CENTRE FOR CONSTITUTIONAL RIGHTS
Upholding South Africa's Constitutional Accord

Patron: The Hon Mr Justice Ian G Farlam

Portfolio Committee on Justice and Correctional Services
Third Floor, Parliament
90 Plein Street
Cape Town
Attention: Mr V Ramaano
Per email: vramaano@parliament.gov.za

10 August 2017

Dear Mr Ramaano

CONCISE SUBMISSION ON THE *CYBERCRIMES AND CYBERSECURITY BILL* [B 6-2017]

1. The Centre for Constitutional Rights (CFCR) is a unit of the FW de Klerk Foundation - a non-profit organisation dedicated to upholding the Constitution of the Republic of South Africa, 1996 (the Constitution). To this end, the CFCR seeks to promote the Constitution and the values, rights and principles enshrined in the Constitution; to monitor developments including legislation and policy that may affect the Constitution or those values, rights and principles; to inform people and organisations of their constitutional rights and to assist them in claiming their rights. The CFCR does so in the interest of everyone in South Africa.

2. Accordingly, the CFCR endeavours to contribute positively to the promotion and protection of our constitutional democracy. This includes the achievement of real and substantive equality and equitable access to land and other resources, but with due regard for those rights concerning property and administrative action that is lawful, reasonable and procedurally fair, as provided for in the Constitution.

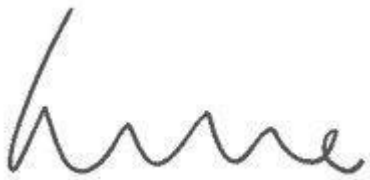
3. As such, the CFCR welcomes the opportunity to make a concise submission to the Portfolio Committee on Justice and Correctional Services (the Committee) regarding the *Cybercrimes and Cybersecurity Bill* [B6-2017] (the Bill) in response to your call for submissions as published on http://www.parliament.gov.za.

4. In this regard, please find attached our submission for the Committee's attention and consideration.

5. It is not the purpose or intention of this submission to provide comprehensive legal analysis or technical assessment of the Bill, but rather to draw attention to key concerns in relation to the Bill.

6. We trust that our submission will be of assistance in guiding the Committee in its deliberations regarding the Bill.

Yours Sincerely



Ms Phephelaphi Dube
DIRECTOR: CENTRE FOR CONSTITUTIONAL RIGHTS

7. **Introduction**

7.1. At the outset, the CFCR wishes to record that there is a real need for legislative measures to address the increase in cybercrimes and breaches of cybersecurity in South Africa. The CFCR welcomes the Bill to the extent it addresses legitimate concerns in this regard.[1]

7.2. The CFCR has previously delivered written submissions to the Department of Justice and Constitutional Development (the Department) on the *Draft Cybercrimes and Cybersecurity Bill* [B-2015] (2015 Draft Bill) in which the CFCR highlighted the undue impact of the Bill on the constitutional right to freedom of expression and the extensive search and seize powers granted to State Security Services.

7.3. The CFCR welcomes certain amendments made to the Bill since the 2015 Draft Bill, especially in relation to the removal of "*Computer related espionage"*; "*Personal information and financial offences*"; "*Infringement of Copyright*" and the removal of the "*prohibition on dissemination of data messages which advocates, promotes or incites hate, discrimination or violence*".

7.4. However, the CFCR is concerned that the Bill in its current format still infringes significantly on an individual's constitutional right to privacy, access to courts and freedom of expression. This is seen especially in relation to the surveillance powers of the State if read with the *Regulation of Interception of Communications and Provision of Communication-Related Information Act* of 2002[2] (RICA).

7.5. To this extent, the CFCR will limits its comments to the provisions of "*malicious communications*" and to certain provisions regarding the "*powers to investigate, search and access or seize*" in relation to the interception of indirect communication and communication-related information. Finally, the CFCR will also highlight further concerns in relation to these specific provisions considering the introduction of "*information sharing*" between various Government structures as provided for in the Bill.

7.6. We wish to draw the Committee's attention to the constitutional rights which may be adversely impacted by the specific provisions of the Bill under discussion, as well as the failure of the Bill to adhere to international principles in this instance.

8. **Legal Framework**

8.1. The right to freedom of expression in terms of section 16(1) of the Constitution specifically includes the right to "*freedom of the press and other media"* and specifically to *"receive or impart information or ideas*".[3]

8.2. It is crucial that the measures proposed in the Bill, especially in relation to the surveillance powers of the State read with RICA, do not stifle the free flow of communication out of fear of possible interception of communication, especially in respