recognised by courts that exclude unlawfulness.
		(b) Software used for advertising, marketing purposes and for conducting research and analyses, may be unlawful. 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. Unlawful access of data, and the other offences should be linked to an intention to commit a serious offence. An example of this approach is contained in the Australian Cybercrime Act, 2001	(b) IT security experts performing pen testing, usually have the express or implied consent of a person that has authority to consent. Ethical hacking is still unlawful access and unless expressed or implied authority was obtained, it will be an offence. Division 477.1 of the Criminal Code of Australia deals with similar offences that are provided for in clause 11 of the Bill (access to commit a serious offence in respect of a serious offence). The less serious offence of access is dealt with in Division 487.1 that does not require the commission of a “serious offence”.
	3.2.7 SAFACT - page	3.2.7 Read with the POPI Act (and once POPIA is fully	3.2.7 This is a fallacious argument

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4	operational) this clause of the Bill will criminalise any access to data which goes beyond a person or entity's authority. It is submitted that, if a person or company does not have an individual's consent to use or store his/her data in a certain manner or for a certain purpose, as contemplated in POPIA, that person or company will be accessing his data unlawfully, as contemplated in clause 2 of the Bill. The Bill thus imposes potentially onerous obligations on electronic communications service providers, which are defined so wide that it will include any person or entity which transmits, receives, processes or stores data on behalf of any other person.	since clause 2 of the Bill intends to criminalise unlawful access, where a person does not have the authority to obtain such access. If a person or company use or store personal information in contravention of the POPIA, there is no unlawful access, since the data was obtained lawfully and is subject to the principles of lawful processing of personal information. However, where a company or person performs an unlawful and intentional act to secure access to data as is contemplated in clause 2, criminal liability may follow.
	3.2.8 Freedom of religion - paragraph 9.2	3.2.8 Clause 2 may have unintended consequences for ordinary Internet users, who through ignorance mishandles other people's data	3.2.8 Ordinary Internet users have access to publicly available data. Access is only prohibited to the extent that a user performs an action, in most instances by way of technical means, to put him or her in a position to, without authority access or use other person's data. It must be pointed out that a direct intention is required to commit the offence.
3.3 Clause 3: Unlawful	3.3.1 Cell C, Telkom and Vodacom -	3.3.1 Clause 3(1): This offence needs to be brought in line with the international position that criminalises the	The Department agrees with the proposal. The following amendment is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
acquiring of data	pages 9 to 13 (paragraphs 2.2.1.4.1 to 2.2.14.18)	"interception" of communications from or within a computer system". Although the current clause addresses this aspect, similar wording used by other legal systems and international instruments will facilitate international cooperation and will further facilitate the interpretation of the clause with reference to foreign judgments. Reference is made to current South African and foreign legislation dealing with this offence and regional and international instruments.	proposed: **Unlawful interception of data** **4.** (1) Any person who unlawfully and intentionally intercepts data within or which is transmitted from or to a computer system, is guilty of an offence. (2) Any person who unlawfully and intentionally possesses data, with the knowledge that such data was intercepted as contemplated in subsection (1), is guilty of an offence. (3) Any person who is found in possession of data, in regard to which there is a reasonable suspicion that such data was intercepted unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence. (4) For the purposes of subsection (1) "interception of data" means the use of technical means to acquire data stored within or which is transmitted to or from a computer system, including electromagnetic emissions from a computer system carrying such data.".

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	3.3.2 Cell C, Telkom and Vodacom - pages 9 to 13 (paragraph 2.2.1.5)	3.3.2 Clause 3(3): The Bill does not define a "satisfactory exculpatory account of possession", and may lead to undue arrests until the courts interpret the expression. It is proposed that this may be addressed through training and possibly the Standard Operating Procedures which should be issued in terms of clause 24 of the Bill.	3.3.2 It is submitted that the offences of possession of data, where there is a suspicion that it was acquired unlawfully and the subsequent failure to give an exculpatory account (meaning an account that exonerates or tends to exonerate the accused of guilt), will be interpreted in accordance with legal precedents that were developed around the interpretation of section 36 of the General Law Amendment Act, 1955 (Act 62 of 1955), that creates a similar offence. In terms of OSMAN AND ANOTHER v ATTORNEY-GENERAL, TRANSVAAL 1998 (2) SACR 493 (CC), the constitutionality of section 36 was considered and according to the court: * Section 36 does not compel a suspect to do anything, nor constituted pressure being applied on such person to make a statement. A person has a choice as to whether or not to provide an explanation for the possession of the goods. Persons are not prejudiced at the trial stage in the absence of an explanation, because they retained the express right to furnish an explanation

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			at the trial if no explanation had previously been given. The section therefore did not violate the right not to be compelled to make an admission or confession in s 25(2)(c) of the interim Constitution. * The right to remain silent and to be presumed innocent in s 25(3)(c) of the interim Constitution required (a) the State to bear the burden of proving each of the essential elements of the offence charged and there was no onus on the accused to disprove any of them; and (b) that the standard of proof was one of proof beyond reasonable doubt. * According to the court, it was the inability and not the failure or unwillingness to give a satisfactory account of possession that constituted the offence in section 36. * The court accordingly held that 36 did not violate any of the rights contained in section 25(2)(c) and (3)(c) of the interim Constitution.
	3.3.3 Michalsons Attorneys - page 6	3.3.3 Regarding clause 3(3), reference is made to S v Zuma 1995 (2) SA 642 (CC), where the Constitutional Court stated that not all statutory provisions that create a reverse onus are unconstitutional (because they	3.3.3 See paragraph 3.3.2. There is no reverse onus, regarding clause 3(3).

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		unjustifiably infringe on the presumption of innocence). The court will weigh up factors relating to the societal need for the successful prosecution of crime. The concern with reverse onuses is not whether the accused must prove or disprove an element but rather that reverse onuses can create a situation where the accused could be convicted where reasonable doubt exists. Where that probability exists, there is a breach of the presumption of innocence.	
	3.3.4 SAHRC - page 5 (paragraph 3.3)	3.3.4 The requirement of 'unable to give satisfactory exculpatory account', is a concern for the SAHRC, among others, where a person does not speak the same language as the inquiring party. The concern is also raised that the offence may involve an element of subjectivity in evaluating whether the account is satisfactory. The SAHRC recommends that a satisfactory exculpatory account be defined.	3.3.4 See paragraph 3.3.3, above. There is no need to define "satisfactory exculpable account", since it was already interpreted by the courts. The explanation must in light of the surrounding circumstances of the possession be a reasonable *bona fide* explanation that the possession is innocent (see among others S v AUBE 2007 (1) SACR 655 (W)).
	3.3.5 Mr Eatwell - page 10 (paragraph 46)	3.3.5 A reverse onus may lead to an injustice in the case where the law enforcement officers or persons responsible for the administration of justice are not trained and knowledgeable about this specific discipline	3.3.5 Noted.
	3.3.6 Internet Solutions - page 4 to 6 (paragraph 2.1.2)	3.3.6 * Section 3(2) and (3) criminalises anyone who knowingly, unlawfully and intentionally possesses data which was acquired unlawfully. Internet Solutions notes	3.3.6 See paragraph 3.1.12, above, regarding submissions that deals with a public interest defence in so far as it

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		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, they submit that the manner in which this clause is drafted fails to provide for public interest defences. It is further submitted that it restricts the right to access to information, since not all information that is published, is acquired lawfully. It is submitted that this clause restricts the role of the media and its contribution to the development of a democratic state. Investigative journalism will especially be hampered by such a clause. This clause is further criticised in that it will interfere with constitutional rights such as freedom of expression and it is submitted that a public interest defence is absolutely necessary. For this reason and with reference to judgments it is submitted that this provision may be unconstitutional as an unjustifiable limitation to the right to freedom of expression. It is further submitted that clause 3(3) imposes a reverse onus on the possessor of the information that may be unconstitutional.	relates to journalists.
	3.3.7 ODAC - pages 1 to 3	3.3.7 See comments from ODAC under clause 2 (paragraph 3.2.5), regarding the requirement of unlawfulness.	
3.4 Clause 4: Unlawful acts in respect of software and	3.4.1 Cell C, Telkom and Vodacom - page 14 (paragraph 2.2.1.6)	3.4.1 This offence criminalises the tools which are used to commit cybercrimes. It is recommended that training should be given to law enforcement to ensure that they are cognisant of the fact that this clause can only be	3.4.1 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
hardware tools		contravened when a specific intent, namely the use of the tools with the intention to commit an offence, need to be present.	
	3.4.2 Mr Eatwell - page 9 (paragraph 45.1)	3.4.2 The clause should be amended in order to ensure that the State must prove that the tools are used for unlawful purposes.	3.4.2 Clause 4 makes it clear that the use of tools is criminalised only if it is used or directly intended to be used to commit criminal offences.
	3.4.3 Internet Solutions - page 6 to 7	3.4.3 A concern is raised with the manner in which the clause is drafted and needs to be reconsidered. Internet Solutions indicates that they are against the offence as contemplated in clause 4(1). These tools should rather be criminalised through the conduct that is committed by use of these tools. Although clause 4(3) attempts to validate clause 4(1), ordinary laptops and the any various programmes that are available has dual functions and according to the author clauses 4(1) and 4(3) should be omitted from the Bill.	3.4.3 See paragraph 3.4.2 above. Clause 4(3), cannot be deleted since it specifically narrows the application of the clause down to tools that are designed or adapted primarily to commit various offences in terms of the Bill.
	3.4.4 ODAC - pages 3 to 4	3.4.4 IT security experts need the prohibited tools to ensure that computer systems are tested in order to protect it against vulnerabilities. This clause criminalises various conduct relating to such tools if it is used to commit an offence. This clause may criminalise the conduct of IT security experts who uses or manufactures such tools.	3.4.4 * During security testing operations IT experts may embark on operations that fall within the various proscriptions of Chapter 2 of the Bill. However, these actions will not attract criminal liability, due to the fact that such conduct is authorised, or is performed in circumstances of necessity and therefore not unlawful.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			*The concern against clause 4(1), that relates to the manufacturing of the tools is noted. If the tools are manufactured, used, possessed or distributed for a legitimate purpose, no criminal liability will follow. It must be taken into account that clause 4(1), also prohibits hardware devices that can be used for similar purposes such as skimming devices and devices that can intercept electronic emissions from a computer.
	3.4.5 MNet - page 20, (paragraph 6.1)	3.4.5 Software used for advertising, marketing purposes and for conducting research and analyses, may be unlawful in terms of this clause. Clause 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.	3.4.5 See paragraph 3.4.2, above. Where there is no intention to commit an offence, criminal liability will not follow.
	3.4.6 MNet – pages 1 to 8	3.4.6 The current focus of the Bill is on computer networks and appears to be narrower than sections 86 of 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	3.4.6 It is submitted that clause 4(1), read with clause (2), (unlawful access) and clause 3 (overcoming security measures and access data), precisely caters for this eventuality. It must however be stated that these clauses

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		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…" (page 1 to page 8)	are not intended to deal with copyright infringements.
	3.4.7 SAFACT - page 4	3.4.7 The developers and users of software that operates like cookies or other similar technologies used for advertising, research and analytics, will have to ensure that the software does not collect data beyond what it is authorised to do, or commit an offence	3.4.7 A cookie is the term given to describe a type of message that is given to a Web browser by a Web server. The main purpose of a cookie is to identify users and possibly prepare customised Web pages or to save site login information for the user. When the user enters a Web site using cookies, he or she may be asked to fill out a form providing personal information; like his or her name, email address, and interests. This information is packaged into a cookie and sent to the users' Web browser, which then stores the information for later use. The next time the user goes to the same Web site, his or her browser will send the cookie to the Web server. The message is sent back to the server each time the browser requests a page from the server. A Web server has no memory so the hosted Web site that is being

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			visited transfers a cookie file of the browser on the hard drive of the computer, so that the Web site can remember the user and his or her preferences. This message exchange allows the Web server to use this information to present customised Web pages. The recent tendency is to request specific permission for the use of cookies. If it is possible to use a cookie that falls within the proscriptions of Chapter 2 of the Bill an offence will be committed. **Proposed amendment** In order to address the concerns that is raised against clause 4(1), the following amendments to clause 4, is proposed: "**4. [(1) Any person who unlawfully and intentionally possesses, manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or hardware tool for the purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence.]**

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			[(2)](1) Any person who unlawfully and intentionally— (a) uses; or (b) possesses, any software or hardware tool for purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1) or 7(1)*(a)* or *(d)*, is guilty of an offence. **[(3)]**(2) …….". (In terms of the proposed amendment, in so far as it relates to the possession of the tools, the State wil have to prove that the tool was possessed for the specific purposes of committing an offence.)
3.5 Clause 5: Unlawful interference with data or computer program	3.5.1 Internet Solutions - page 7 (paragraph 2.1.4)	3.5.1 It is proposed that section 5 should include "intention to cause harm"	3.5.1 It is submitted that such an intention is part of the proscription, since "interference" is defined as to delete, alter, damage, or to render ineffective data or a program and the intention is directed to these actions.
3.6 Clause 6: Unlawful interference with data storage medium and computer systems	3.6.1 Cell C, Telkom and Vodacom - page 14 (paragraph 2.2.1.7) 3.6.2 MTN - page 4 (paragraph 2.3)	3.6.1 The offence is supported. 3.6.2 This clause may criminalise interference in the ordinary course of system maintenance, upgrades, testing, etc.	3.6.1 Noted. 3.6.2 It is difficult to see how these maintenance actions can be regarded as unlawful.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	3.6.3 Internet Solutions - page 7 (paragraph 2.1.5)	3.6.3 This conduct should only be criminalised if it causes serious impairment.	3.6.3 The *de minimus non curat lex* – principle applies in the South African law (see among others, S v SEWEYA 2004 (1) SACR 387 (T): "Clearly no definitive rule can be formulated to distinguish between trivial cases meriting criminal censure and trivial ones that can be excluded on the principle *de minimus non curat lex*. Thirion J expresses the view that the court 'has to some extent to pass a value judgment in regard to the reprehensibility of the offending conduct, viewed in the light of the principles of morality and conduct generally accepted as the norm in society'. The same view is expressed in LAWSA (op cit at para 280) where the learned authors express the view that: 'It is difficult to propound hard and fast rules for distinguishing the trivial cases of … from the serious ones. What is of a sufficiently serious character depends to a large extent on the modes of thought and conduct prevalent in a particular community at a particular time and in a particular place and is, in principle, determined by an objective test."
	3.6.4 IAB - paragraph 3.2	3.6.4 The definition of unlawfulness, among others, include 'permanently or temporarily altering any	3.6.4 See paragraph 3.1.7, above regarding the discussion of

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		resource of; or interrupt or impair (i) the functioning of; or (iv) the availability of a computer data storage medium or computer system'. Given the lack of clarity on what constitutes unlawful interference, this provision can give rise to inadvertent offences for interferences in the ordinary course of system maintenance, upgrades, testing.	unlawfulness. Unlawfulness in short means the absence of any defence recognised by law. It is submitted that "interference" is defined in clause 6(2) to mean any alteration, interruption or impairment of storage mediums and computers.
3.7 Clause 7: Offences relating to passwords, access codes and similar data or devices	3.7.1 Western Cape - page 1 of Annexure to letter	3.7.1 Items (i) and (ii) of subclause 7(3) are applicable to all the descriptions of what are considered as a password, access code or similar data or devices.	3.7.1 The intention with clause 7(3)(g), is to restrict the "word or string of characters or numbers" to the instances referred to in items (i) and (ii). The definition in subclause (3), does however not restrict "passwords, access codes or similar data and device" to the listed items in paragraphs (a) to (g) by virtue of the expression "without limitation" and is merely a description of what must be regarded as passwords, access codes etc.
	3.7.2 Cell C, Telkom and Vodacom - page 14 (paragraphs 2.2.1.8 and 2.2.1.9)	3.7.2 The offence is supported. This information is used to commit other cybercrimes. However, in respect of clause 7(2) it is remarked that the Bill does not define a "satisfactory exculpatory account of possession", and may lead to undue arrests until the courts interpret the expression. It is proposed that this may be addressed through training and possibly in the Standard Operating Procedures which should be issued in terms of clause 24 of the Bill	3.7.2 See the discussion under paragraph 3.3.2, above.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
3.8 Clause 8: Cyber Fraud	3.8.1 Cell C, Telkom and Vodacom - pages 14 to 15 (paragraphs 2.2.2.1.)	3.8.1 This offence is supported. This offence read with the other offences in the Bill will greatly facilitate the prosecution of traditional telecommunications fraud such as International Revenue Fraud, Wangiri fraud etc.	3.8.1 Noted.
3.9 Clause 9: Cyber forgery and uttering	3.9.1 Western Cape - page 1 of Annexure to letter	3.9.1 The words “passes off” in clause 9(2), is used in relation to unlawful competition and other words should be used.	3.9.1 The definition is substantially in line with the common law offence of forgery and uttering. In terms of the common law: (a) Any person who intentionally and unlawfully makes a false document to the actual or potential prejudice of another is guilty of the offence of forgery. (b) Any person who intentionally or unlawfully passes off a false document to the actual or potential prejudice of another is guilty of the offence of uttering.
	3.9.2 Cell C, Telkom and Vodacom - pages 14 to 15 (paragraphs 2.2.2.1 and 2.2.2.2)	3.9.2 The offence is supported and can be used for prosecuting the offence of phishing, where a false communication is submitted to a victim to lure the victim to provide his or her personal information.	3.9.2 Noted.
3.10 Clause 10: Cyber extortion	3.10.1 Cell C, Telkom and Vodacom - page 15 (paragraphs 2.2.2.3)	3.10.1 This offence is supported	3.10.1 Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	3.10.2 TBCSA - page 3 Item 2	3.10.2 Cyber extortion is not clearly defined.	3.10.2 The offence is substantially in line with the common law offence of extortion that consist of the following element – (a) the acquisition; (b) of a benefit, which may be of a patrimonial or non-patrimonial nature; (c) by applying pressure which induces the victim to hand over the advantage; (d) a causal link between the pressure and the acquisition of the benefit; (e) unlawfulness; and (d) intention. (Snyman, Criminal Law Fifth Edition, page 426) According to Snyman, page 427, the common law crime of extortion requires that the advantage must be handed over to the perpetrator before the act is complete. If the perpetrator is apprehended after the threat has been made but before the acquisition of the advantage, he or she can only be convicted of attempted extortion. Unlike the common law offence of extortion, the pressure element in terms

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			of this clause consists of threat to commit an offence or commit an offence to move a person to hand over an advantage or to compel a person to perform or abstain from performing an act. The clause does not require that the advantage must be handed over to complete the offence. A real life example of computer-related extortion is where a cybercriminal encrypts the whole database of a hospital and then asking for payment of Bitcoins to provide the decryption key.
3.11 Clause 11: Aggravated Offences	3.11 Cell C, Telkom and Vodacom - page 15 (paragraphs 2.2.3.1)	3.11 There is a need to create aggravated cyber offences, and the clause is supported. However, a consultative process in terms of clause 57 needs to be followed before the declaration of critical information infrastructures	3.11 Noted. However, the following amendments are proposed: (a) Clause 11(1): (i) The offences should be intended to affect a restricted computer system; and (ii) a restricted computer system should be restricted to a critical information infrastructure. (b) Clause 11(2): A specific intention to cause the results in paragraph (a) to (g) should be a requirement of the offence
3.12 Clause 13: Theft of an incorporeal	3.12.1 Western Cape - page 2 of Annexure to letter	3.12.1 "incorporeal" is an adjective and the word "property" should be inserted after incorporeal.	3.12.1 The term aims to denote something that is intangible, non-material non-physical and is usually a right which a person has either in

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			respect of corporeal property or intangible property. However it can also be the intangible property itself (a newly developed computer operating system of which the only copy is stored on a computer may be copied and the original may be deleted). Various terminologies have been used to describe intangible objects - incorporeal rights, incorporeal things, incorporeal assets and incorporeals. As long as there is a clear understanding that incorporeal includes an incorporeal *res* as well as rights pertaining to corporeal and incorporeal thing, there would be no objection to include the word "property" after the word "incorporeal". Proposed amendment: "The common law offence of theft must be interpreted so as not to exclude the theft of **[an]** incorporeal property or things.".
	3.12.2 Cell C, Telkom and Vodacom - page 15 (paragraphs 2.2.4.1)	3.12.2 This clause is welcomed.	3.12.2 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
3.13 Clause 14: Penalties	3.13.1 South African Communications Forum - page 2 (paragraph 12.)	3.13.1 The penalties should be proportionate to the magnitude of the impact of the crime. The penalties in clause 14 are not proportionate to the magnitude of the impact of cybercrime and should be increased to be a deterrent.	3.13.1 It is submitted that although cybercrime is extensive, the penalties are adequate and proportionate to the offences provided for in Chapter 2 of the Bill.
	3.13.2 Cell C, Telkom and Vodacom - page 15 (paragraphs 2.2.3.1)	3.13.2 The penalties are supported. However, the stipulation of a maximum penalty might act as an additional deterrent.	3.13.2 Clause 14 prescribes maximum penalties. Although a fine is not prescribed the Adjustment of Fines Act, 1991 (Act 101 of 1991), will be

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			applicable. In terms of this Act a magistrate's court may in accordance with the current determination in terms of section 92(1)(*b*) of the Magistrates' Courts Act, 1944 (Act 32 of 1944), impose a fine of R120 000, for each year of a sentence that is prescribed. A regional court may impose a fine of R300 000 for each year of a sentence that is prescribed. A High Court may impose any fine and is not limited by the application of that Act. The Bill also amends the Criminal Law Amendment Act, 1997 (Act 105 of 1997), in order to provide for enhanced penalties in respect of contraventions of clauses 8, 9, 10 and 11(2) of the Bill which among others deal with cyber fraud, cyber forgery and uttering, cyber extortion and aggravating offences that involves life and limb situations.
	3.13.3 Cell C, Telkom and Vodacom - page 15 (paragraphs 2.2.3.1)	3.13.3 It is proposed that it must specifically be stated that a contravention of section 12 shall attract sanctions of equal severity as the fines and imprisonment prescribed in clause 14.	3.13.3 Clause 12 deals with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence, as contemplated in Chapter 2. Clause 12 already provides that a person who is convicted in terms of the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			clause is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.
	3.13.4 Jamie Band	3.13.4 Clause 14(1): Hackers tend to be teenagers or young adults who engage in the activity out of pure curiosity. Most are ignorant and do not necessarily mean harm by it. To lock such a person up for five years is simply too harsh. Realistically, it should be no more than two to three years.	3.13.4 This was taken into account when the Bill was drafted. The Child Justice Act, 2008 (Act 75 of 2008), will be applicable with its various options to deal with children, who are in conflict with the law. Schedules 2 and 3 to the Child Justice Act, is further amended in the Schedule to the Bill. In terms of section 77(3) of the Act, a child who is 14 years or older at the time of being sentenced for the offence may only be sentenced to imprisonment, if the child is convicted of an offence referred to in - * Schedule 2, if substantial and compelling reasons exist for imposing a sentence of imprisonment; and * Schedule 3. The amendments to these Schedules are in line with other current offences in these Schedules.
	3.13.5 Jamie Band	3.13.5 Clause 14(2): Ten years is too harsh for unlawful	3.13.5 Cognisance must be taken of the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		acquisition of data. What of the Gupta emails? The person who exposed these emails did so for the public good. With such harsh sentences, it will discourage whistle blowers from exposing Government and commercial corruption.	fact that a crime was committed. Other factors can be raised in mitigation of to reduce a sentence. In this regard we refer to case law in support (see among others S v KEARNS 1999 (2) SACR 660 (SCA) at 663g – h and S v TRUYENS 2012 (1) SACR 79 (SCA)).
	3.13.6 Jamie Band	3.13.6 Clause 14(3): Hacking is dealt with in clause 2(1). There is no need to have a separate section outlining even harsher penalties because the target happens to be a Government entity. Fifteen years is excessive and is not proportional to the crime. Section 11(1) should be removed.	3.13.6 The offence in clause 11(1) aims to protect critical objectives where cybercrime may have a substantial impact on society, the economy, public administration or economic interests.
	3.13.7 TBCSA - page 3 (Item 2)	3.13.7 Clause 14(5): Attorney fees and litigation suffered by businesses; cybersecurity improvements that should be carried out as a result of the offence committed against businesses; the rand value of operational disruption; reputational damage/damage on brand and company name, which may have affected profitability, etc, should also be taken into account	3.13.7 The resultant damage caused by any crime is taken into account during the imposition of a sentence.
	3.13.8 SAHRC - page 5 (paragraph 3.3)	3.13.8 The SAHRC is of the opinion (with reference to the offences in clauses 2, 3 and 5), that mitigating factors should also be included which must be taken into account in imposing a sentence.	3.13.8 Factors that should be considered during sentencing have been developed comprehensively by the courts and must be considered during sentencing. It is best left to the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			courts to consider these on a case by case basis.
3.14 Clause 15: Competent verdicts	3.14. Cell C, Telkom and Vodacom - page 15 (paragraph 2.2.3.1)	3.14.1 This clause is supported.	3.14. Noted.
4. CHAPTER 3: MALICIOUS COMMUNICATIONS			
4.1 General	4.1.1 All Rise - page 3 (paragraph 10)	4.1.1 For the purposes of the malicious communications provisions, it is recommended that providers of blogging and social networking services be included within the definition of electronic communications service providers and not only licensed entities, since malicious communications may be distributed through these providers.	4.1.1 2.6.1 It is submitted that clauses 19, 20 and 21 of the Bill, includes providers of blogging and social networking services as a result of the phrase “persons in control of a computer system”.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.1.2 MediaMonitoring: Africa - page 12 (paragraph 24)	4.1.2 The protection of the best interests of the child in cybercrimes and cybersecurity should specifically be acknowledged. It is proposed that provisions which deals with the protection of children must be included in clauses 16 to 18 of the Bill. Alternatively, provisions should be inserted that criminalises exposure of children to pornography, the use of technology to groom and exploit children, and the need to develop appropriate *curricula.*	4.1.2 These clauses also aim to protect children. The Bill, in the Schedule, also amends the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, to deal with instances of child pornography and harmful disclosure of pornography. Grooming and exposure of children to pornography are already catered for in the SOA.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.1.3 MediaMonitoring: Africa - page 12 (paragraph 24)	4.1.3 The Bill is criticised in that there is limited reference to information rights, including the constitutional right to freedom of expression. A concern is also raised that the Bill does not adequately acknowledge that information rights are equally as applicable online as they are offline, a position recently restated by the United Nations Human Rights Council. It is submitted that information rights, and their applicability in the cybercrimes and cybersecurity framework, need to be properly considered in the Bill.	4.1.3 Information rights relates to rights and obligations relating, among others, to communication, collection, access, use and control of data and include among others, the right to privacy, intellectual property access to information and freedom of expression. This has been adequately dealt with in the Bill.
	4.1.4 MediaMonitoring: Africa - pages 12 to 13 (paragraph 26); ODAC - page 4; Centre for Constitutional Rights - page 6 (paragraph 10.2)	4.1.4 A concern is raised regarding unintended consequences which may result from the provisions of clauses 16, 17 and 18 on the enjoyment of freedom of expression and it is proposed that it be carefully and narrowly drafted to avoid ambiguity. The necessity of this Chapter is also challenged.	4.1.4 From the perspective of unintended consequences and necessity, the following must be taken into account: Malicious communications may well infringe some basic human rights. The Constitution imposes a duty on the State not to perform any act that infringes the entrenched rights such the right to life, human dignity, and freedom and security of the person. Section 16 of the Constitution provides that everyone has the right to freedom of expression, which includes, among others, freedom to receive or impart information and freedom of artistic creativity. However, this right does not extend to incitement of imminent violence or advocacy of hatred based

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			on race, ethnicity, gender, religion and any action that constitutes incitement to cause harm. This means that the right of the person to exercise artistic creativity and other constitutional entrenched rights on the Internet will have to be weighed against the victim's rights to privacy and dignity. It is submitted that a person's dignity is impaired and or when he or she is treated in a cruel, inhumane or degrading way. Malicious communications has the potential to affect the physical, psychological and emotional integrity of the cyber victim. To illustrate this, malicious communications may cause the cyber victim to experience fear, feelings of depression, low self-esteem, social anxiety and suicidal tendencies and usually have real life consequences. The psychological impact of malicious communications is also regarded to be more traumatising than physical abuse because of the public and online nature of the bullying where an infinite number of persons may read the malicious communication. It is submitted that malicious communications has the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			potential to infringe various human rights such as the right to freedom of expression, right to dignity, right to bodily and psychological integrity and right to privacy. The Department is of the view that there is an appropriate balance between the right to freedom of expression and the rights to privacy, human dignity and bodily and psychological integrity. All rights in the Constitution are subject to the limitation clause in terms of section 36. It is submitted that the infringement on these rights are necessary and proportional to the extent of the infringement. To this end, legislation should be enacted to adequately protect the rights of online users and to promote tolerance and respect for diverse opinions in a fair manner. The European Court of Human Rights, in K.U. v. FINLAND AND PERRIN V. THE UNITED KINGDOM, has recognised that freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			expression will be respected. However, it was also pronounced that such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. In SOUTH AFRICAN NATIONAL DEFENCE UNION v MINISTER OF DEFENCE AND ANOTHER, the importance of the right to freedom of expression protected in section 16 of the Bill of Rights was emphasised when this court held that: "Freedom of expression lies at the heart of democracy. It is valuable for many reasons, including its instrumental function as a guarantor of democracy, its implicit recognition and protection of the moral agency of individuals in our society and its facilitation of the search for truth by individuals and society generally. The Constitution recognises that individuals in our society need to be able to hear, form and express opinions freely on a wide range of matters.". This aspect was also dealt with in SOUTH AFRICAN BROADCASTING CORP LTD v NATIONAL DIRECTOR OF

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			PUBLIC PROSECUTIONS AND OTHERS 2007 (1) SACR 408 (CC). Like any other right in the Bill of Rights, the right to freedom of expression may be limited. In circumstances where the right competes with other rights in the Bill of Rights, its limitation may be justified. However, that justification has to be subject to the Constitution - ISLAMIC UNITY CONVENTION V INDEPENDENT BROADCASTING AUTHORITY AND OTHERS, 1998 (2) SA 1143 (CC) (1998 (4) BCLR 415) (paragraph 7). For instances where the right was limited see, DE REUCK v DIRECTOR OF PUBLIC PROSECUTIONS, WITWATERSRAND LOCAL DIVISION, AND OTHERS 2003 (2) SACR 445 (CC) – (child pornography); PHILLIPS AND ANOTHER v DIRECTOR OF PUBLIC PROSECUTIONS, WITWATERSRAND LOCAL DIVISION, AND OTHERS 2003 (1) SACR 425 (CC) (paragraph [17] – 'repulsive, degrading, offensive or unacceptable' conduct to the extent that the limitation was justifiable in 'an open and democratic society based on human dignity, equality and freedom' *in*

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			casu selling liquor at a strip club). Clause 18 is not criticised but generally welcomed by commentators. * Section 22 of the SADC Model Law proposes the criminalisation of the conduct of a person, who initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behaviour. Also see section 18 of the HIPCAR Model Law, the UK Malicious Communications Act, 1988, the Australian Criminal Code Division 474.15 (threats to kill and threats of serious harm) and 474.17 (menacing, harassing or offensive communications)

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.1.5 MediaMonitoring: Africa - pages 5 and 17 (paragraphs 41	4.1.5 There is a need to provide for the disclosure of malicious communications in the public interest. The Bill makes no reference to communications, intentionally made available, broadcast, or distributed which are in	4.1.5 See paragraph 3.1.12, above. A public interest defence in relation to criminal offences has not yet been recognised by our courts. It submitted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	and 42)	the public interest, the interest of justice, or already in the public domain. The chilling effect of this omission is that journalists or human rights defenders who publish malicious communications, which may be in the public interest or in the interest of justice, are still criminally liable in terms of the Bill. To enable the protection and promotion of the right to freedom of expression, the Bill should include a public interest defence to malicious communications, which will ensure that public officials and powerful individuals can be held accountable by members of the media and human rights defenders.	that the Bill cannot deal with such a defence since it must apply to all criminal conduct.
	4.1.6 Legal Aid SA - page 4	4.1.6 There was a failed attempt to deal with cyber harassment, bullying and revenge pornography in the Films and Publications Amendment Bill and was merely copied in the Bill.	4.1.6 The offences in the Bill dealing with malicious communications are substantially different from the offences in the Films and Publications Amendment Bill.
	4.1.7 All Rise - pages 1 and 2 (paragraphs 2 to 4)	4.1.7 40% of the world population use the Internet, which equates 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 six times. 38% had suffered cyber abuse themselves. There are evident concerns that cyber abuse, which encompasses cyberbullying, cyber-trolling, cyber	4.1.7 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		harassment and cyber-stalking, are on the rise.	
	4.1.8 All Rise - page 2 (paragraph 5)	4.1.8 Many countries across the world are recognizing the need to address cyber abuse related crime. Although the criminal conduct covered by the Bill is already unlawful under existing laws, the offence in the Bill, not only consolidate and strengthen the law in this area, but also sends a strong signal that tackling cybercrime is a priority for the country.	4.1.8 Noted.
	4.1.9 All Rise - page 2 to 3 (paragraph 6)	4.1.9 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 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.	4.1.9 The Bill substantially increases jurisdiction in respect of cybercrimes, and provision is made for agreements with other countries to curb cybercrime, which includes malicious communications. Unlike the Protection of Harassment Act that relies on a civil remedy, the fact that malicious communications are criminalised may ensure international co-operation in respect of the offences in question. The comprehensive research of the UK Law Reform Commission at page 109 (paragraph 2.227 also suggested that extra territorial jurisdiction is necessary. Hover, it is submitted that the procedures in terms of clauses 19, 20 and 21 will in most instances only have national application.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.1.10 All Rise - page 3 (paragraphs 7 to 9)	4.1.10 Electronic communications service providers are a critical part of the solution, with cybercrime happening via their networks. The introduction of formal obligations for all service providers including blogging and social networking service providers, to assist, rather than relying on goodwill is supported.	4.1.10 Noted.
	4.1.11 Internet Solutions - page 8 (paragraph 2.1.6)	4.1.11 The opinion is held that section 16 and 17 should not form part of the Bill since it is not offences committed against computer systems. It is further submitted that this type of crime is already criminalised in South African law and is merely recriminalised with reference that it is committed by means of a computer system. It is further submitted that such malicious communications can be prosecuted in terms of the provisions of the Hate Crimes Bill and the provisions are more appropriate to the Hate Crimes Bill.	4.1.11 It is submitted that the offences primarily aim to address the proliferation and effects of the use of computer systems to harm or treat persons in a cruel, inhumane and degrading manner and to address cyber bullying. The fact that there may be overlaps with other laws on the Statute Book is discussed under paragraph 4.1.4. It is submitted that the Hate Crimes Bill does not address the conduct provided for in clauses 16 and 17, since the ambit of that Bill is to criminalise conduct that relates to racism, racial discrimination, xenophobia and related intolerances. Hate speech is dealt with in clause 4 of that Bill and is limited to communications based on grounds such as race, gender, intersex, ethnic or social origin, colour, sexual orientation, religion, belief culture, language. These

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			offences fall outside the ambit of clauses 16 and 17 of this Bill.
	4.1.12 R2K - page 5	4.1.12 Protecting freedom of expression online is a challenge in an environment where patriarchy, racism, hatred and toxicity thrive. However, Chapter 3 of the Bill creates a legal framework that is wide open to abuse, especially viewing the full scope of how the Bill defines what messages are considered harmful. This appears to be Government's proposal to 'regulate' social media.	4.1.12 See paragraph 4.1.4, above. It is submitted that these provisions cannot be interpreted as to give powers to Government to regulate the social media. Offences that flow from these provisions are subject to a criminal process that is constitutional and offences must be interpreted within the ambit of the Bill of Rights and its limitations. Clauses 19, 20 and 21, by implication only apply if a criminal charge is laid with the SAPS (clause 20(1)). Affected persons or electronic communications service providers may apply to a court to set aside a protection order (clause 20(6)). The order of court is subject to appeal or review (clause 20(11)). It is submitted that Chapter 3 does not give powers to the State to regulate social media or in an unjustifiable manner to infringe on the right of privacy or freedom of expression.
	4.1.13 R2k - page 7	4.1.13 The Bill makes it a crime to resend malicious communications even if the re-sender is not the author.	4.1.13 The resending of harmful digital communications must not be treated as

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		This does not take into account the intention of the re-sender.	an exception to the prohibition. In most instances the resending of malicious communications contributes to the problem that this Chapter of the Bill aims to address.
	4.1.14 R2K - page 8	4.1.14 It is proposed that the Chapter be revised and that all clauses that deal with malicious communications except the clause that deals with revenge pornography be omitted from the Bill. It is stated that there are already mechanisms to combat malicious communication. In many cases, these mechanisms have been weakened by poor implementation and a justice system that fails the poor and marginalised, especially women. The solution is not to pile on new, heavy-handed criminal penalties, but to invest in creating a more just and responsive justice system.	4.1.14. As is pointed out in paragraph 4.1.4, the elements of the offences are substantially similar to offences already on the Statute Book and the challenge of the constitutionality of the provisions in question is therefore without basis. Regarding other mechanisms, other than criminal offences, it is correct that the Protection from Harassment Act may be used to address malicious communications, where a protection order may be acquired against a perpetrator not to harass the victim. However, in the context of the Internet, if harmful communications are made available it stays on the Internet and may be redistributed over and over. The coverage that such communications received may therefore be unlimited and the harm caused thereby may be extensive. Take down orders in terms of section 77 of the ECTA, is not very effective and does not provide for

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			checks and balances as is provided for in Chapter 3 of this Bill, where a court order is necessary to take down, which is in itself subject to appeal or review.
4.2 Section 16: Data message which incites damage to property or violence	4.2.1 Cell C, Telkom and Vodacom - page 16 (paragraphs 2.3.1) 4.2.2 R2K - pages 5 to 6; ODAC - pages 4 to 5	4.2.1 Clause 16 should be weighed up against an individual's right to freedom of speech and expression. 4.2.2 It is desirable that people should not threaten each other with violence and damage to property. However, laws that prohibit free speech should be rejected because it could possibly cause harm. Rather than create a chilling threat to freedom of speech, which could include hyperbolic or satirical speech, criminal penalties should only apply to demonstrable harm done. The Riotous Assembly Act and Intimidation Act already	4.2.1 See paragraph 4.1.4, above 4.2.2 See paragraph 4.1.4 above

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		deal with the offences in question. The mere resending of a message which falls within the prohibition may lead to criminal liability. ODAC argues that clause 16 may be unconstitutional. ODAC again raised the same objection as is discussed under clause 2 in relation to the use of the word "unlawful".	
	4.2.3 Centre for Constitutional Rights - page 6 (paragraph 10.3)	4.2.3 Clause 16 specifically refers to a broad manner that a data message can be sent to a specific person or to the general public by referring to terminology such as "making available", "broadcast" or "distribute" which is not defined in the Bill. The definition of a "data message" conflicts with the definition used in the Hate Crimes Bill and it is not clear to the public what conduct in terms of these proposed Bills are, as a matter of fact, prohibited.	4.2.3 The broad ambit of the application of the clause is restricted by the fault element of "intention to incite" the conduct provided for in paragraphs (a) and (b) of clause 16. It is not necessary to define the terminology of "makes available, broadcasts or distributes". The meaning of these words is evident and must be interpreted in accordance with their ordinary understanding in so far as it relates to electronic communications.
	4.2.4 Centre for Constitutional Rights - page 6 (paragraph 10.4); SAHRC - page 6 (paragraph 3.4); Freedom of Religion SA - paragraph 6.1	4.2.4 Clause 16(*b*) specifically states that if this data message is made with the "intention to incite...violence against a person or group of persons", a person will be guilty of an offence. It has to be reiterated that section 16(2) of the Constitution specifically refers to "incitement of imminent violence" and not just "violence" which is not only not defined but is also glaringly vague. The reference to "incitement to imminent violence" appears to originate from the United States' Supreme Court	4.2.4 The Department is of the view that the clause is constitutionally aligned, but will propose an amendment to correct an omission in the draft Bill, as follows: Proposed amendment: Drafting error: "**16.** Any person who

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		matter of *Brandeburg v Ohio* which emphasised that this expression "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action". It is submitted that if an offence is to be created in this instance, it must be constitutionally aligned.	unlawfully and intentionally ……".
4.3 Section 17: Data message which is harmful	4.3.1 ODAC - pages 5 to 6	4.3.1 Cyber bullying can be addressed by means of other legislation already on the Statute Book, among others, PEPUDA, assault, Protection from Harassment Act, etc. In many American States bullying must be dealt with at school level. This may be an appropriate way to deal with this aspect.	4.3.1 It is acknowledged that other legislation may be used to address aspects that are dealt with in clause 17. The Protection from Harassment Act, however, provides a civil remedy *ex post facto* after the initial harassment that prohibits the harasser not to continue with the harassing act. However, the nature and effect of cyber harassment is that a single act of "harassment" can cause irreparable harm to a victim. The discussions in paragraph 4.1.4 and 4.2.4, are equally applicable to the offences referred to in clause 17(1) read with clause 17(*a*) and (*b*). The reference to the USA position is incorrect. According to available information all States have laws in place

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			that deal with bullying and legislation of 23 of these States deal with cyber bullying. 18 States criminalise cyber bullying. The Most recent investigation relating to cyber bullying is the UK Law Reform Commission Report, which at pages 5 to 6 (paragraph 24)has the following to say in respect of cyberstalking: "… developments in Scotland and England and Wales where specific stalking offences were introduced in 2010 and 2012 respectively. The experiences of these jurisdictions strongly suggest that the introduction of specific stalking offences led to an increase in reporting and prosecution of stalking. Specifically naming stalking as an offence also carries great significance for victims of stalking, because of the "hidden" nature of the crime as well as its aggravated nature compared to harassment. The Commission therefore recommends that a specific stalking offence should be enacted." (The UK Harassment legislation requires repeated, unwanted contact, whilst the Harassment Act requires a single act of harassment.)
	4.3.2 Deloitte - page 2	4.3.2 Clause 17(2)(*d*): It is proposed that the requirement of the data message being false in nature	4.3.2 The aim of the additional elements is to restrict the ambit of the false

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		should be sufficient for the data message to be harmful and the remainder of the elements should not be required.	communication to those that causes mental, psychological, physical or economic harm to an identified person or group of persons.
	4.3.3 MediaMonitoring: Africa - page 12 (paragraph 25)	4.3.3 With regard to clause 17(2)(*a*)(i), the reference to "any property" does not consider the possible different thresholds for movable, immovable, and, increasingly, virtual property such as one's brand or intellectual property online.	4.3.3 It is submitted that property means all corporeal and incorporeal property (such as the defacement of a website).
	4.3.4 MediaMonitoring: Africa - page 12 (paragraph 25)	4.3.4 It is proposed that the word "imminent" should be inserted before all references to violence in subclauses 17(2)(*a*) and (*b*).	4.3.4 See paragraph 4.1.4 and 4.2.4, above.
	4.3.5 MediaMonitoring: Africa - page 12 (paragraph 26)	4.3.5 The words "intimidates, encourages or harasses" should be replaced by the word "incites" to bring it in line with other legislation.	4.3.5 The Department disagrees. This will change meaning of the terminology used.
	4.3.6 All Rise - page 3 (paragraphs 11 and 12)	4.3.6 Cyber harassment as a specific offence is supported. However, it may be useful to extend it to offline conduct as well, in order to comprehensively criminalise harassment.	4.3.6 The ambit of the Bill is mainly to address conduct in cyber space.
	4.3.7 All Rise - pages 3 and 4 (paragraph 13)	4.3.7 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	4.3.7 Intention is an element of criminal liability and cannot be dispensed with. The reasonable person test is to restrict

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		harm (intent) and (ii) that a reasonable person would regard the message to be harmful. The inclusion of an intent requirement whereby perpetrators can argue that they did not have the intention 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 while pleading it wasn't their intent to pull the trigger." The reasonable person test alone is sufficient and a well-established and understood concept that is more than sufficient to ensure fairness. It is recommended that the aforementioned intent requirement should be deleted.	the ambit of the clause.
	4.3.8 Centre for Constitutional Rights - page 7 (paragraphs 1.5 to 10.10)	4.3.8 Clause 17 of the Bill is criticised on the basis of vagueness. According to the comment: (a) Clause 17(1) specifically stipulates that a person will be guilty of an offence if a data message which is "harmful" is "unlawfully" and "intentionally" (again vaguely) made "available", "broadcast" or "distributed". The term "harmful" is not used in the Harassment Act. The Harassment Act specifically refers to "harm" which is defined as "any mental, psychological, physical or economic harm". The term "harmful" is specifically used in section 10 of the Equality Act in relation to the prohibition of hate speech which includes "communication based on the prohibited grounds which is harmful". "Harmful" is not defined in the Equality Act and what clause 17(2)(*a*) to (*d*) essentially does, is to create vague instances when such data messages will	4.3.8 (a) Unlawfulness and intention are essential elements for liability in accordance with the criminal law of South Africa. There is no need to define these concepts. The concept of "harmful" is defined in clause 17(2), which specifically prescribes when a data message must be considered as harmful, namely when it falls within the ambit of paragraphs (*a*) to (*d*) of that subclause. If a word or concept is not defined in legislation the rule is that it must be understood in its ordinary meaning within the context that it is being used. The objective criteria, which is according to the commentator absent

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		be considered "harmful" and then be guilty of an offence. Not only is reference made to undefined terminology such as "to threaten with violence" or to "intimidate" a person but it also states that "harmful" includes a data message which is "inherently false in nature and is aimed at causing mental, psychological, physical harm". - No definition is provided for "inherently false" data and what objective criteria would be applied in this instance to determine if it would fall within this category. It appears that this specific sub-provision was drafted considering the fear of 'fake news'. In this instance, it is emphasised that there already exist remedies available to a person, namely the common law crime of *crimen injuria* and defamation.	from this clause to evaluate a harmful communication can be found in the closing paragraph of clause 17(2), that requires that the conduct in paragraphs (a) to (d) must be evaluated from the perspective of a "reasonable person in possession of the same information and with regard to all the circumstances".
		(b) Clause 17 is also silent on defences available to an accused in this instance.	(b) The general principles of criminal law would apply. In this regard there are no numerous defences that would be available to the accused. If specific defences are provided for it will limit the grounds of justification and may operate unfavourably towards an accused person.
	4.3.9 MediaMonitoring: Africa - pages 12 to 13 (paragraphs 27 and 29); R2K - pages	4.3.9 Section 17(2)(*d*), is an unjustifiable limitation of free speech in so far as it criminalises the distribution of a harmful data message that is inherently false in nature. This conduct is criminalised online but is not criminalised offline and creates disunity between criminal laws in	4.3.9 The mere distribution of fake news is not criminalised. What this clause aims to protect is the result of such communications. A false data message will only fall within the proscription if it is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	6 to 7; Freedom of Religion - paragraph 6.5	online and offline spaces. It appears that this provision aims to address 'fake news', and as such would be a severe limitation on the right to freedom of expression, and would arguably not be justifiable under section 36 of the Constitution whether applied online or offline. It is suggested that this clause be omitted from the Bill	aimed at causing mental, psychological, physical or economic harm to a person or a group of persons. Furthermore, this proscription is subject to a limitation, namely that "a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful". The proposed offence in the Bill requires that the distributor of the communication must know of the falsehood of the communication and that it is distributed to cause harm. The clause was not intended to deal with fake news, being disinformation or wrong conclusions that drawn from a fact of circumstances.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.3.10 Cell C, Telkom and Vodacom - page 16 (paragraph 2.3.2 and 2.3.3)	4.3.10 Although the Protection of Harassment Act, 2011 was put on the Statute Book to comprehensively deal with harassment in the real and virtual world, many countries have recognised the seriousness of cyber harassment and have enacted specific laws which criminalise such communications. Cyber harassment is currently not recognised as a specific category of conduct in terms of the South African law and should be criminalised. This clause is supported.	4.3.10 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.3.11 Michalsons Attorneys - page 8	4.3.11 Clause 17(2)(*d*), potentially criminalises satire, parody or artistic or other works that are intended to be used as political commentary. It is proposed that a defence be included to cater for the aforementioned.	4.3.11 There are no closed categories of grounds of justification in SA law that will lift the unlawfulness of prohibited conduct. In any event, it is submitted that the limitation test of a reasonable person in possession of the same information and with regard to all circumstances implies that any ground of justification which will justify conduct that complies with the proscription, must be taken into account. Possible defences may include (a) truth that is in public interest and (b) reasonable comment. In any event the offence in question has similarities with criminal defamation and *crimen iniuria*, where the ambit of the offences and grounds of justification was already extensively interpreted by the court. False allegations may fall within the ambit of both these offences. The use of the words "inherently false in nature" further qualifies the ambit of this offence.
	4.3.12 R2K - page 6; Freedom of Religion - paragraphs 6.4.1 and 6.4.2	4.3.12 The intention to protect vulnerable people from harassment online is appreciated but this could also have a chilling effect on freedom of expression, which includes robust political expression that is often crude, aggressive and unpleasant. In any case, such	4.3.12 See in general paragraph 4.1.4. As was already pointed out the Protection of Harassment Act is a civil remedy *ex post facto*, meaning that the harm was already done. The fact that

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		communication should be dealt with in the Protection from Harassment Act, which allows for a protection order against harassment. Additional criminal penalties to deal with this type of communications are not necessary.	other remedies of a civil nature may be available to deal with malicious communications (which is similar to defamation) was considered in S v MOTSEPE 2015 (2) SACR 125 (GP) at paragraph [47] where reference is made to foreign decisions where the courts found as follows: * "Although it is important to recognise the right of the person defamed to sue for monetary damages it is equally if not more important that society discourage the intentional publication of lies calculated to expose another individual to hatred and contempt. . . . Defamatory libel can cause long-lasting or permanent injuries to the victim. The victim may forever be demeaned and diminished in the eyes of her community. . . . The harm that acts of criminal libel can cause is so grievous and the object of the section to protect the reputation of individuals is so meritorious that the criminal offence is of such importance that the offence should be maintained.' - (R v Lucas [1998] 1 SCR 439 ((1998) 50 CRR (2d) 69 (SCC)) para 73.])
	4.3.13 SAHRC - page 7	4.3.13 (a) The SAHRC welcomes the intention of the clause. However, it requests clarity on what the	4.3.13 (a) Fake news is addressed in paragraph 4.3.9. It is correct that fake

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		implications may be for publication of 'fake news', which may not always necessarily be considered as 'harmful,' yet could have several implications in misleading the public.	news may not always cause harm as is contemplated in clause 17(2)(*d*). It is submitted that if the ambit of the operation of the clause is to be extended to cover the sending of misleading information, which does not cause harm, the clause may then be regarded as unconstitutional.
		(b) The SAHRC further notes the inclusion of the 'reasonable person' standard in assessing the degree of harmfulness i.e. a *reasonable person* in possession of the same information and with regard to all the circumstances would regard the data message as *harmful*" (emphasis added). The SAHRC however recommends that in order to fully establish a reasonable person standard in the Bill, reference ought to be made to the context in which a data message may have been sent.	(b) The words "all circumstances" will include the context within which the data message was sent.
	4.3.14 Freedom of Religion - paragraphs 6.5 to 6.7	4.3.14 (a) Clause 17(2)(d) – The expression "inherently false in nature" is not defined and is open to multiple interpretations and subject to what a person believes.	4.3.14 (a) There is no need to define words that have an ordinary meaning, which is not being changed in this proposed clause. It is submitted that the word "inherently" connotes a meaning of "an essential constituent or characteristic" of the data message, namely that it must be false. "False" in turn means "not the truth".

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(b) It is further not clear whose "aim" it should be to "cause harm". Must this be attributed to the person who originally distributes the fake news or the person who shares the fake news?	(b) The "aim" must be interpreted within the context of clause 17(1), namely, the person who distributed the data message, which includes the maker and the subsequent distributer.
		(c) Since specific forms of harm are mentioned, other forms of harm are excluded. Clause 17 should be revised to bring it in line with section 16(2) of the Constitution, or alternatively, the applicable defences against defamation should be made applicable to the offences.	(c) It is correct that the ambit of the clause is restricted to specific forms of harm only namely "mental, psychological, physical or economic harm to a specific person or a group of persons" The evaluation of the fake news clause against section 16(2) of the Constitution is discussed under paragraph 4.1.4 and 4.3.9, above. Unlawfulness is a part of the offence of distributing fake news and this implies that any defence that is recognised by the law may be used to justify an act falling within the proscription. The Department proposes the following amendments to clause 17, which may address concerns that were raised against the clause. Proposed amendments:

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			Data message which threatens persons with violence or damage to property **17.** Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which— (*a*) threatens a person with— (i) damage to any property belonging to, or violence against, that person; or (ii) damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person; or (*b*) threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons,

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as a threat of violence or damage to property, is guilty of an offence. **New clause:** **Data message which is harmful** … . (1) Any person who unlawfully and intentionally and persistently makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence. (2) For purposes of subsection (1)— (*a*) a data message is harmful when it— (i) intimidates, encourages or harass a person to harm himself or herself or any other person; or (ii) is inherently false in nature and it is aimed at causing harm, and a reasonable person in possession of the same

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			information and with regard to all the circumstances would regard the data message as harmful; and (*b*) "**harm**" means any mental, psychological, physical or economic harm.
4.4 Section 18: Distribution of data message of intimate image without consent	4.4.1 Western Cape - page 1 of Annexure to letter; Deloitte - page 2	4.4.1 The offence of distributing intimate images without consent is welcomed but should be extended to include sexual activity where no visible nudity as contemplated in section 18(2)(b) is involved	4.4.1 Sexual activity where there is no visible nudity is addressed in the Schedule to the Bill, where it is proposed that a new section 10A be inserted in the Sexual Offences Act. The definition of "pornography" in section 1 of the the Sexual Offences Act, includes acts of "of an explicit or sexual nature" that is intended to stimulate erotic feelings, including any such image or description of such person among others – "(h) engaged in sexually suggestive or lewd acts"; or "(k) showing or describing the body, or parts of the body, of that person in a manner or in circumstances which, within the context, violate or offend the sexual integrity or dignity of that person or any other person or is capable of

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			being used for the purposes of violating or offending the sexual integrity or dignity of that person or any other person".
	4.4.2 Deloitte - page 2	4.4.2 This offence can only be committed where intention is proved. It is proposed that negligent conduct falling within the clause should also be criminalised	4.4.2 For purposes of the Act, and in general, criminal liability flows from willed or intentional acts, only.
	4.4.3 All Rise - page 4 (paragraphs 14 and 15)	4.4.3 This offence is welcomed. Given the increasing prevalence of 'creep shots' and 'upskirt' images, it is proposed that the Bill should also cover possession and distribution of such images which per se is not restricted to nude images.	4.4.3 The Department agrees and will consider an amendment. 4.4.4 The Department disagrees that this offence requires the element of harm. The clause is concerned with the distribution of intimate images of a person, without consent. Harm is inherent within the act of distribution.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	4.4.4 Media Monitoring - page 13 (paragraph 28)	4.4.4 Section 18 does not require the element of harm and thus leads to the possible absurdity of the criminal prosecution of a parent who shares a nude picture of a new born baby with family members.	
	4.4.5 Michalsons Attorneys - pages 6 to 7	4.4.5 (a) The limitation of the clause to only cover nudity is insufficient. Revenge porn can include pictures or descriptions that do necessarily depict the victim fully nude, but can be equally damaging to their dignity. As an example, “cum shots” (a picture of a person, frequently a woman with male ejaculate on her face or other body parts) as they are referred to would not be covered. The amendment proposes that what constitutes as revenge porn should be wider to include these sorts of pictures or descriptions as they are equally as damaging.	4.4.5 Clause 18 does not aim to deal with revenge pornography, see the Schedule to the Act, where it is proposed that section 10A be inserted in the Sexual Offences Act to deal with this aspect. (a) The proposed section 10A covers conduct of a sexual nature where there is no nudity (see paragraph 4.4.1, above) and will include images and descriptions. Graphic descriptions falling within the definition of “pornography” will therefore be prosecuted under the harmful pornography provision.
		(b) The requirement of “identifiable” also limits the clause. According to the representation the data message itself must be able to identify the victim which is insufficient to protect victims. It is argued that revenge porn may not have identifiable marks or even depictions of the actual victim, but is depicted in a context or with	(b) The identifiable requirement is not an element of the offence in terms of 10A(1). It is submitted that clause 18 as well as the proposed section 10A(1) of the Sexual Offences Act is broad enough to cover persons that is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		additional information that is intended to make the recipient of the message believe it is the victim.	identifiable from surrounding circumstances.
		(c) It is also argued that the "reasonable expectation of privacy" limitation is unjustified. There have been several cases where revenge porn is captured in "public" areas and typically where the victim is in some way compromised (drunk, or under the influence of narcotics). It also needs to cover the eventuality that the victim may have consented to the creation of the data message (and even intended for it to be distributed) but then changes their mind.	(c) This aspect is dealt with in the proposed section 10A(1), which requires as part of the proscription that the disclosure takes place without consent. For purposes of clause 18, it is submitted that that where a person exposes him or herself in the public, that person is in general not entitled to protection of his or her dignity. There may however be certain instances where such a person should be allowed to be protected, among others, where the person is mentally challenged.
		(d) It is further proposed that this offence be dealt with as part of the Sexual Offences Act and not in Chapter 3 of the Bill.	(d) The offence of harmful disclosure of pornography is dealt with in the Bill as an amendment to the Sexual Offences Act.
		(e) It is proposed that this clause be redrafted as follows: "The non-consensual, creation, possession, solicitation, publication or distribution of any data message, however created, or any description of a person, real or simulated, showing or describing the body, or parts of the body, of such person in a manner or in	(e) This proposal has various shortcomings, among others that it does not relate to "pornography" that it aims to address. However, the description aspect, as proposed may be included in the current clause to deal with content

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		circumstances which, within the context, violate or offend the sexual integrity or dignity of that person"	other that a visual depiction of a person, among others where written material is published which is of intimate nature, or where images are wrongly identified.
	4.4.6 R2K - pages 7 to 8	4.4.6 A similar offence is contained in the Films and Publications Amendment Act currently under consideration. R2K supports the inputs of Media Monitoring Africa, and do not have any concerns with this clause.	4.4.6 See responses to the Films and Publications Amendment Bill above.
	4.4.7 SAHRC - pages 7 to 8 (paragraph 3.6)	4.4.7 The SAHRC welcomes the clause, noting the high levels of cyberbullying and the phenomenon of 'revenge porn' where intimate images are shared by partners on a non-consensual basis. The SAHRC however notes the use of the term 'female' in clause 18(2)(ii) and points out that the term is limited to biological status. It is recommended that the term is replaced with the word 'woman' which is broader, taking into account intersex, transgendered and persons with body variations, who identify themselves as woman.	4.4.7 The word "female" relates to a person with certain biological status having certain characteristics that uniquely classify such a person as a female.
	4.4.8 Digital Law Companies	4.4.8 Revenge pornography is an increasingly prevalent and alarming phenomenon and has a severe and adverse impact on the lives of persons. The provisions dealing with revenge pornography should be included in the Sexual Offences Act. The following suggestions are	4.4.8 Clause 18 does not address revenge pornography. See paragraph 4.4.5, above

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		made – (a) The culpa requirement should also include negligence (paragraph 1).	(a) The general requirement for criminal liability is *dolus*. This means that only willed acts are punishable. For purposes of the offence in question, that primarily aims to address the making available of images that harm a person's dignitas, it is submitted that negligence may not be the appropriate form of *mens rea.*
		(b) The provisions should not only apply to images distributed via a computer system but should also apply to images otherwise distributed (paragraph 2).	(b) The primary aims of clauses 16, 17 and 18 is to deal with harassing conduct in cyberspace and to address cyber harassment, only. What is criminalised in terms of clause 18 is the using of a computer system to distribute intimate images. This can be expanded upon to deal with the distribution of intimate images in the real world as opposed to the virtual world, but will then expand beyond cyber harassment.
		(c) Identifiable should include indirectly identifiable or incorrectly identified persons (paragraph 3);	(c) As pointed out above, the identifiable requirement is not an element of the offence in terms of section 10A(1) which deals with the harmful disclosure of pornography. Both clauses 18 and the proposed section 10A(1) of the Sexual Offences Act is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			broad enough to cover persons that are identifiable from surrounding circumstances. The aspect of incorrectly identified persons will fall within the ambit of clause 17(1) read with clause 17(2), that deals with data messages of a false nature that is aimed to cause harm.
		(d) The words "knows that consent has not been given" should be replaced with wording to the effect that criminal liability will attach unless the perpetrator "knows consent has been given". This will place the burden of proof on the perpetrator (paragraph 4).	(d) In criminal cases, the State must prove all the elements of an offence and in the context of clause 18(1), the fact that consent was not given for the distribution of the intimate image. The concern relates to the fact that a burden is placed on the state to prove that the perpetrator knows that the victim did not consent to the distribution of the intimate image. The submission propagates criminalisation unless the perpetrator knows that consent has been given for the distribution. Both instances relate to knowledge of absence of permission or implied permission.
		(e) The harmful material should also be extended to include descriptions (paragraph 6);	(e) The aim of the clause, in the context of Chapter 3 of the Bill is, to criminalise conduct which is considered

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			immediately necessary to protect persons against degrading conduct in cyber space. The description of a person in nude does not have the same degrading effect as an image of that person in nude since viewers do not actually observe that person in nude. Graphic descriptions of a pornographic nature will be criminalised in terms of the proposed section 10A of the Sexual Offences Act. The UK Law Reform Commission Report, covers the offence contemplated in clause 18 of the Bill as well as ntimate descriptions (see page 168 – proposed offence to deal with taking or distributing intimate image without consent). A possible inclusion to this effect may be considered.
		(f) Privacy is not the only yardstick and dignity of person should be considered (paragraph 7)	(f) The reference in clause 18(2), to "reasonable expectation of privacy" restricts the ambit of the proscription to a space where a person can expect to engage in conduct to the exclusion of others. The publication of a nude image *on its own,* infringes on the dignity of a person if it is done outside the determined space where the person chooses to be nude.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(g) Revenge porn need not depict nudity or genitals (paragraph 8).	(g) See paragraphs 4.4.3 and 4.4.5(a), above.
4.5 Clause 19: Order to protect complainant pending finalisation of criminal proceedings	4.5.1 Cell C, Telkom and Vodacom - page 17 (paragraph 2.3.5); MTN - page 7 (paragraph 3.2.1) - (same concern about social media services)	4.5.1 The clause is supported subject to the following: (a) In view of the fact that 'Social Media' or normal multi-media messaging services could be used to commit such offences, the provision of clause 19(1)(*b*) does not seem effective, since such messages become self-propagating, especially with reference to clauses 17 and 18. (b) A concern is raised that instructions to "remove or disable access" could be regularly challenged where such instructions cannot be readily fulfilled. The fulfilment of such instructions can commonly only be determined after proper analysis of the manner by which the messages are being conveyed. Where messages are conveyed by common IP packet transport, for instance, such transport may simultaneously carry multiple services including voice calls (using VoIP) for which further access to the telecommunications network cannot necessarily be allowed or disabled on a service-specific, selective basis. To "remove or disable access" can otherwise readily be fulfilled if a court order lists all services to be suspended.	4.5.1 (a) and (b) The concern is noted. Clause 19(1) makes provision of protection orders against service providers and persons. In terms of clause 20, service providers or persons who may include a social media provider" must identify the service and customer from where the malicious communication originates. Once this information is known the court may issue a protection order directing the electronic communications service provider or person to stop distribution of the malicious communication or to remove or disable access to the malicious communication. The service, the customer and the service provider or person will thus be identified before a protection order is issued. Multiple protection orders may therefore be issued if multiple services, persons or service providers are involved.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(c) Clause 19(1)(*b*) only makes reference to a "computer system" and not "computer storage medium" or "computer program" and should be included.	(c) A "computer system" is defined as one or more computers. Computer is further defined to include "a data storage medium" and by implication also consists of a program that causes it to perform a function. (This is based on the new proposed definition)
	4.5.2 All Rise - page 3 (paragraph 10)	4.5.2 For purposes of this Chapter the definition of electronic communications service provider should be extended to also include providers of blogging and social networking services.	4.5.2 As is pointed out under paragraph 2.6, these persons or entities are included in clauses 19 to 21 by virtue of the reference to "person in control of a computer system".
	4.5.3 All Rise - page 4 (paragraph 17)	4.5.3 The obligations on service providers to help enforce interim protection orders for victims is a critical part of the solution and removes the need to rely on goodwill to address cyber abuse.	4.5.3 Noted
	4.5.4 All Rise - pages 4 to 5 (paragraph 21)	4.5.4 How will the issue of anonymity in cyber harassment be addressed and managed for example where blogging platforms and social networks are involved and the identity of the perpetrator has not been validated	4.5.4 The question of anonymity is an international problem and it is submitted that this ought to be addressed on another level. Most services originate from outside the country and are not subject to the legislative jurisdiction of South Africa. The protection that this Chapter intends to afford is mainly restricted to South Africa. Provision is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			made in clause 59 that the executive may enter into international agreements relating to the investigation of criminal offences as contemplated in clauses 16, 17 and 18, which to an extent may ensure international co-operation and extradition of a person.
	4.5.5 All Rise - pages 4 to 5 (paragraphs 23 to 26)	4.5.5 The collection of information to prosecute cyber harassment cases is difficult, in light of the following three factors:	4.5.5 ISPs are not compelled currently to store call-related information. However, information is kept for a short period of time (this varies from internet service provider to internet service provider). On judicial authority the service providers will make this information available to the court.
		(a) Anonymity – many blogging and social media platforms do not validate user identity, when users sign up for a service (meaning that only IPO addresses, device ID and traffic data will be available), which is in many instances not sufficient.	(a) The malicious communication will be available in most circumstances but there is in many circumstances an inability to identify the user of the services. Additional investigation procedures are required to identify the user of social media services. However, even if the perpetrator cannot be identified the court still has the powers to prohibit distribution of the malicious communication in terms of clause

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			19(1)(*b*).
		(b) Volume abuse – due to the increasing volume of cyber abuse, automated processes regarding evidence gathering, application processes for court orders and warrant processes and requests for evidence may need to be implemented.	(b) The regulations giving effect to this Chapter will follow the same trend as regulations that were made in terms of the Protection from Harassment Act that provides for electronic service of process in order to identify the perpetrator and the submission of this information to the court. Clause (4) provides that the order may be served in the prescribed form and manner, which may include electronic processes.
		(c) Evidence outside jurisdiction – The most effective way to deal with this is to ensure that legislation has extra territorial jurisdiction, as is provided in the Bill. Mutual Legal Assistance Treaties may also facilitate this.	(c) Chapter 6 of the Bill deals with aspects relating to mutual assistance in investigation of cybercrime that also recognises the offences in Chapter 3 as offences to which that chapter applies. Chapter 6 can be used to secure evidence pending a formal application in terms of the International Co-operation in Criminal Matters Act, 1996, to make the evidence available to the Republic. Clause 51 aims to facilitate the admissibility in proceedings of evidence so obtained. If malicious communications originates from outside

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			the Republic, and depending where the perpetrator is situated, formal extradition proceedings may be required to extradite the person to the Republic.
	4.5.6 All Rise - page 5 (paragraph 27)	4.5.6 With reference to expedited preservation of data as contemplated in clause 39 of the Bill, a concern is raised that this may contribute to mental anguish and suicide and a concern is raised that this process may not be suitable for cyber harassment.	4.5.6 Preservation of evidence does not imply that the evidence will be available to the victim or the public. A court may order electronic communications service providers to remove or disable access to the malicious content. Simultaneously, law enforcement may request a service provider to preserve evidence relating to the communication for a certain period to assist in the investigation and prosecution.
	4.5.7 Centre for Constitutional Rights - pages 7 and 8 (paragraph 10.11)	4.5.7 Clause 19 makes it possible for a person to make an application to the court on an *ex parte* basis for essentially a protection order pending the finalisation of the criminal proceedings. This order is not only served on the person, but also on the electronic communication service provider without notice. This is in contrast to section 4 of the Harassment Act, which only provides for a direction order for information to be made to electronic communication providers after the court is satisfied that the requirements for an interim protection order has been met. In terms of clause 19, no provision is made	4.5.7 The Protection from Harassment Act, deals with real world as well as cyber harassment. The Bill only deals with cyber harassment. Clause 19 deals with the issuing of a protection order if there is *prima facie* evidence that a malicious communication took place 19(3). Once the court is satisfied that prima facie evidence exists, and the perpetrator or the services provider from where the communication

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		for the electronic communication provider to first provide information to the court and this will lead to contrasting obligations between the Harassment Act and this Bill.	originated cannot be identified, the court will make use of clause 20(1) to identify the person or service provider of the perpetrator. These procedures are the same as under the Harassment Act. However, the Harassment Act makes provision for an interim protection order that can be made final on the return date. This is not part of clause 19. This difference is necessary since the Harassment Act is civil in nature and in terms of clause 19, the protection order can only be applied for or be issued if a criminal charge is pending. If clause 19 followed the same route as the Harassment Act, both the victim and perpetrator may be prejudiced in that both may be required to give evidence which is relevant to later criminal proceedings based on the same facts. Interim relieve is available for the alleged perpetrator to challenge the order (see clause 19(6) and further). The decision of the court is subject to review or appeal. It is submitted that the only difference between the Harassment Act and the Bill is that no provision is made for an interim order that must later be confirmed by a court.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
4.6 Clause 20: Electronic communications service provider or person in control of computer system to furnish particulars to court	4.6.1 Cell C, Telkom and Vodacom - pages 17 to 18 (paragraphs 2.3.6 and 2.3.7)); MTN - page 7 (paragraph 3.2.2)	4.6.1 In terms of clause 20, electronic communications service providers are compelled to assist a court (during proceedings in terms of clause 19) to make available particulars of a person who distributed the malicious communications in order to ensure that the interim protection order can be served on him or her. Electronic communications service providers however do not exercise control of the posting of, the transmission of or storing of contents on certain sites, for example social media and may not be able to comply in full with this provision. It is acknowledged that clause 20 provides that electronic communication service providers may, by means of an affidavit, apply to a court that they be exempted from complying with an order of the court since the data is not under their control.	4.6.1 Noted
	4.6.2 TBCSA - page 3 (Item 3)	4.6.2 Does the reference in clause 20 to electronic communication service providers include a reference to Internet cafes as they are used for the bulk of fraud that takes place in guest houses?	4.6.2 Internet cafes are used to commit various crimes due to the fact that it offers anonymity. For purposes of Chapter 3, Internet cafes must be seen as a medium to access a computer system and a tool that may be used to store malicious communications or distribute malicious communications. Any person in control of a computer system, which is wide enough to include internet café, falls within the ambit of clauses 19, 20 and 21 and the same obligations that are applicable to

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			electronic communications service providers will apply to these persons/businesses.
4.7 Clause 22: Penalties	4.7.1 Cell C, Telkom and Vodacom - pages 17 to 18 (paragraphs 2.3.6 and 2.3.7)); All Rise - page 6	4.7.1The penalty should be increased to a fine or imprisonment not exceeding 5 years.	4.7.1 The harm caused through the distribution of malicious communications is significant. Australia, criminalises threats to kill or to cause serious harm with penalties ranging from 7 to 10 years. The Australian harassment offence by means of ICTs is criminalised with a penalty of 3 years. It is however submitted that the offences in question should not be visited with punishment that is disproportional to similar conduct that is committed in the real world and it is submitted that the penalties in question are proportionate to the harm they may cause.
	4.7.2 Deloitte - page 2	4.7.2 A minimum sentence for non-compliance will render the provisions more effective.	4.7.2 A minimum sentence does not take into account the circumstances under which an offence is committed and in effect interferes with the discretion of the court to impose a suitable sentence with due regard to the circumstances under which the offence was committed and other principles applicable to punishment.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
5. CHAPTER 4: JURISDICTION			
5. Clause 23: Jurisdiction	5.1 Cell C, Telkom and Vodacom - page 18 (paragraph 2.4.1))	The clause is supported.	5.1 Noted
6. CHAPTER 5: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE			
6.1 General	6.1.1 DFIRLABS - page 1 (paragraph 1.1 and paragraph 3), pages 4 to 9	6.1.1 In order to implement the Bill successfully, the capacity of and digital forensic practitioners need to be addressed. The commentator stresses the need for proper investigative capacity.	6.1.1 Digital forensic investigators are essential to investigate cybercrime and to deal with electronic evidence in general. Specialised training programs are provided for in clause 54(2) of the Bill.
	6.1.2 Cell C, Telkom and Vodacom - page 18 (paragraph 2.5.3)	6.1.2 The investigative procedures provided for in Chapter 2 of the Criminal Procedure Act are insufficient as they are object based and do not deal with the specialised procedures which are required to investigate cybercrimes, specifically when dealing with electronic evidence which is of an incorporeal nature and by its very nature fragile. Special procedures are further necessary to ensure the integrity of electronic evidence which is not specifically catered for in the Criminal Procedure Act and is now be addressed in the Bill.	6.1.2 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	6.1.3 Cell C, Telkom and Vodacom - page 20 (paragraphs 2.5.15)	6.1.3 Where cellular devices are targeted by search, access and seize operations, such actions must be approached with significant caution and oversight, since these devices commonly contain much personal information. “Investigator assistants” that may commonly assist with ‘search’, ‘access’ and ‘seize’, could possibly fulfil a role of independent oversight. This should be addressed in training and in the Standard Operating Procedures and if these operating procedures are also publicised in regulations, it would enhance public confidence and transparency in the fairness of such procedures.	6.1.3 The comment relates to the protection of privacy during a search and seizure. If the seizure is authorised by a warrant in terms of clause 27, the warrant will determine the nature and extent of access. Where there is a search and seizure on the grounds that a device was involved in the commission of an offence, a warrant is required to access the information. Only in exigent circumstances are law enforcement allowed to access the information without a warrant.
	6.1.4 legal Aid SA - page 4	6.1.4 It is increasingly possible for people to be spied upon through their own devices.	6.1.4 The Bill as well as the RICA, prohibits such conduct unless it takes place in terms of judicial authorisation.
	6.1.5 MTN - page 4 (paragraph 2.4)	6.1.5 The words “integrity” and “availability” (as used in clauses 39(4), 40(3), 41(4), 42(8), and 48(2)) should have the same meaning as contemplated in section 14 to 17 of the ECTA that deals with the admissibility of electronic evidence in proceedings.	6.1.5 The ECTA sets out the standard to be applied in order to determine whether electronic evidence can be relied upon as evidence. These standards are in line with international benchmarks and have been applied by courts in the RSA to evaluate electronic evidence. These concepts will be interpreted within that ambit. The South African Law Reform Commission (SALRC) has recently completed an

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			investigation relating to electronic evidence and suggestions were made to better the current position. When these recommendations are implemented by way of legislation, the concepts will be interpreted to be in line with the new developments.
	6.1.6 Liquid Telecom - pages 4 to 7	6.1.6 Under the heading "opportunity to remedy RICA issues" the commentator refers to various problems that exist in respect of the RICA and which may impact on the Bill among others, Chapter 3 of the Bill which deals with malicious communications, where the identification of the origins of communications may be sought by a court in proceedings under that Chapter, clauses 38 to 42 of the Bill that deals with aspects which may also have a bearing on RICA. It is proposed that the Portfolio Committee should intervene and set up a technical workshop between the Department and experts of the industry to address these aspects before the Bill is finalised.	6.1.6 The RICA is currently being revised by the Department. The Department is aware of the concerns of the electronic communications service providers. A concern that can probably be addressed in this Bill relates to the obligations that were imposed on service providers to verify and retain customer information. Section 39 of the RICA requires that fixed line operators must store copies of the ID documents of customers. Section 40 does not impose similar obligations on Mobile Cellular Operators.
	6.1.7 IAB - paragraph 2.4	6.1.7 This Chapter rectifies the legal *lacunae* that existed in the Criminal Procedure Act, which only dealt with access to documents, which was later extended to computer data. This Chapter also provides for the much needed expedited preservation of e-evidence procedure. However, these powers must be exercised carefully and	6.1.7 The comment is noted. It is submitted that the powers to investigate cyber offences, as is provided for in this Chapter, is in line with the principles that were developed by the courts to regulate search and seizures in South

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		in line with the Constitution.	Africa.
	6.1.8 Cell C, Telkom and Vodacom - page 21 (paragraphs 2.5.16 and 2.6.6)	6.1.8 There are no regulatory impact assessments of the cost of compliance that have been conducted in order to assess the financial burden that may be associated with compliance with the directives proposed in Chapter 5 of the Bill.	6.1.8 The cost of compliance is minimal and in line with other obligations already imposed on the electronic communications service providers in terms of RICA. Small deviations from the regulatory measures currently in place in RICA are necessary to deal with aspects relating to mutual assistance. However, these measures will not impact on electronic communications service providers that are RICA compliant.
	6.1.9 Credit Bureau Association - paragraph 2.3	6.1.9 A concern is raised that the judiciary may issue warrants and that law enforcement officers may seize and search for articles involving credit bureaus. The Credit Bureau Association is concerned about the expertise to investigate cybercrimes on highly sophisticated systems. According to them such measures infringe on the constitutional rights of privacy of a person and the duty of bureaus to keep information confidential. A general concern is raised about capacity and expertise in the Republic to investigate, prosecute and adjudicate on cyber offences.	6.1.9 Section 205(3) of the Constitution specifically provides that the SAPS must investigate crimes. Search and seizure provisions serve an important purpose in the fight against crime and the interests of the State to ensure the security and freedom of the public. It is submitted that this objective is sufficiently important to justify the limitation of the right to privacy of an individual in certain circumstances. Constitutional rights are not meant to shield criminal activity or to conceal evidence of crime from the criminal

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			justice process. On the other hand, State officials are not entitled without good cause to invade the premises of persons for purposes of searching and seizing property. A balance must therefore be struck between the interests of the individual and that of the State, a task that lies at the heart of the inquiry into the limitation of rights (INVESTIGATING DIRECTORATE: SERIOUS ECONOMIC OFFENCES AND OTHERS V HYUNDAI MOTOR DISTRIBUTORS (PTY) LTD AND OTHERS 2000 (2) SACR 349 (CC)). On the other hand and in relation to investigation of cyber offences searches and seizures must be carried out in the least intrusive and disruptive manner (see BEHEERSMAATSCHAPPIJ HELLING I NV AND OTHERS v MAGISTRATE, CAPE TOWN, AND OTHERS 2007 (1) SACR 99 (C) and CONCALVES v MINISTER OF LAW AND ORDER 1993 (1) SA 161 (W)). The concern about lack of expertise to deal with highly sophisticated computer systems is acknowledged in the provisions of this Chapter. Investigators (persons with the required expertise)

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			may be appointed to assist the SAPS during investigations. If damage is caused to systems the SAPS can be held liable for such damage. A provision that is not taken into account by the commentator is clause 42(1)(*a*), which may be used where it is not necessary to resort to the coercive and infringing powers of search and seizures.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
6.2 Clause 24: SOPS	6.2.1 Western Cape - pages 1 and 2 of Annexure to letter	6.2.1 SOPS are welcomed and necessary. It is suggested that this be aligned with the Electronic Communications and Transactions Act, 2002.	6.2.1 Noted. In order to ensure that electronic evidence is admissible to courts, due regard will be paid to the provisions of the ECTA
	6.2.2 Cell C, Telkom and Vodacom - page 19 (paragraphs 2.5.1 and 2.5.2)	6.2.2 A public consultation process should be followed in the drafting of the SOPS and should also be made applicable to private sector computer security incident response teams to ensure uniformity of process and ease of presenting evidence in courts.	6.2.2 Clause 24, specifically provides that a public consultation process must be followed in the formalisation of the SOPs and that it would apply to the investigation of any offence in terms of Chapter 2 or section 16, 17 or 18 of the Bill or any other offence which is or was committed by means of or facilitated by the use of computer technology.
	6.2.3 MTN - page 3 (paragraph 2.2)	6.2.3 MTN suggests that the general acceptable six principles relating to SOPS should be taken into account in finalising the document.	6.2.3 Noted.
	6.2.4 DFIRLABS - page 5 (paragraphs 3.6 and 3.7) and page 9 (paragraph 4); Mr Eatwell - page	6.2.4 The following concerns are raised against the clause: (a) The clause does not include persons in the private sector that deals with digital evidence. In many instances persons in the private sector initiate initial	6.2.4 (a) The SOPs will apply to investigation of any offence in terms of Chapter 2 or section 16, 17 or 18 of the Bill or any other offence which is or was committed by means of or facilitated by

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	10 (paragraphs 4.5.3 and 4.5.4) – (competency of investigators)	investigations before it is handed over to the SAPS and during this process the evidence may already have been compromised due to the lack of compliance with general accepted principles. (b) SOPS should be in the form of subordinate legislation which makes it enforceable. (c) SOPS, if made in line with international standards will play a significant role in improving digital forensics in South Africa. (d) One of the requirements of SOPS is that digital forensic investigations should be done by competent persons. This aspect should be provided for in the SOPS which will address the concerns as pointed out by the author in paragraph 6.1.1.	the use of computer technology (clause 24(1)). (b) It is not necessary to issue SOPs in the form of regulations. (c) Noted. (d) Noted
	6.2.6 Information Regulator - page 5; IM Governance - page 1 (paragraph 1)	6.2.6 Include the Information Regulator to oversee that the SOPS are not unlawfully with respect to the processing of personal information.	6.2.6 The Information Regulator will, like other persons that have an interest in the formulation of SOPs, be consulted on the SOPs. It is submitted that the Information Regulator should not specifically be included in the clause.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
6.3 Clause 27: Article to be searched for, accessed or seized or under search warrant	6.3.1 Cell C, Telkom and Vodacom - page 19 (paragraphs 2.5.5 and 2.5.6) 6.3.2 Cell C, Telkom and Vodacom - page 19 (paragraph 2.5.7)	6.3.1 The case law regarding the conduct of search and seizure operations in South African law is well-defined and would still be applicable in instances where the provisions of clause 27 are invoked. 6.3.2 Exercise of search warrants although trite law must always be done with due regard to the rights of individuals and the businesses concerned and also where electronic communications service providers are concerned, that interference with infrastructure and networks can disrupt communications for millions of South Africans.	6.3.1 Noted 6.3.2 The principle of the limitation of a search and seizure to what is necessary for the criminal investigation has been recognised by our courts, see the cases referred to in paragraph 6.1.9. The general requirements for a search warrant is summarised in ZOECO SYSTEM MANAGERS CC v MINISTER OF SAFETY AND SECURITY NO AND OTHERS 2013 (2) SACR 545 (GNP) (see Annexure B). It is submitted that the same interpretation should be given to clause 27 as that which has been developed by our courts in respect of section 21 of the Criminal Procedure Act, 1977 (see among others MINISTER OF SAFETY AND SECURITY AND OTHERS v MOHAMED AND ANOTHER 2012 (1) SACR 321 (SCA), where section 29 of the NPA Act was interpreted with reference to the authorities in relation to

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			sections 20 and 21 of the Criminal Procedure Act, 1977). The Bill itself provides for a "scales clause", see clause 34(1) and other provisions in the Bill that specifically concerns the execution of powers by law enforcement. In terms of clause 34(1), powers conferred by the Bill on law enforcement must be exercised with – * strict regard to decency and order; and * due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.
	6.3.3 Cell C, Telkom and Vodacom - page 19 (paragraph 2.5.8)	6.3.3 The mere fact that a data message was conveyed by an electronic communications service provider's computer system should not imply that its computer system is involved in the commissioning of any category or class of offences, and thus an article to be searched for, accessed or seized.	6.33 "Article" is defined in clause 1 of the Bill and the definition is basically the same as section 20 of the Criminal Procedure Act. Judgments relating to the extent of the powers that may be authorised in terms of a search warrant will therefore also be applicable to clause 27 of the Bill. A computer system may be used to commit an offence or may be involved in the commission of an offence. This may be compared to real world searches,

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			where law enforcement is authorised to access property to look for article/s on the property. Similar to such real world searches, it is necessary to allow law enforcement access to a computer system to search for and seize evidence. The extent of these powers is dependent on the authority provided in the search warrant which must be interpreted within the ambit of its authorising legislation. To that extent, the "scales clause" again requires reasonable conduct by the investigator, taking into account the rights and obligations of other persons, including the service provider whose system is to be accessed in order to search and seize for an article.
	6.3.4 Western Cape - page 2 of Annexure to letter	6.3.4 In terms of clause 27(1)(*a*)(ii) the criteria for issuing a search warrant is that the article is "being used or is involved in the commission of an offence". It is pointed out that the definition of article already incorporates these requirements. It is proposed that the clause should be drafted in line with clause 28(4)(a)(ii), which provides that as follows: "to search for, access or seize an article— (*aa*) within his or her area of jurisdiction; or (*bb*) within the Republic….."	6.3.4 Item (ii) explains a prerequisite when a search warrant can be authorised if it is not in the area of jurisdiction of the magistrate. This prerequisite relates to the fact that it is uncertain within which area of jurisdiction the article is being used or is involved in the commission of an offence.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	6.3.5 Legal Aid SA - pages 4 to 5	6.3.5 The Bill clearly fails to outline the particularity requirement in a search warrant, namely, the exact location of the evidence within a computer device or computer network. This means that investigators can search through a person's emails, social networking profiles, messages and computer files in search for evidence. There is no actual limit for the search, which leaves individuals vulnerable and violated. This amounts to the state exceeding the bounds of a search and infringing a person's right to privacy.	6.3.5 It is impossible to determine the exact location of an article in a computer system. In THINT (PTY) LTD v NATIONAL DIRECTOR OF PUBLIC PROSECUTIONS AND OTHERS; ZUMA v NATIONAL DIRECTOR OF PUBLIC PROSECUTIONS AND OTHERS 2008 (2) SACR 421 (CC), at paragraphs [146] to [147] it was said that investigators should restrict their search, examination, and seizure to those classes of items that they have reason to believe might have a bearing on the investigation in question. That reason may flow from prior knowledge of the investigation, or it may occur to an investigator during the course of the search or emerge during a conversation with persons at the searched premises, but a reason they must have. That reason, moreover, should also be sufficiently plausible to outweigh the countervailing risk that the item might be irrelevant to the investigation and examining it would amount to an invasion of privacy. Section 29 should not be interpreted to

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			authorise the examination or seizure of an item in circumstances where there is no reason to believe that it might have a bearing on the investigation. According to the court this approach, gives appropriate recognition to the constitutional principles at play and, at the same time, respect the language of section 29 of the Act" (section 29 refers to section 29 of the NPA Act). Also see the POLOYFIS – judgment in Annexure B, where the court came to the conclusion that "It will be inherent in the nature of the authority to search that the searcher might, in appropriate circumstances, be entitled to examine property that is not itself connected with the crime — for example, the contents of a cupboard or a drawer, or a collection of documents — to ascertain whether it contains or is the article that is being sought.". In any event, like section 29 of the NPA Act, that was considered in the THINT judgment, clause 34 places a limitation on the actions of the searcher (also see MINISTER OF SAFETY AND SECURITY AND OTHERS v MOHAMED AND ANOTHER 2012 (1)

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			SACR 321 (SCA)).
	6.3.6 MTN - page 6	6.3.6 An application should be considered by the designated judge appointed in terms of section 1 of the RICA. The designated judge will be in a better position to consider this type of applications and will give effect to the provisions of POPIA that deals with the protection and confidentiality of information.	6.3.6 The task of the RICA judge is primarily to deal with the interception of communications. Search warrants are issued on a daily basis to provide for computer-related searches. The POPIA has limited application in relation to the powers to search and seize in terms of a warrant on the basis that it is necessary to infringe privacy to investigate crimes.
	6.3.7 MTN - page 6	6.3.7 The section in effect authorises the seizure of a whole electronic communications network. It is suggested that limitations needs to be specified in the warrant and such limitations should only be confined to access control information relating to the network.	6.3.7 The mere fact that a computer system was involved in the commission of an offence, such as cyber fraud, will not give rise to the seizure of an entire electronic communications system of a public service provider. However, a private computer system (consisting of one or more computers), may for instance be involved in botnet activities or used to distribute child pornography on the Darknet or is used in planned terrorist attacks on critical information infrastructures, and it is submitted that the Bill authorises the seizure of the whole computer system to investigate

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			the offences in question. Clause 27(2), specifically provides that any action taken in response to a warrant is limited to the extent set out in the warrant.
	6.3.8 MTN - page 6	6.3.8 Damage may result from seizure of information and communications technologies and may cause the disruption of legitimate processing of information. The court has taken a cautionary approach to Anton Piller orders. It is critical for businesses or persons to continue with their daily operations in the event of a search and seizure operation.	6.3.8 It is true that damage may arise from a search and seizure. However, if it is necessary to investigate crime this cannot be helped. Wrongful search and seizures are criminalised in terms of clause 35 of the Bill and section 300 of the Criminal Procedure Act is made applicable to such unlawful conduct. A wronged party can institute a civil claim for damages that was suffered. Regarding Anton Piller orders see MINISTER OF SAFETY AND SECURITY AND OTHERS v MOHAMED AND ANOTHER 2012 (1) SACR 321 (SCA) at paragraph 29, where the court dealt with Anton Piller orders in the context of search and seizures: “The Anton Piller order is a remedy that the courts have created in the exercise of their inherent powers. It is to be expected in those circumstances that the courts have fashioned a body of rules determining

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			when and in what form such an order may be issued. But that is not what we are concerned with in this case. We are concerned with warrants that are issued under statutory powers. It is the statute that must dictate what is required for a warrant to be valid and not the warrant that must dictate to the statute." The Bill in essence follows the requirements in terms of section 21 of the Criminal Procedure Act. The scales clause provided in clause 34(1), will again restrict the ambit of application of the powers of law enforcement agencies. Clause 40 provides for an order similar to an Anton Piller order that may be used to preserve an article in certain circumstances subject to the rights, responsibilities and legitimate interests of other persons. The aim of this provision is to ensure the integrity of data or other evidence pending the taking of further steps that is necessary to seize the article in question. The Bill, by means of clause 42(1)(b), makes provision for a less invasive process to obtain data (other evidence is excluded), which will in most instances

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			be resorted to where electronic communications service providers or financial institutions collect data regarding the commission of an offence. As pointed out above, searches and seizures must be carried out in the least intrusive and disruptive manner so as not to impede on business operations.
	6.3.9 Centre for Constitutional Rights - page 11 (paragraphs 11.22 and 11.23 to 11.26)	6.3.9 The relationship of clause 38 of the Bill to clause 27 of the Bill is not clearly stipulated. A real risk exists that clause 27 increases the State's "surveillance powers". It does appear to conflict with RICA and perhaps unintentionally creates a parallel surveillance system. Section 22 of RICA provides for the application of an "entry warrant", which can also be made on application of an interception order in terms of section 16 of the Act. This section clearly stipulates the requirement for such an entry warrant and it can only be made by the "designated judge" who hears the application for the interception order. The above entry warrant may be issued if, for instance, it is "impracticable" on "reasonable grounds" to intercept the communication in any other way and an interception-device, as defined in RICA, is needed.	6.3.9 The relationship of clause 27 to the RICA may be explained on similar basis as section 21 of the Criminal Procedure Act, 1977 to the RICA. Clause 38 provides that the RICA will be applicable if information is to be intercepted or to be provided in terms of the RICA. Section 21 of the Criminal Procedure Act cannot be used to search for or seize information that must be provided in terms of the RICA since section 21 deals with the seizure of an article other than communications that is transmitted within the ambit of the RICA. Clause 27 of the Bill similarly deals with seizure of articles and cannot be used to obtain information that must be obtained in terms of the RICA. Clause 27 therefore does not

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			extend the application of the RICA. Section 22 of the RICA provides for trespass interception of direct communications, among others the planting of a "bug". Section 22 of the RICA cannot be used to search for or seize an article.
	6.3.10 Centre for Constitutional Rights - page 11 (paragraphs 11.24 to 11.26)	6.3.10 Clause 1 of Bill states that an "article" includes "data, a computer program, computer data storage medium or a computer system" which is "reasonably believed" to be concerned with the commission of any cybercrimes offence. If read with clause 27, any "article" can be searched for, accessed or seized by virtue of a search warrant issued by a magistrate or judge of the High Court. The search warrant in terms of clause 27(2) may include the authority to enter such premises and the use of any "instrument" or "device" to "access" an article identified in the search warrant. Furthermore "accessed" in terms of clause 1 of the Bill is loosely defined to include making "...use of data, a computer program, a computer data storage medium…to the extent necessary to search for and seize an article". No definition is provided for "device" in clause 1 of the Bill and it is plausible that it could include a device which could also intercept data as defined in RICA. It is not clear whether clause 27 could possibly be used to circumvent approaching the "designated judge" and the more onerous procedure as set out in section 22 of	6.3.10 The use of devices as contemplated in clause 27(2)(*h)*, merely authorise the tools that is necessary for forensic investigators to obtain evidence in digital format from a computer system. These devices are not interception apparatus. If a digital investigator intercepts information within the ambit of the RICA he or she will commit an offence as contemplated in section 45 of the RICA. As pointed out in paragraph 6.3.9, clause 27 of the Bill relates to searches and seizures and nothing more. Clause 38, ensures that RICA must be used to intercept or obtain RICA-related information and *ipso facto* restricts the application of clause 27 from any interpretation that it can be used during a search and seizure operation to obtain information that must be dealt with in terms of the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		RICA to gain entry to certain premises in order to also place an instrument to "intercept" data. This possible anomaly has to be specifically clarified by the drafters of the Bill by ensuring that the process to gain access to premises in order to intercept data cannot be circumvented.	RICA. There is therefore no anomaly. Furthermore, in terms of clause 35(2), the use of any device outside the ambit of a search warrant that is provided for in clause 27(2), is criminalised.
	6.3.11 SAHRC - page 8 (paragraph 3.7)	6.3.11 According to the SAHRC the word "near" in clause 27(2)(*d*) of the Bill is contextually unclear. A lack of guidance in this regard could potentially be used as justification to search persons outside the immediate scope of the item which is subject to a search and seizure operation.	6.3.11 It is submitted that the clause is clear. Before a person can be subjected to a search within the context of clause 27(2)(*d*), there must be compliance with the provision that requires – * a person must be in close proximity of an article identified in the warrant; * there must be a belief on reasonable grounds, that the person would be able to furnish information; * the information must be of material importance concerning the matter under investigation; and * the search must fall within the context of authorisation as set out in the warrant. It is submitted that these requirements ensures that the powers to investigate are limited to what is necessary.
6.4 Clause 28:	6.4.1 Cell C, Telkom	6.4.1 This clause is supported.	6.4.1 Noted.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
Oral application for search warrant or amendment of warrant	and Vodacom - page 19 (paragraph 2.5.9)		
6.5 Clause 29: Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent	6.5.1 Cell C, Telkom and Vodacom - page 19 (paragraph 2.5.9)	6.5.1 This clause is supported.	6.5.1 Noted
6.6 Clause 30: Search for, access to, or seizure of article involved in the commission of an offence without search warrant	6.6.1 Cell C, Telkom and Vodacom - page 19 (paragraph 2.5.9)	6.6.1 This clause is supported.	6.6.1 Noted
6.7 Clause 31: Search for, access to and seizure of article on arrest of	6.7.1 Cell C, Telkom and Vodacom - page 19 (paragraph 2.5.9) 6.7.2 SAHRC - page	6.7.1 This clause is supported. 6.7.2 In terms of clause 31(1)(b) a police official may	6.7.1 Noted 6.7.2 In DUNCAN V MINISTER OF

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
person	8 (paragraph 3.7)	without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person "whom he or she *reasonably suspects* of having committed any offence in terms of Chapter 2 or section 16, 17 or 18". A concern is expressed that the broad nature of the provision may lead to abuse. The Commission recommends that the standard for 'reasonable suspicion' within the context of the Bill is expanded upon to ensure a proper balance between the need to combat cybercrimes and the protection of personal dignity.	LAW AND ORDER 1986 (2) SA 805 (A) at 818G it was held that the jurisdictional facts which must exist before the power conferred by s 40 (1)(*b*) may be invoked are: * Firstly, the arrestor must be a peace officer. * Secondly, he or she must entertain a suspicion. * Thirdly, the suspicion must be that the arrestee committed an offence referred to in Schedule 1 (least severe offence in the Schedule is 6 months imprisonment without option of a fine) of the Criminal Procedure Act, 1977. * Fourthly, the suspicion must rest on reasonable grounds. The test whether a peace officer "reasonably suspects" a person of having committed an offence within the ambit of s 40(1)(*b*) is an objective one. The test is not whether a police officer believes that he or she has reason to suspect, but whether, on an objective approach, he or she in fact has reasonable grounds for his suspicion. The test as set out in the DUNCAN judgments was endorsed in MINISTER

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			OF LAW AND ORDER AND OTHERS v HURLEY AND ANOTHER 1986 (3) SA 568 (A) at 579H and MINISTER OF SAFETY AND SECURITY v SEKHOTO AND ANOTHER 2011 (1) SACR 315 (SCA) at paragraph [6] and MINISTER OF SAFETY AND SECURITY AND ANOTHER v SWART 2012 (2) SACR 226 (SCA) at paragraph 17. Since clause 31(1)(*b*) is in line with section 40(1)(*b*), it will be interpreted similarly.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
6.8 Clause 32: Assisting member of law enforcement agency or investigator	6.8.1 Cell C, Telkom and Vodacom - page 20 (paragraph 2.5.11); Banking Association SA - page 2	6.8.1 It is submitted that the requirement to provide assistance is broad and should be narrowed to take into account what may be limited circumstances on the part of the person required to provide the assistance. The request by a police official or investigator may be beyond the means of the person being requested to assist or unreasonable. The following amendments is proposed to clause 32(1)(*b*): "(*b*) such other assistance as may be reasonably necessary for the specific investigation,"	6.8.1 Clause 32 aims to address the fact that computer systems are complicated and nature. The service providers have the required expertise to assist the law enforcement agencies to trace information on their systems that is necessary for the investigation of cybercrimes. The reasonableness of the assistance to be provided must be interpreted with reference to what is authorised in the warrant. Clause 32(1), expressly refers to a search and seizure authorised in clause 27(1). To request assistance that does not relate to the authority granted in the warrant is therefore impermissible. If a service provider cannot render the requested assistance due to the absence of necessary expertise, no criminal liability will follow as a result of the criminalising provision in clause 32(2). However, to accommodate this concern the following amendment may be considered: "(1) An electronic communications service provider, a financial institution or person, other than the person who is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			suspected of having committed the offence which is being investigated, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer program, computer data storage medium or computer system that is subject to a search authorised in terms of section 27(1) must, if required, provide— *(a)* technical assistance; and *(b)* such other assistance as may be reasonably necessary, to a police official or an investigator in order to search for, access and seize an article.".
	6.8.2 MTN - pages 7 and 8 (paragraph 3.2.3)	6.8.2 With reference to this clause and the obligations in terms of clause 33 that service providers should render assistance, it is remarked that seizure of critical information may hamper the day to day operations of a service provider and it is proposed that a digital copy should rather be provided to the police official.	6.8.2 This aspect has already been dealt with under paragraph 6.1.9, above. In a digital forensic investigation, a mirror image of the required data is made that is verified. It has already been discussed that the concept of search and seizure must be applied in a manner that causes the least possible infringement. Clause 34 of the Bill further restricts the exercise of powers to what is necessary in the circumstances and with regard to the rights of others.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	6.8.3 Engen Petroleum - page 2 (paragraph 10)	6.8.3 The principle of rendering assistance to law enforcement agencies is acceptable. However, there is no indication how cost relating to such assistance is to be regulated as well as the security and confidentially of information that is to be provided.	6.8.3 It is not required of a service provider to acquire additional expertise to help the police in the investigation of a cybercrime. Service providers employ highly qualified personnel in their daily cyber activities that know the structuring and outlay of their systems. This general available expertise is what is required assist in the investigation of crime.
6.9 Clause 35: Wrongful search, access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access	6.9 Cell C, Telkom and Vodacom - page 20 (paragraph 2.5.13)	6.9 This clause is supported.	6.9 Noted
6.10 Clause 36: False information under oath or by way of affirmation	6.10 Cell C, Telkom and Vodacom - page 20 (paragraph 2.5.13)	6.10 This clause is supported.	6.10 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
6.11 Clause 37: Prohibition on disclosure of information	6.11.1 Cell C, Telkom and Vodacom - page 20 (paragraphs 2.5.13 and 2.5.14)	6.11.1 This clause is supported. However, the instances where disclosure is permitted should be addressed in more detail. Where it pertains to police officials it can be addressed in SOPS. The electronic communications service providers indicate that they are hesitant to allow for information sharing by investigators that were designated to assist with searches where no legal remedies would be available for unlawful disclosure e.g. non-disclosure agreements are not in place. Where employees of an electronic communications service provider and financial institution would have obtained such information during the normal course of their duties (e.g. investigators) then there is no impediment to sharing according to normal business practice.	6.11.1 It is submitted that the clause is comprehensive and regulates instances where information sharing would be permitted. The clause does not prohibit information sharing during the course of the duties of a person see clause 37(1)(*b*). Information sharing in the course of the duties of a person is necessary in order to ensure that appropriate measures are implemented or developed to address similar criminal conduct.
	6.11.2 Banking Association SA - page 3	6.11.2 It is proposed that clause 37(1)(*e*) be amended where a competent authority requests information before criminal proceedings are initiated to provide as follows: "(e) to any competent authority which requires it for the institution of criminal proceedings and the use of such information for evidentiary purposes in court proceedings." Alternatively, the view is held that disclosure of information is sufficiently covered in clause 37(1)(c) as it reads "if it is information which is required in terms of any law or as evidence in any court of law".	6.11.2 In mutual assistance proceeding as well as criminal proceedings, information is not per se always required to be used as evidence in a court of law. Information is necessary to investigate an offence that has allegedly been committed and the requested information is necessary to determine whether or not an offence has been committed. The proposed amendment to clause 37(1)(*e*), will unduly restrict the clause to "evidence" only and it may be argued that initial information that is used in criminal investigation are not

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			covered by the prohibition in clause 37.
	6.11.3 Deloitte - page 2	6.11.3 Clause 37(1)(*e*) should be amended to include that the information must also not be disclosed during the course of investigation of criminal proceedings and not only in the institution of criminal proceedings, to extend of the protection of the information during the investigation phase.	6.11.3 It is submitted that clause 37(1)(e) restricts the sharing of information during the investigative phase. Once criminal proceedings are instituted, evidence that is tendered to proof the offence will become public knowledge and cannot be restricted.
	6.11.4 Centre for Constitutional Rights - page 12 (paragraph 11.27)	6.11.4 Clause 37(1), which strictly prohibits the disclosure of information which would relate to intercepted data in terms of clause 38, does provide additional exceptions to those set out in section 42 of RICA. In specific, an exception is made for "information sharing" as set out in Chapter 10 of the Bill. Chapter 10 of the Bill provides for the creation of various new structures to deal with cybersecurity, and the fact that no independent oversight is provided for to examine the manner in which this information is shared between these new structures, poses a real threat to the right to privacy.	6.11.4 Information sharing for purposes of Chapter 10 of the Bill relates to necessary measures to implement cybersecurity measures. The building blocks that is necessary for cybersecurity is referred to in clause 1.25. In order to handle cyber threats it is necessary to bring those threats to the attention of the structures that deal with cybersecurity. If these structures are not informed of the threats, how can they implement measures to address those threats? Clause 56 requires that regulations be made to regulate information sharing. The purpose of the regulations is to ensure that relevant necessary information is distributed and that the information is scrubbed of personal details that are obviously not

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			necessary to address cybersecurity. By implication information sharing for purposes of cybersecurity will be subject to the provisions of the POPIA with its protection mechanisms to ensure the lawfulness of making available personal information. The opinion that this exclusion poses a threat to the right of privacy is misconceived.
6.12 Clause 38: Interception of indirect communication, obtaining of real-time communication-related information and archived communication-related information	6.12.1 Cell C, Telkom and Vodacom - page 22 (paragraph 2.6.5)	6.12.1 According to the electronic communications service providers, the Bill now imposes onerous obligations on all to determine in what activities a person is engaged in. In other words, the Bill wishes to obtain sight of a person's activities on the Internet without the collection of metadata or the analysis of the contents of indirect communications where such information could previously be obtained and placed at the disposal of investigators through interception measures applied in terms of RICA.	6.12.1 * Clause 38(1) provides that the interception of indirect communications must take place in terms of an interception direction that is issued by the designated judge in terms of section 16 or 18 of the RICA. Clause 38(2) provides that the obtaining of real-time communication-related information must take place in terms of section 17 or 18 of the RICA. **These clauses therefore make it obligatory to use the RICA to obtain the communications in question.** * Clause 38(3) deals with service providers that must be RICA compliant in respect of the storing of call-related information, but who are not required in terms of the RICA directive to store such information. This clause ensures

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			that these service providers must on an *ad hoc* basis, act as required in terms of the Bill, to preserve call-related information. The service providers in question are internet service providers. Therefore: * If an electronic communications service provider is RICA compliant, subclauses (1) and (2) will be applicable and no obligations are imposed. * If there are no obligations to store call-related information, such service providers must on an *ad hoc* basis comply with provisions in the Bill that ensures that such information is captured and is preserved. These obligations can however, by means of the RICA directive, be imposed on them.
	6.12.2 Cell C, Telkom and Vodacom - page 22 (paragraph 2.6.7)	6.12.2 There is no safeguard against duplicate costs due to obligations under RICA and the Bill that may serve the exact same purpose (and deliver similar results).	6.12.2 As pointed out above, there is no duplication of costs if a service provider is RICA compliant. Cell C, Telkom, Vodacom and MTN do also operate an internet based service. It is noted that the Internet Service Providers Association (ISPA) has considered these provisions and no adverse comment were received from them.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	6.12.3 Cell C, Telkom and Vodacom - pages 22 and 23 (paragraphs 2.6.8)	6.12.3 (a) RICA contains prescripts that confine the role of the designated judge to solely effect and oversee the objectives of that Act. In the context of clause 38(3) and clause 46(6), the designated judge is now additionally commissioned to further the objectives of preservation of data, evidence or other article, seizure of data, the expedited disclosure of traffic data and data obtained from interception and preservation. According to the commentators the following difficulties arise: (i) An interception order in terms of RICA commonly holds a higher security classification than requests for information concerning more common criminality. Should orders be issued that otherwise instruct the preservation or seizure of data, a "confidential" status should be allocated to the order to enable staff receiving such order to forward orders to other departments and staff for execution thereof, without fear of prosecution. (ii) New obligations are imposed on electronic communications service providers to retain the results of lawful interception. The current RICA regime does not provide for such orders and it is submitted that technical prescripts must be added to the RICA regime to deal with these aspects. Reference is made to clause 46(7)(*b*) and it is indicated that "persons, electronic communications service provider and financial institution" may now be compelled to intercept	6.12.3 (a)(i) The classification status that is applicable to the RICA should *ipso facto* apply to the orders issued in terms of clause 38(4). These orders relate to indirect communications, real-time communication-related information and archived communication-related information and it is submitted that it cannot be treated otherwise. (ii) Where a service provider is RICA compliant, such communications will be routed to the Interception Centre, where it can be collected by law enforcement and stored pending the formal application for co-operation. Clause 46(6) does not necessarily give the designated judge the power to request service providers to preserve

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		communications, notwithstanding the fact that only electronic communications service providers must be able to do this in terms of RICA. It is pointed out that ordinary persons and financial institutions will not have the necessary facilities to intercept communications.	intercepted indirect communications. The RICA process will be applicable but in instances where a service provider cannot intercept and route the information, the option is always open the give an appropriate order to ensure interception and preservation. Extensive record keeping obligations is applicable to financial institutions and the clause must be interpreted in the context within which a financial service provider operates. Indirect communications within the context of financial institution relates to the financial information that is transmitted over their systems, and it is submitted falls within the definition of indirect communication of the RICA. Financial institutions can however not route this information to the interception centre and therefore need to be preserved.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	6.12.4 R2K - pages 10 to 12; ODAC - pages 6 to 7	6.12.4 Various criticisms are raised against the RICA. According to ODAC clause 38(1) and (2) provides that RICA must be used when getting evidence of call-related information and points out that the passing of a second law, providing how another must be implemented, is unusual. In future, to understand the relevant sections in RICA, you will have to read them with clause 38.	6.12.4 The concerns are noted. RICA is currently subject to a constitutional challenge. The Department is also revising the RICA. The constitutional challenge will however not adversely affect the Bill. It is not unusual in one law to refer to or make the provisions of other law applicable to a set of circumstances. The primary rule is to ensure that there is no conflict in the applications so incorporated. From the perspective of clause 38(1) and (2), it is submitted that these provisions merely demarcate the application of the Bill vis-a-vi the RICA. Clause 38(3) aims to provide for aspects that are not addressed in the RICA but which can be conveniently addressed in the Bill with reference to its object and purpose. Clause 38(4), aims to further regulate mutual legal assistance, where, among others, it is necessary to intercept communications in relation to cyber offences.
	6.12.5 Centre for	6.12.5 It is submitted that a revision of RICA together	6.12.5 The concerns about RICA are

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	Constitutional Rights - pages 5 to 6 (paragraph 9)	with the Bill is needed to ensure that effective procedural safeguards are built in, as required in terms of the Budapest Convention, especially considering concerns of interception of the communication of journalists in South Africa and the lack of any effective civilian oversight. Furthermore, it is submitted that the International Principles on the Application of Human Rights to Communications Surveillance (commonly known as the “Necessary and Proportionate Principles”) be specifically considered to measure the communication-surveillance measures of the Bill, with reference to RICA and the additional measures proposed in the Bill. The Budapest Convention specifically states that the “interception of content data” by the State is subject to article 15 which stipulates the need for safeguards and conditions to ensure adequate protection of human rights. Article 15(2) of the Budapest Convention specifically states that the “...conditions and safeguards, as appropriate in the view of the nature of the procedure or power concerned, inter alia, includes judicial oversight or other independent supervision, grounds justifying the application, limitation of scope and the duration of such power or procedure.”.	noted. Regarding the constitutionality of other provisions of the Bill that deal with search and seizure, the following: Search warrants are statutory creations designed to assist the State in its fight against crime. It has been held that the impact it has on an individual's right to privacy is necessary in order to strike a balance between the interests of the State and that of the individual. The provisions of the Bill, do strike a balance between the need for search and seizure powers and the right to privacy of individuals, similar to sections 20 and 21 of the Criminal Procedure Act, 1977. Thus construed, these provisions provide sufficient safeguards against an unwarranted invasion of the right to privacy. It follows, therefore, that the limitation of the privacy right in these circumstances is reasonable and justifiable. (Also see paragraph 2.2.5, above and the judgments summarised in Annexure B). Reference is made to the safeguard that is proposed by the Budapest Convention, which entails the following: * Proportionality in that the power or procedure shall be proportional to the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			nature and circumstances of the offence. * Judicial oversight. * Grounds justifying the application of the power and the limitation on the scope of the power. * Powers to be exercised must be reasonable and the impact on the rights, responsibilities and legitimate interests of third parties must be taken into account. (See paragraphs 145 to 148 of the Explanatory Report to the Convention regarding an interpretation of Article 15) It is submitted that the provisions of this Chapter are compliant with these safeguards that also form part of the law of South Africa, when the private sphere of persons are encroached upon.
	6.12.6 Centre for Constitutional Rights - page 8 (paragraphs 11.1 to 11.6) Various other concerns are raised against the RICA (paragraphs 11.7 to 11.20 of the	6.12.6 Clause 38 provides for additional unclear obligations on communications service providers, which is in conflict with the RICA. Clause 38(1) of the Bill specifically stipulates that an interception order must be issued in terms of the procedure as set out in RICA regarding the interception of "data", "which is an indirect communication" as defined in RICA. However, "data" in terms of clause 1 of the Bill is defined as "electronic	6.12.6 An indirect communication may qualify as "data" as is defined in clause 1, but clause 38(1) clearly states that data that qualifies as an indirect communication for the purposes of RICA must take place in terms of an interception direction that is issued by the designated judge in terms of section

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	submission).	representations of information in any form" and it is not clear whether it only includes "data" which relates to telecommunication as stipulated in RICA. This vagueness has to be clarified. In this regard it is also noted that the Minister of Justice and Correctional Services is acutely aware that section 205 of the Criminal Procedure Act has been abused to obtain "real-time" or "archived communication-related information" outside the procedure of RICA. The manner clause 38(1) is drafted appears to be an attempt to close this loophole but currently it is vaguely stated and it is submitted that it is also crucial that RICA be simultaneously revised in this regard.	16 or 18 of the RICA. In terms of section 1 of the RICA, an indirect communication is information, including a message or any part of a message, whether in the form of speech, music or other sounds; data; text; visual images, whether animated or not; signals; radio frequency spectrum; or in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system. The qualifier that distinguishes an indirect communication from other data, is the fact that it is being transmitted over an electronic communications system when it is to be intercepted. Clauses 27, 29, 30 and 31 can by no stretch of imagination be used to intercept an indirect communication. It is submitted that clause 38(1) is clear and should not be redrafted.
	6.12.7 Centre for Constitutional Rights - page 10 (paragraphs 11.14 and 11.15)	6.12.7 The definition of a "serious offence" in section 1 of RICA is specifically amended in terms of the Schedule to the Bill to also include the offences of "cyber fraud", "cyber forgery and uttering" and "cyber extortion", as well as "aggravated offences". This would now mean that if on the low threshold of a "reasonable belief" any of	6.12.7 The commentator loses sight of the fact that the current threshold in the RICA, is "a period of imprisonment exceeding five years without the option of a fine". What is not referred to by the commentator is the fact that these

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		these offences "has been or is being committed or will probably be committed", a designated judge may in terms of RICA issue an interception order. This considerably widens the scope of RICA with the addition of these "serious offences", which were initially restricted to offences such as high treason or sedition for instance, but read with the low threshold and the vagueness of core elements of these additional offences, it creates potential for abuse. This is worsened by the fact that the legality of the interception order cannot be reviewed.	offences must involve an amount of R200 000 or more to fall within the ambit of the RICA. It is submitted that the offences in question that are inserted in the Schedule definitely may incur punishment of 5 years or more without the option of a fine.
6.13 Clause 39: Expedited preservation of data direction	6.13.1 Cell C, Telkom and Vodacom - pages 21 to 22 (paragraph 2.5.16)	6.13.1 With reference to clause 38, the electronic service providers are of the opinion the Bill does not provide differently in respect of matters that resort under the RICA and that any preservation directions (clause 39) or disclosure directions (clause 42) that fall outside the ambit of RICA will be handled and served completely separately. The electronic communications service providers indicate that they agree to such an approach as it would not compromise the secure RICA processes. They, however, recommend that similar processes and prescripts be put in place when dealing with any preservation or disclosure directions, to secure the processes in question.	6.13.1 This is a correct interpretation of clause 39. Clause 39(1), is subject to clause 38(1) and (2) that provides for the interception of indirect communications or provision of call-related information, respectively. This means that clause 39(1) cannot be used to preserve that information. In terms of clause 38(3), the expedited preservation order would apply to service providers that are not required to store archived communication-related information. If a service provider is RICA compliant, clause 39(1) cannot be used to ensure data retention unless there is an extension of the period regarding archived communication-

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			related information whose storage period is to come to an end (the type of communication-related information that must be retained by service providers in terms of RICA are prescribed in terms of Government Notice No. 1325 of 2005). The clause mainly aims to target ISPs and other entities and persons that are not under an obligation to store data. It is submitted that it is not necessary to put in place similar processes or prescripts relating to the preservation of data as is contained in the RICA. It is submitted that it is not necessary to put in place similar processes or prescripts relating to the preservation of data as is contained in the RICA.
	6.13.2 Cell C, Telkom and Vodacom - page 24 (paragraphs 2.6.9.2 and 2.6.9.3)	6.13.2 The Bill gives no specific direction on any further data or evidence that must be preserved or would commonly be required under direction of police officials, magistrates or judges or the designated judge. Only "traffic data" as is intended in terms of RICA can be provided. It must accordingly be understood that it is a daunting prospect to be served with any order to obtain and preserve *data* or *evidence (clause 42)* to allow for criminal proceedings supported by expert testimony in cases of the commission of cybercrime(s) where these	6.13.2 (a) Clause 38(1), already excludes indirect communications and real-time communications on an ongoing basis. The ambit of these communications is defined in the RICA directive and need not to be preserved if a service provider is RICA compliant. As correctly pointed out, this procedure therefore relates to archived communication-related information.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		orders should apparently be complied with on an *ad hoc* and highly disruptive basis. Each order might require a unique or customised approach or solution that may not be immediately evident or may be costly or complex to implement. Some orders might in any event not be feasible and could be contested.	RICA compliant service providers only have an obligation to retain this type of information. ISPs do not have an obligation to store archived communication-related information and this procedure, therefore, is primarily intended to address this current operational shortcoming in the RICA. The coercive measures in the RICA can be used to impose this obligation on ISPs. However, in light of the need to roll-out internet throughout South Africa to all persons, the cost of compliance with such a directive may be disproportionate to the legitimate aim of ensuring that Internet services should be available to everyone. It is submitted that section 30 of the RICA in its current format is a blunt tool and require storage between three and five years, which may be unrealistic if it is applied to ISPs. This clause therefore balances the need of law enforcement to investigate crime with legitimacy and the need to ensure access to the Internet. ISPA considered this provision and did not object thereto. The clause was also specifically discussed with the ISPA and they acknowledged that this

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			is the least infringing mechanism that caters for the objectives of law enforcement and their obligations to ensure comprehensive affordable Internet coverage in the Republic. (b) The aim of clause 42 is misunderstood. The correct reference in the presentation should be to clause 40 and not clause 42. Clause 40 deals with preservation of evidence (hardware (computers) and software (data/programs)). It is submitted that this must be construed as an order that will ensure integrity and the availability of evidence until it is dealt with further in terms of the Chapter. The aim is to ensure that the least disruptive mechanism that is needed to investigate crime is implemented thereby serving the public interest, that crime should be addressed and the need of the affected party to continue with its daily activities subject to the preservation order until the article can be dealt with in terms of clause 27(seizure) or where data can be dealt with in terms of clause 42(disclosure of data). Since the police do not seize the data in question, there must be a safety

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			mechanism to ensure that authenticity and reliability of evidence is preserved, and in order to achieve this, obligations are imposed on the party in whose possession the data is, to provide assurances to the court as is set out in clause 42(8). Clauses 40(5) and 42(6) both provide that these procedures may be challenged on the basis that the service provider or person "cannot in a reasonable fashion comply" with the procedures. In any event the "scales clause" as is provided in clauses 40(1) ensures that the procedure must be implemented with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence, limits the procedure in question.
	6.13.3 Cell C, Telkom and Vodacom - pages 24 to 25 (paragraph 2.6.10)	6.13.3 Preservation of data directions might necessitate the involvement of individuals that do not have a sufficient security clearance. Also preservation of data directions may impact on the availability of resources of electronic communications service providers to store the information. Equipment used for preservation of data may also be classified as listed equipment as contemplated in section 44 of the RICA and in order to	6.13.3 * RICA already imposes obligations on service providers to record and store the required information that is necessary for criminal proceedings. The contention that the procedure may impact on available resources to store data is addressed in paragraph 6.13.2.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		possess such equipment an exemption needs to be obtained in terms of section 46 of the RICA, otherwise the use and possession of such equipment will be unlawful. The electronic communications service providers are also concerned with the cost implications of preservation orders.	* The involvement of persons that do not have sufficient security clearances is a basis on which the preservation direction may be challenged in that a service provider cannot in a reasonable fashion comply with the direction. It was already pointed out that a service provider does not need to obtain additional experts to give effect to a preservation order. If the service provider does not have persons capable to implement the measure it can request a court to set aside the direction. * The contention that the preservation direction may involve the use of listed equipment that is prohibited under section 44 of the RICA is incorrect. By virtue of the RICA Directive, read with section 30 of the RICA all service providers must have the capability to intercept communications and store communication-related information, unless they are an Internet service provider who currently only have obligations to intercept communications. This capability to intercept includes the implementation of technical solutions on their systems to intercept

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			communications. The uses of these devices are therefore specifically authorised. On the other hand most service providers keep billing information for a certain period, which is basically the same information that will form the subject of a preservation order.
	6.13.4 Banking Association SA - page 3	6.13.4 Clause 39(2)(*a*), by implication extends the period for which archived communication-related information is to be stored as is required in terms of RICA. This is an implied obligation. For certainty and clarity, it is suggested that an express provision be used to require an extended retention period for this information by electronic communication service providers.	6.13.4 The period that is prescribed in terms of section 30(2)(a)(iii) of the RICA is three years. The period can be extended to five years. However, it is submitted that to extend this period to all archived communication-related information, may have undue cost implications for service providers and may also be challenged on constitutional grounds (see among others DIGITAL RIGHTS IRELAND LTD V MINISTER FOR COMMUNICATIONS, MARINE AND NATURAL RESOURCES AND OTHERS (IRISH HUMAN RIGHTS COMMISSION INTERVENING) ((Joined Cases C-293/12 and C-594/12), where the data retention period under Directive 2006/24/EC was declared invalid). It is submitted to extend a statutory period for retention of

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			information for specific purposes is however justifiable.
	6.13.5 Centre for Constitutional Rights - page 12 (paragraphs 12.1 and 12.2) and (paragraph 12.4)	6.13.5 In terms of clause 39(1) of the Bill it appears that a "specifically designated police official" may, subject to clause 38(1) and (2), issue an expedited preservation order if there are "reasonable grounds" to believe that any person may receive data which may in various and vague ways be connected to the intended commission of any cybercrime or malicious communication provided for in the Bill. The above clause is confusing on several grounds. Firstly, it is not clear whether, if the designated judge who granted the interception order has to be approached again, or if the "designated police official" on the strength of an interception order can "issue" a direction for an expedited preservation order. If the latter is the case, it would seriously infringe the right to access to courts as any judicial oversight of the process of applying for a preservation order is removed at this instance. This clause has to be clarified.	6.13.5 Clause 39(1)(*a*) excludes information that is subjected to a directive by the designated judge from the application of this provision. In terms of section 19 of the RICA, archived communication-related information may be obtained in terms of a direction issued by other judicial officers. This however only relates to archived communication-related information that is stored in terms of the RICA. ISPs and other entities, that do not qualify as electronic communications service providers are not under obligation in terms of RICA to store archived communication-related information and section 19 of the RICA can therefore not be utilised. In practise section 205 of the Criminal Procedure Act may be used to acquire such information. However this is subject to the fact that the person or entity has stored this information and therefore operates ex post facto. In terms of clause 39, where there is reasonable

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			grounds to suspect that a cyber-related offence is being or may be committed, clause 39 may be used as a measure to compel a person or entity to store relevant information for a period of 21 days, subject to an extension of the period in terms of clause 40, whereby the period may be extended up to 90 days. Data subject to a preservation order may be made available only on judicial authorisation as is provided for in clause 42 (disclosure of data direction)
	6.13.6 Centre for Constitutional Rights - page 12 (paragraph 12.3)	6.13.6 An interception order granted under clause 38 is supposed to be justified on the basis of the fact that the communication to be intercepted would lead to the evidence of a serious offence or of an actual threat to public safety or national security for instance. However, clause 39 makes it clear that the area of the interception is in fact much wider and this raises a serious threat to the right to privacy.	6.13.6 As pointed out in paragraph 6.12.1, there is no extension of interception measures under any circumstances in so far as it relates to indirect communications and communication-related information on an ongoing basis. Data subject to a preservation order may be made available only on judicial authorisation as is provided for in clause 42 (disclosure of data direction)
	6.13.7 Centre for Constitutional Rights	6.13.7 Clause 39(2) makes it clear that clause 39(1) also applies to “archived communication-related information”	6.13.7 The rationale for the period of extension is that the information on

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	- page 12 (paragraph 12.4)	and electronic communication providers might even be required to provide this information after the maximum required years that obliged electronic communications service providers to retain such information has lapsed. This specific clause creates uncertainty, as it goes beyond RICA and it is unclear for how long and in what manner such "communication-related information" must in fact be retained.	reasonable grounds relates to a cybercrime and that it further be preserved. As is pointed out above clause 39 may be used to extend the period of preservation to 21 days. A period of extension of up to 90 days can further be granted in terms of clause 40, by a judicial officer.
	6.13.8 Centre for Constitutional Rights - page 12 (paragraph 12.5)	6.13.8 Clause 39(1)(*a*) to (*e*) is vague, especially if one considers that a preservation of property order in terms of the Prevention of Organised Crimes Act, for instance, only refers to the request for a preservation order of property which on reasonable belief is an "instrumentality of an offence".	6.13.8 Clause 39(1), requires that the functionary must "on reasonable grounds believe" that the data is involved in a cybercrime. This believe must be based on reasonable grounds, which makes the test an objective test with reference to information that is at the disposal of the police official that a cyber offence has or is being committed.
	6.13.9 Information Regulator - page 6	6.13.9 The preservation of data should be considered in light of the eight principles relating to data protection.	6.13.9 Section 3(2)(*b*) of the POPIA provides that if any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3, the extensive conditions prevail. Section 6(1)(*c*)(ii) of the POPIA provides that the POPIA does not apply

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			to the processing of personal information by or on behalf of a public body for purposes to detect or investigate unlawful activates to the extent that adequate safeguards have been established in legislation for the protection of such personal information. Without evaluating the eight principles on which the POPIA is based (accountability, processing limitation, purpose specification, further processing limitations, information quality, openness, security safeguards and data subject participation), it is submitted that clause 39, within the ambit of Chapter 5 of the Bill, provide for appropriate safeguards to protect the right to privacy of information. In terms of clause 39: * There must be a reasonable suspicion that an offence is being committed before the police may request a preservation of evidence direction. * Only specific police officials may issue preservation of data directions, namely a commissioned officer that was authorised by the National Commissioner to issue such orders. Not every police official can therefore at will

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			approach a service provider * Police may not access this information and the service providers may not provide this information to the police unless it is authorised by a disclosure of data direction in terms of clause 42. The disclosure of data direction can only be granted by a judicial officer if application is made under oath to a judicial officer and it appears to the judicial officer that there is reasonable grounds to believe that an offence as contemplated in the Bill was or is being committed and that the preserved data in question may afford evidence of the offence. * The Chief Justice may issue directives to further regulate applications for disclosure of information. * No information obtained as a result of a preservation order may be made available to others, unless it falls within the exceptions of clause 37. * Preservation is restricted to 21 days only and can be extended by a judicial officer to a further 90 days. * A false application for a protection order is criminalised in terms of clause 36(1)(*d*) and civil liability may follow in terms of clause 36(2).

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			* A court may in terms of clause 42(5) may impose specific conditions or restrictions relating to the provision of data authorised in a disclosure of data direction. The right to privacy is not meant to shield criminal activity or to conceal evidence of crime from the criminal justice process – INVESTIGATING DIRECTORATE: SERIOUS ECONOMIC OFFENCES AND OTHERS v HYUNDAI MOTOR DISTRIBUTORS (PTY) LTD AND OTHERS; IN RE HYUNDAI MOTOR DISTRIBUTORS (PTY) LTD AND OTHERS v SMIT NO AND OTHERS 2000 (2) SACR 349 (CC) at paragraph 54. The court referred to CALIFORNIA V CIRAOLO 476 US 207 (1985) at 213-4, where Chief Justice Warren Burger held: "that a person who was using a garden to grow illicit drugs could not expect it not to be searched by the State. The following has been said in Colb 'Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence' (1996) 96 Columbia Law Review 1456, 1460: '[I]f a government official knows that an individual is using her privacy to commit crimes and to hide evidence of those crimes, the official is

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			legally entitled to a warrant authorising a search of the individual's premises. By committing a crime, the individual in effect creates the circumstances that may ultimately relieve the government of its obligation to respect her privacy.'. In THINT (PTY) LTD V NATIONAL DIRECTOR OF PUBLIC PROSECUTIONS AND OTHERS; ZUMA V NATIONAL DIRECTOR OF PUBLIC PROSECUTIONS AND OTHERS 2008 (2) SACR 421 (CC), where the court, after stressing the importance of an understanding of the range of protections for the right to privacy at the different stages of a criminal investigation and trial, added in paragraph 80: "Courts must take care that in ensuring protection for the right to privacy, they do not hamper the ability of the State to prosecute serious and complex crime, which is also an important objective in our constitutional scheme."). An interference should however be constitutionally justifiable. The POPIA is based on general principles applicable to the EU and among others aims to give effect to Article 8 of the European Convention on

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			Human Rights, which guarantees the right to respect for private and family life, home and correspondence. Various judgments has confirmed that the right to privacy must yield to the public interest to investigate and prosecute crime (see among others UZUN V GERMANY Application No 35623/05, where this was applied within the context of the preservation of evidence for criminal proceedings. In light of the above it is submitted that clause 39 complies with section 6(1)(c)(ii) of the POPIA.
6.14 Clause 40: Preservation of evidence direction	6.14 Cell C, Telkom and Vodacom – page 21 (paragraphs 2.5.16 and 2.6.6)	6.14 There are no regulatory impact assessments of the cost of compliance that have been conducted in order to assess the financial burden that may be associated with compliance with the directives proposed in Chapter 5 of the Bill.	6.14 See paragraph 6.13.2(b), above
6.15 Clause 41: Oral application for preservation of evidence direction	6.15 Cell C, Telkom and Vodacom – page 21 (paragraph 2.5.16)	6.15 There are no regulatory impact assessments of the cost of compliance that have been conducted in order to assess the financial burden that may be associated with compliance with the directives proposed in Chapter 5 of the Bill.	6.15 See paragraph 6.13.2(b), above
6.16 Clause 42: Disclosure of data direction	6.16.1 Cell C, Telkom and Vodacom – page 21 (paragraph 2.5.16)	6.16.1 There are no regulatory impact assessments of the cost of compliance that have been conducted in order to assess the financial burden that may be associated with compliance with the directives proposed in Chapter 5 of the Bill.	6.16.1 See paragraphs 6.13.1 (no undue obligations); 6.13.2 (aims to address the needs of ISPs) and 6.13.2 (b) (order for criminal cases to ensure party in possession of device or digital

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			evidence are not unnecessarily burdened).
	6.16.2 Cell C, Telkom and Vodacom – page 24 (paragraph 2.6.9.5)	6.16.2 A disclosure of data direction is expected to convey further instructions to refine the data to be disclosed (this is presumed to include the analysis and filtering of data previously preserved, by order) and the format in which such data must be provided (ad clause 42(2)(*d*))(this is presumed to further prescribe the preparation and pre-processing of data prior to submission for further forensic analysis, in a specific format). It cannot be assumed that such data processing/formatting facilities are readily available or can otherwise be readily acquired or operated with little skill by electronic communications service providers.	6.16.2 The commentator does not take the operation of clause 42(6) into account that provides that a service provider may apply for the cancelation of the direction if such service provider cannot in a "reasonable fashion comply with the direction". Service providers do not need to acquire additional expertise or resources to give effect to their statutory obligation in terms of this clause or to implement technical measures that are not available to such service provider.
	6.16.3 Cell C, Telkom and Vodacom – page 26 (paragraph 2.6.11)	6.16.3 Clause 42 also covers the preservation of evidence (clause 42(1)(a)). It remains uncertain how and under what conditions and authority, custody of preserved evidence (or article) must be transferred to criminal investigators. Such evidence could be a whole computer system that may also be of significant monetary value.	6.16.3 The aims of clause 40 (preservation of evidence) have been discussed under paragraph 6.13.2(b). The reference to an "article" in that clause means that it covers "any data, computer program, computer data storage medium, or computer system". However, clause 42 only covers data and provides for the manner in which data must be dealt with. Objects that are preserved must be seized in terms of clause 27 and further be dealt with in

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			terms of the Criminal Procedure Act (clause 25). In order to clarify the clause, the following amendment is proposed: Heading: **Disclosure of data direction and seizure of articles under preservation** Addition of following subsection: "(10) (*a*) A police official may, at any time, apply for a search warrant in terms of section 27(1) to search for, access or seize an article that is subject to a preservation order. (*b*) Articles under preservation that is not "data" must be seized in terms in terms of section 27(1).".
6.17 Clause 43	6.17.1 Banking Association of SA - page 3	6.17.1 Clause 43 requires some clarification as the wording is not clear and raises the following concerns: (a) The expression, "confidentiality and limitation of use" is used in this clause (as well as a number of other clauses relating to granting a police official access to data). Will this not have an effect on other laws, for example, certain provisions of the PAIA and POPIA? If it does have an effect, it is suggested that "confidential and limitation of use" be defined in the Bill.	6.17.1 (a) When data is made available it will be subject to other laws on the Statute Book that regulates "confidentiality and limitation of use" in respect of data that is made available. Clause 6(1)(*c*) of the POPIA makes provision for instances where the POPIA does not apply, if necessary safeguards are built into legislation relating to the investigation and detection of unlawful activities. In the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			interpretation of this clause, due regard must be had to the eight principles for processing of personal information as is provided for in the POPIA. In terms of section 37(1) of the POPIA, the Regulator may, by notice in the *Gazette*, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information, or any measure that gives effect to such condition, if the Regulator is satisfied that, in the circumstances of the case the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing. In terms of section 37(3) of the POPIA, the Regulator may impose reasonable conditions in respect of any exemption granted under subsection (1). In terms of section 37(2), public interest is defined as to include that of national security and the prevention, detection and prosecution of offences. The effect of this provision is that the Bill cannot and should not deal with this aspect and that the Regulator has the final

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			responsibility to determine what is allowable. The courts have already interpreted the right to privacy under the Constitution extensively and the sharing of information must fall within the ambit of such interpretations until POPIA is functionally implemented.
		(b) Section 43(1)(*a*) states that it applies "regardless of the geographical location of the data". Will this not be viewed as contravention of foreign law and also having cross-border implications?	(b) Clause 1 of the Bill defines "**publicly available data**" as data which is accessible in the public domain without restriction. If anyone else can access it so can police officials. The problem with this clause is however the use of the word "seize". Where a police official accesses this data and downloads or prints it, it should not be regarded as a seizure. It is proposed that paragraph (a) be substituted with the following paragraph: "***(a)*** **[search for, access or perform the powers referred to in paragraphs *(c)* or *(d)* of the definition of "seize" in respect of]** obtain and use publicly available data regardless of where the data is located geographically; or".

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(c) Paragraph (*b*) states that disclosure is voluntary. Does this mean that a request for access to information can be declined and if so, what are the implications for such a decline?	(c) Clause 43(*b*), aims to deal with the situation where a person, who has lawful authority, to disclose the data, goes to a police station and furnishes the data to a police official. Furthermore, the terms and conditions under which that information is furnished to the police will dictate the manner in which that information may be used. Access to information is addressed in the PAIA, and it is submitted that once such information forms part of a police investigation access thereto cannot be acquired in terms of the PAIA.
	6.17 2 TBCSA - page 3 (Item 4)	6.17.2 The clause provides that a police officer may search for or seize publicly available data…without any specific authorisation. How does the Bill deal with police abuse of power in cases where it is used for personal gain?	6.17.2 See paragraph 6.17.1, above. It is difficult to see how the police can abuse a power in so far as it relates to publicly available data.
	6.17.3 IM Governance - page 1 (paragraph 2)	6.17.3 Clause 43(b) must be amended to include "such conditions regarding confidentiality and limitation of use which he or she deems necessary <u>to comply with the conditions for processing personal information lawfully</u>".	6.17.3 The fact that a person has "lawful authority" implies that he or she consents that the police may use that information. The person who hands the information to the police may determine

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			the extent of how this information may be used. Lawful authority in the context of clause 43(1)(*b*), implies that the person has lawful authority to all data that is provided to the police. The application of POPIA is discussed under paragraph 6.17.1(a), above.
	6.17.4 Information Regulator - page 6	6.17.4 This clause should be reconsidered in light of the POPIA.	6.17.4 Regarding clause 43(*a*), it is submitted that POPIA cannot be applicable if the data qualifies as publicly available data as is defined in clause 1 of the Bill (see paragraph 6.17.1(b)) * Regarding clause 43(*b*), see paragraph 6.17.1 (a).
7. CHAPTER 6: MUTUAL LEGAL ASSISTANCE			
7.1 Clause 45: Spontaneous information	7.1.1 IM Governance - page 2 (paragraph 3)	7.1.1Clause 45(1) should be amended to read: "The National Commissioner may, on such conditions regarding confidentiality and limitation of use as he or she may determine and after obtaining the written approvals of the National Director of Public Prosecutions as contemplated in subsection (2) <u>and of the Information Regulator"</u>	7.1.1 As pointed out above the functions and powers of the Information Regulator *vis-a-vis* legislation are provided for in section 40(1)(*b*)(ix) of the POPIA that provides for the examining of any proposed legislation only. The Information Regulator plays an oversight role and this role may be compromised should it become involved in the granting of approvals.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
7.2 Clause 46: Foreign requests for assistance and cooperation	7.2.1 IM Governance - page 2 (paragraph 4)	7.2.1 Clause 46(1) should be amended to provide that the request must also be submitted to the Information Regulator.	7.2.1 See clause 7.1.1 above.
7.3 Clause 48: Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data	7.3.1 Cell C, Telkom and Vodacom - pages 26 to 27 (paragraph 2.7)	7.3.1 The electronic communications service providers give an outline of this Chapter and refer to clause 48(2), which provides for the submission of traffic data to a foreign country. The question is then asked as to whether section 48 envisages a deviation from the RICA process and more particularly as to whether the information should be handed to a designated police official who will then provide it to the 24/7 point of contact.	7.3.1 Clause 46(1)) provides that the order must be executed by a designated police official. This implies that the police official must receive the information and then submit it to the 24/7 point of contact. The designated judge may however in his or her discretion specify the manner in which the information must be handed over. The obligations of the service providers in terms of the RICA are to either route the information to the Interception Centre or provide such information to the law enforcement agencies. In most instances information of this nature is also obtained in terms of section 205 of the Criminal Procedure Act, 1977. The Chapter therefore does not deviate from current practices in terms of which information is made available to the law enforcement agencies.
8. CHAPTER 7: ESTABLISHMENT OF 24/7 POINT OF CONTACT			

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
8. Clause 50: Establishment of the 24/7 point of contact	8.1 Western Cape - page 2 of Annexure to letter; Cell C, Telkom and Vodacom - pages 27 (paragraph 2.8)	8.1 This clause is supported. The point of contact should be adequately resourced and staffed otherwise it will not be effective.	8.1 Noted.
	8.2 IM Governance - page 2 (paragraph 5)	8.2 Clause 50(1)(*a*) should be amended to provide for the appointment of deputy information officers dedicated to cybercrime as is necessary to be readily accessible to data subjects.	8.2 The Department disagrees. The application of the POPIA cannot be extended to include aspects that will impede of the criminal process relating to the investigation of crime.
9. CHAPTER 8: EVIDENCE			
9.1 Clause 51: Proof of certain facts by affidavit	9.1 Cell C, Telkom and Vodacom - pages 4 and 27 (paragraphs 1.1.6 and 2.9)	9.1 The outcome of the investigation by the SALRC should be taken into account.	9.1 See paragraph 1.16, above.
	9.2 DFIRLABS - pages 9 and 10 (paragraphs 4.7 to 4.9)	9.2 This clause has the following shortcomings: (a) No provision is made in this clause to identify the person who made an affidavit as an expert witness. In terms of the clause any person who possesses the necessary skills in aspects referred to in section 51 can make an affidavit. It is proposed that clause 51(1)(i)	9.2(a) It is submitted that clause 51(ii), already addresses this aspect. The commentator is of the opinion that the SOPs issued in terms of clause 24 should prescribe the competency of persons that may conduct digital

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		should be amended in order to make provision for "relevant qualifications, expertise and experience as defined in regulations issued in terms of clause 24 of the Bill". (b) Clause 51(1)(i) should further include digital forensic practitioners in the employ of a private body prescribed by notice in the *Gazette*".	forensic investigations. If such standards are provided for in the SOPs, clause 51(ii) should be interpreted that the clause in question will apply to those persons. In any event, the fact whether a person can be regarded as an expert, is in the discretion of the court. Appropriate qualifications do not necessarily make a person an expert and experience is also required. On the other hand persons without qualifications have been regarded as experts. (b) Such provision will greatly clarify the ambit of use of clause 51, if the categories of persons are identified by notice in the *Gazette.* Persons that do not fall within the prescribed category of persons therefore need to give evidence *viva voce.* The concern is however, that it may be difficult to comprehensively identify all categories of persons that must be regarded as competent to make use of this clause. The courts should rather be afforded discretion in order to determine whether a person complies with clause 51(ii).

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		(c) Clause 51(1)(iii) should be amended to state "has established such facts by means of a scientifically validated and documented examination process, which is fully documented in the affidavit".	(c) From the perspective of digital forensic investigations a "scientifically validated and documented examination process" is always required. This is part of the SOPs. However, there may be instances where this is not a requirement, for instance the identification of an artefact. The insertion of such requirements, that will in general be applicable to the categories listed under paragraph (a) to (f) of clause 51(1), may unduly restrict the ambit of this provision and open up the clause to unnecessary challenges. On the other hand, a documented examination process will also ensure that the other party to proceedings are fully informed of the nature and extent of the evidence that may be adduced in criminal proceedings. The SOPs in terms of clause 24 should deal with this aspect.
		(d) A paragraph (*d*) should be added to subsection (5) in order to provide that the "opposing party may request that the person who makes the affidavit should submit himself or herself for cross-examination".	(d) It is submitted that clause 51(3) and 51(5)(*c*), already provides for such an eventuality. These provisions state that the court before which an affidavit is produced as *prima facie* proof of the relevant contents thereof may, in its

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			discretion, cause the person who made the affidavit to be subpoenaed to give oral evidence in the proceedings or may request that the affidavit be clarified. In terms of section 212 of the Criminal Procedure Act, where an aspect is challenged, the maker of the affidavit is usually called to testify (see among others S v HLONGWA 2002 (2) SACR 37(T)).
10. CHAPTER 9: OBLIGATIONS ON ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND FINANCIAL INSTITUTIONS			
10. Clause 52: Obligations on electronic communications service providers and financial institutions to report cybercrime to the SAPS and to retain information	10.1 ISPA - paragraph 10 10.2 Banking Association SA - page 4	10.1 ISPA supports the inclusion in the Bill of subclause 52(4), which affirms the position under the Electronic Communications and Transactions Act that ECSPs are not required to monitor all data passing over their networks or to actively seek out facts or circumstances indicating any unlawful activity. This reflects the reality of communications service provision as well as the fundamental right of South Africans not to have the privacy of their communications infringed upon. 10.2 Clause 52(4) of the Bill does not place obligations on ECSPs and financial institutions to continuously monitor data. However, the BIS Guidance on Cyber	10.1 Noted. 10.2 Clause 52(4) is “subject to any other law or obligation”, meaning that if there is other obligations on financial

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
which may help in the investigation of cybercrimes		resilience referenced by the recently issued SARB Guidance Note 4/2017, Financial Market Infrastructures (including financial institutions) are required to do continuous monitoring in order to detect anomalous activities and events. The BIS Guidance on Cyber resilience addresses the aspect of detecting a cyberattack and continuous monitoring which requires an FMI to establish capabilities to continuously monitor (in real-time or near real-time) and detect anomalous activities and events. One practice that may help to accomplish this is to set up what is commonly referred to as a "Security Operations Centre". These capabilities should adaptively be maintained and tested. It is suggested that the SARB Guidance Note be aligned to the Bill, and clarity be provided on which one takes precedence.)	institutions, those obligations will prevail.
	10.3 ISPA	10.3 Subclause 52(3) should be amended to allow for a discretion in the quantum of any fine imposed upon an ECSP for a contravention of subclause 52(1). The following wording are suggested: "An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine of not exceeding R50 000.".	10.3 Agree. Proposed amendment to subsection (3): "(3) An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine **[of]** not exceeding R50 000.".
	10.4 Western Cape - pages 2 and 3 of Annexure to letter	10.4 The penalty of R50 000 is insufficient to compel the institutions to give effect to their obligations in terms of the clause and should be revisited.	10.4 The Department is of the view that the fine suggested is sufficient to compel compliance, especially when

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			considered in light of the adverse effect of public perceptions that a service provider in not complying with statutory obligations to address cybercrime is concerned.
	10.5 Cell C, Telkom and Vodacom - pages 27 and 28 (paragraph 2.10)	10.5 The electronic communications service providers remarked that clause 52 should not be interpreted as to imply that the mere conveyance of a data message by an electronic communications service provider's computer system would imply that its computer system is involved in the commissioning of any category or class of offences provided for in Chapter 2.	10.5 It is important to ascertain which systems are used in the commission of offences and to that extent the use of such a system falls within the ambit of the provision. The perceived wide extent of the application of the clause is, however, addressed through the following measures: * The category of offences that must be reported will be prescribed in terms of clause 52(2). From the International experience, this will only involve serious crimes that have been committed (involving a loss or damage exceeding R50 000). * There is no active duty on electronic communications service provider as opposed to financial institutions to actively monitor their systems for involvement in offences.
	10.6 Michalsons Attorneys - pages 8	10.6 The clause does not consider that the ECSP or financial institution may have its own internal incident	10.6 Clause 52(1)(a) provides adequate leeway for service providers to first

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	to 9	response policy that deals with this situation. For example, it does not consider that an ECSP may not want to broadcast that they have had a breach in their systems especially if they have not had the opportunity to address it internally and fix it, before they report it to the police. There is a big risk to an ECSPs' reputation especially if they have to report every single incident. Reporting should take place after they have exhausting their internal policies to deal with the issue and reporting to the police should not be required for every single circumstance. High priority incidents should be reported to the police. Incidents that can be dealt with internally should not be required to be reported. This reporting section should consider section 22 of POPIA which deals with the notification of security compromises and requires notification as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system." This approach allows the ECSP or financial institution to implement its internal incident response policies. The clause should be reworded considering these POPIA requirements. Reference is made to the European Union's General Data Protection Regulation (GDPR) where in terms of Article 33(1) it is required a data breach should be reported "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural	address the vulnerability before reporting it to the police. The clause provides that the incident must be reported "without undue delay and, where feasible, not later than 72 hours after having become aware of the offence". It is not envisaged that each and every cyber incident should be reported. The category of offences that must be reported will be prescribed in terms of clause 52(2). From the International experience, this will only involve serious crimes that have been committed (involving a loss or damage exceeding R50 000). This provision therefore gives effect to the suggestion that only high priority incidents should be reported.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		persons." A risk-based approach should be followed to ensure that the police are not overrun with ECSPs and financial institutions reporting every single incident to them. An ECSP or financial institution should be allowed to give reasons where they do not report an incident with 72 hours. There should also be a possibility of an extension to the time period.	
	10.7 Michalsons Attorneys - pages 8 to 9	10.7 The requirement in the clause that ECSPs or financial institutions preserve any information that can assist in an investigation, is not feasible as the information may be located in various forms such as servers, cloud storage etc. Storing that amount of information for an unspecified time is not realistic. A time period should be put in place so that ECSPs or financial institutions are not holding the information for indefinite period. The Minister of Police must also prescribe how long ECSPs or financial institutions must preserve data necessary to assist in investigations.	10.7 The duty to preserve is to ensure that the police may use that information in the investigation of an offence. A reasonable period is envisaged. Once the information is handed over to the police, there is in general no further need to keep the information. This is however dependant on the circumstances of a matter. Some providers will keep this information for a certain period as a result of possible civil claims that may flow from the offence in question.
	10.8 Michalsons Attorneys - pages 8 to 9	10.8 The fine in clause 52(3) does not consider the size of the organisation and whether the amount would be feasible for small ECSPs or irrelevant to large ones. The fine should be a percentage of annual turnovers, like the mechanism in the GDPR.	10.8 See paragraph 10.3. It is submitted that the proposed amendment will cater for small service providers. From experience, electronic communications service providers strive to comply with their statutory obligations and it is the

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			possibility of a conviction that serves as deterrent and not necessarily the extent of penalty that is imposed.
	10.9 MTN - page 9 (paragraph 3.3)	10.9 It is submitted that clause 52(2), should also provide that the manner in which the prescribed crimes must be reported to the SAPS must be done on a confidential basis.	10.9 All information relating to a criminal investigation is confidential. This aspect will further receive attention during the drafting of the notice contemplated in clause 52(2).
	10.10 Deloitte - page 3	10.10 Clause 52(1)(a): It is proposed that “feasible” be defined as it is unclear and could lead to the requirement being ineffective as it contradicts the requirement for reports to be made within 72 hours.	10.10 It is submitted that the word “feasible” in the context of the clause means “where practical” or “where reasonable”. The commentator referred to in paragraph 10.6, pointed out that there may be circumstances which will not make this reporting within 72 hours feasible, namely that the entity in question must first try to address the vulnerability. If a vulnerability is not addressed it will be dangerous to publicise that certain vulnerability exists, since it may give rise to further offences based on the vulnerability
	10.11 Deloitte - page 3	10.11 Clause 52(3): It is not very clear how the fine will be attributed. Will an electronic communications service provider or financial institution be fined R 50 000 per category/class of offence or per offence which it fails to	10.11Clause 52(3) is clear that each time an entity fails to report a prescribed offence the entity would contravene clause 52(3).

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		report timeously.	
	10.12 Minister of Finance - paragraph (b)	10.12 Clause 52(5) excludes from its application a financial sector regulator or function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989. Since the South African Reserve Bank also performs functions in terms of other legislation, it is proposed that the following words be added after "the South African Reserve Bank Act, 1989", namely "or any other legislation". Other legislation includes the Currency and Exchange Act, 1933 and the National Payment Systems Act, 1998.	10.12 Agree. Proposed amendment to clause 55(5): "(5) This Chapter does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989, or any other legislation.".
	10.13 All Rise - page 5	10.13 It is proposed that similar reporting requirements as well as the requirements relating to assistance should be imposed in respect of cyber harassment.	10.13 The rationale for the reporting requirement is to ensure – * that serious cybercrimes are reported; * that the nature of cybercrimes can be determined in order to ensure the implementation of adequate measures to deal with these crimes; * statistic are available of the extent of cybercrime and the effectiveness of law enforcement and the Prosecuting Authority to deal with these offences it is prosecuted. Although the clause does not deal with malicious communications, the established Cyber Hub, do provide for the reporting of cybercrimes in terms of

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
			the Bill. Statistics can further be obtained from the service providers regarding protection orders that was served on them in terms of clause 19 of the Bill and statistics that is kept by courts. Clause 60 provides that the National Prosecuting Authority has a duty to keep statistics on the prosecution of offences contemplated in clauses 16, 17 and 18 of the Bill.
	10.14 MTN - page 3 (paragraphs 13 to 18); Internet Solutions - pages 8 to 10 (paragraph 2.1)	10.14 A concern is raised that this provision may adversely impact on the general obligations of electronic communications service providers to ensure the confidentiality and privacy of communications. It is pointed out that in terms of the RICA electronic communications service providers may only in narrowly defined instances retain and access certain information. It is requested that special consideration be given to align the legislative provisions to enable electronic communications service providers to assist the law enforcement agencies. Internet Solutions also indicates that the Bill does not define at what stage the electronic communications service provider or financial institution should be deemed as "being aware" of an offence. According to Internet Solutions, electronic communications service providers receive a number of complaints on a daily basis alleging that offences have been committed on their networks but this, however.	10.14 Clause 52(4), specifically ensures that service providers are not required to actively monitor their systems for criminal offences. In most instances a complainant will bring an offence to the attention of a service provider or the service provider may itself detect an offence where it is committed against their system. In such circumstances sections 4 (interception of communication by party to communication), 5 (interception of communication with consent of party to communication), and 6 (interception of indirect communication in connection with carrying on of business in so far as it relates to the business) of the RICA must be considered. However, it is not

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
		does not determine whether or not an offence has indeed been committed.	envisaged that preservation of indirect communications will be required. Where communication-related information is involved and the service provider is RICA compliant, it is submitted that much of these information will be stored in terms of their RICA obligations. In any event the clause in question must also be seen as an authorisation that can be used to retain information directly relating to an offence and must be read in conjunction with section 15 of the RICA that deals with the availability of other procedures for obtaining real-time or archived communication-related information. Regarding the concern of Internet Solutions, clause 52(1), specifically states that a computer system must be involved in the commission of an offence and will usually entail that the service provider has received information from a client, investigated the matter and is of the opinion that its computer system is involved in the commission of an offence.
	10.15 Liquid Telecom - page 4 (paragraph	10.15 Chapter 9 of the Bill is in line with the right of privacy as enshrined in the Constitution, the ECTA and	10.15 Noted

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	14 to 17)	the RICA, in that it prohibits unlawful monitoring of communications and does not provide that a service provider must actively monitor communications to detect crime. It is pointed out that this provision of the Bill applies to all electronic communications service providers which are dissimilar with the RICA which imposed obligations on only certain service providers.	
	10.16 IM Governance - page 3 (paragraphs 6 and 7)	10.16 Clause 52 should be amended to provide that an electronic communications service provider must appoint such number of information officers with authority to establish procedures for its clients to report cybercrimes to the electronic communications service provider's information officer. Provision should also be made that the offence should be reported to the Information Regulator.	10.16 This aspect is addressed above. As pointed out, the POPIA has a specific area of application, namely the protection of personal information. The application of that Act cannot be extended to include aspects that falls outside the ambit of that Act, which predominantly provides for the protection of personal information.
	10.17 IM Governance - page 4 to 5 (paragraph 8)	10.17 Clause 52(1)(b) should be amended to provide that "the information should not be preserved for a period longer than necessary".	10.17 This is implied and will be regulated by the POPIA.
	10.18 SAFACT - page 5	10.18 If an ESCP's infrastructure is not able to track or store information or if the offender is using encryption, would the ESCP still be held liable?	10.18 No positive obligations are imposed to participate in an investigation. It is only required to preserve information which may be of assistance to law enforcement
	10.19 Bowline -	10.19 It should be mandatory for companies to report	10.19 Consideration may be given to

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	paragraph 1	cyber breaches and it is submitted that the Bill does not address the reality that each and every person and organisation in this country is potentially a service provider.	this fact and to include that everyone should report a cyber offence as is prescribed in terms of clause 52(2) to the SAPS. The clause only covers electronic communications service providers and financial institutions, which exclude other entities that use ICT to conduct business. However, in most instances where a monetary loss is incurred, this will be reported to the SAPS for compliance and insurance purposes.
		1	
	10.20 Bowline - paragraph 2	10.20 The Bill should provide for fines where organisations in the private and public sphere deal with personal information without a dedicated information security officer	10.20 The POPIA aims to regulate this aspect.
	10.21 Bowline - paragraph 3	10.21 Management of private and public companies should be held responsible in their personal capacity for cyber breaches within their organisations.	10.21 Sections 76 and 77 of the Companies Act, 2008 (Act 71 of 2008), do provide for this eventuality under certain circumstances where a director of a company does not exercise his or her duties with the required degree of care, skill and diligence, which may include appropriate measures to ensure cyber security. Civil liability may also follow in certain circumstances.

SECTIONS OF BILL	COMMENTATORS	COMMENTS	RESPONSES
	10.23 Credit Bureau Association - paragraph 2.2	10.23 The broad definition of electronic communications service provider may ensure that credit bureaus are included in this clause. Concerns are also raised that obligations to report cybercrime to the police and retain information imposes unnecessary and costly burdens on credit bureaus. According to the presentation, POPIA requires that information breaches relating to personal information be reported to the Information Regulator and this obligation is a duplication of functions and an unnecessary financial burden.	10.23 The Department disagrees. The definition of electronic communications service provider clarifies the issue.

Annexure A

SEIAS

Annexure B

ZOECO SYSTEM MANAGERS CC v MINISTER OF SAFETY AND SECURITY NO AND OTHERS 2013 (2) SACR 545 (GNP), where the following was said:

[37] In terms of s 20 of the Act, an article which is liable to seizure by the state includes any article:

[37.1] Which is concerned in or is on reasonable grounds believed to be concerned in the commission of an offence;

[37.2] which may afford evidence of the commission or suspected commission of an offence.

[38] In Minister of Safety and Security v Van der Merwe and Others 2011 (2) SACR 301 (CC) the following remarks were made:

'[38] Sections 20 and 21 of the CPA give authority to judicial officers to issue search and seizure warrants. The judicious exercise of this power by them enhances protection against unnecessary infringement. They possess qualities and skills essential for the proper exercise of this power, like independence and the ability to evaluate relevant information so as to make an informed decision.

[39] Secondly, the section requires that the decision to issue a warrant be made only if the affidavit in support of the application contains the following objective jurisdictional facts: (i) the existence of a reasonable suspicion that a crime has been committed and (ii) the existence of reasonable grounds to believe that objects connected with the offence may be found on the premises or persons intended to be searched. Both jurisdictional facts play a critical role in ensuring that the rights of a searched person are not lightly interfered with. When even one of them is missing that should spell doom to the application for a warrant.'

[39] The court goes on to state that —

'[40] The third safeguard relates to the terms of the warrant. They should not be too general. To achieve this, the scope of the search must be defined with adequate particularity to avoid vagueness or overbreadth. The search and seizure operation must thus be confined to those premises and articles which have a bearing on the offence under investigation.

[41] The last safeguard comprises the grounds on which an aggrieved searched person may rely in a court challenge to the validity of a warrant. The challenge could be based on vagueness, overbreadth or the absence of jurisdictional facts that are foundational to the issuing of a warrant.'

[40] The court continued to state that the principle of intelligibility requires that, even in the case of a CPA warrant, 'the person whose premises are being invaded should know why' (Minister of Safety and Security v Van der Merwe and Others para 54).

[41] The court then held at para 55 that:

'What emerges from this analysis is that a valid warrant is one that, in a reasonably intelligent manner:

(a) States the statutory provision in terms of which it is issued;

(b) identifies the searcher;

(c) clearly mentions the authority it confers upon the searcher;

(d) identifies the person, container or the premises to be searched;
(e) describes the articles to be searched for and seized, with sufficient particularity; and
(f) specifies the offence which triggered the criminal investigation and names the suspected offender.'

[42] The court then gave the following guidelines to be observed by a court considering the validity of the warrants (para 56):

[42.1] The person issuing the warrant must have authority and jurisdiction. I

[42.2] The person authorising the warrant must satisfy herself that the affidavit contains sufficient information on the existence of the jurisdictional facts.

[42.3] The terms of the warrant must be neither vague nor overbroad.

[42.4] A warrant must be reasonably intelligible to both the searcher and the searched person.

[42.5] The court must always consider the validity of the warrants with a jealous regard for the searched person's constitutional rights.

[42.6] The terms of the warrant must be construed with reasonable strictness.

[43] Information must be placed on oath before a judicial officer (which can include hearsay information), from which it appears to such judicial officer that there are reasonable grounds for believing that an article referred to in s 20 of the CPA is within his or her jurisdiction.

[44] The 'reasonable grounds for believing' in s 21(1)(a) are not grounds measuring up to an objective standard, but are grounds which in the subjective opinion of the judicial officer are reasonable (Mandela and Others v Minister of Safety and Security and Another 1995 (2) SACR 397 (W) at 404g – i).

[45] The belief on the part of the judicial officer that there are reasonable grounds to believe that the article in question is an article referred to in s 20 of the CPA is not objectively justiciable. The court may therefore not interfere with the judicial officer's decision merely because the decision is considered to be wrong (Mandela and Others v Minister of Safety and Security and Another supra at 404).

[46] The court will interfere with the judicial officer's decision to issue a search warrant in terms of s 21(1)(a) of the CPA in limited circumstances only, for example, if the judicial officer had not properly applied his mind to the matter (Mandela and Others v Minister of Safety and Security and Another supra at 404j – 405a).

POLONYFIS v MINISTER OF POLICE AND OTHERS NNO 2012 (1) SACR 57 (SCA) at paragraph [9]:

“ Before I deal with each of these contentions it is worth referring to some of the broad principles applicable to search and seizure warrants that Nugent JA recently restated in Minister of Safety and Security v Van der Merwe:

'From the earliest criminal codes — both in this country and abroad — statutory powers of search and seizure have existed for the detection and prosecution of crime. Such powers, to search and seize in relation to crime, are generally authorised in the following way.

A court or judicial officer is empowered by the statute to authorise, first, a search of premises, and secondly, the seizure of articles found in the course of that search, by issuing a warrant to that effect. Most often, the power to issue such a warrant is dependent upon it being shown, by information on oath, that it is suspected, on reasonable grounds, that an article (or articles) connected with a suspected offence is to be found on premises.

For a warrant to be justified, in such circumstances, the information that is placed before the court or judicial officer will necessarily need to demonstrate, firstly, that there are reasonable grounds to believe that a crime has been committed; and secondly, that there are reasonable grounds to believe that an article connected with the suspected crime is to be found upon particular premises. In order to demonstrate the existence of those jurisdictional facts, the ''information on oath'' will necessarily need to disclose the nature of the offence that is suspected.

In some cases it will be known that a particular article exists that is connected with the suspected crime. In those cases the purpose of the search will be to discover the particular article, and the article will thus be capable of being described in specific terms. In other cases it will not be known whether any particular article exists, but it can be expected that an article or articles of a particular kind will exist if the offence was committed. In such cases the purpose of the search will be to discover whether such articles or article exist/s, and thus they or it will be capable of being described only by reference to their genus. It is in relation to warrants of this kind that problems of validity most often arise. It will be inherent in the nature of the authority to search that the searcher might, in appropriate circumstances, be entitled to examine property that is not itself connected with the crime — for example, the contents cupboard or a drawer, or a collection of documents — to ascertain whether it contains or is the article that is being sought.

The authority that is conferred by a warrant to conduct a search, and then to seize what is found, makes material inroads upon rights that have always been protected at common law — amongst which are rights to privacy and property and personal integrity. In those circumstances — as demonstrated by the review of decided cases by Cameron JA in Powell NO and Others v Van der Merwe NO and Others 2005 (1) SACR 317 (SCA) (2005 (5) SA 62; 2005 (7) BCLR 675; [2005] 1 All SA 149) — the courts in this country have always construed statutes that authorise the issue of warrants strictly in favour of the minimum invasion of such rights — which is in accordance with a general principle of our law to that effect. As the learned judge said in that case:

"Our law has a long history of scrutinising search warrants with rigour and exactitude — indeed, with sometimes technical rigour and exactitude. The common-law rights so protected are now enshrined, subject to reasonable limitation, in s 14 of the Constitution:

'Everyone has the right to privacy, which includes the right not to have —

(a) their person or their home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.'

'A challenge to the validity of a warrant will thus call for scrutiny of the information that was before the issuing officer, to determine, firstly, whether it sufficiently disclosed a reasonable suspicion that an offence had been committed; and secondly, whether it authorises no more than is strictly permitted by the statute.

Questions that arise in relation to the second issue will generally fall into either of two different categories. The first is whether the warrant is sufficiently clear as to the acts that it permits. For, where the warrant is vague, it follows that it will not be possible to demonstrate that it goes no further than is permitted by the statute. If a warrant is clear in its terms, a second, and different, question might arise, which is whether the acts that it permits go beyond what is permitted by the statute. If it does, then the warrant is often said to be "overbroad" and will be invalid so far as it purports to authorise acts in excess of what the statute permits. A warrant that is overbroad might, depending upon the extent of its invalidity, be set aside in whole, or the bad might be severed from the good.

Needless to say, a warrant may be executed only in its terms. But it is important to bear in mind that it is not open to a person affected by a search to resort to self-help to prevent the execution of a warrant, even if he or she believes that its terms are being exceeded — which is in accordance with ordinary principles of law. As Langa CJ pointed out in Thint:

While a searched person may in certain cases collaborate and aid the investigator . . . the legislation envisages a unilateral exercise of power that is not dependent on such collaboration.

'Thus it is ultimately the searcher who must decide whether an article or articles fall within the terms of the warrant, though he or she does so at the risk that, if not, his or her conduct might be found to have been unlawful.'".

Also see among others **MAGAJANE v CHAIRPERSON, NORTH WEST GAMBLING BOARD AND OTHERS** 2006 (2) SACR 447 (CC); **INVESTIGATING DIRECTORATE: SERIOUS ECONOMIC OFFENCES AND OTHERS v HYUNDAI MOTOR DISTRIBUTORS (PTY) LTD AND OTHERS; IN RE HYUNDAI MOTOR DISTRIBUTORS (PTY) LTD AND OTHERS v SMIT NO AND OTHERS** 2000 (2) SACR 349 (CC); **MISTRY V INTERIM MEDICAL AND DENTAL COUNCIL OF SOUTH AFRICA AND OTHERS** 1998 (4) SA 1127 (CC) at 1147D - 1148B, that deals with the appropriate safeguards before a search and seizure can take place.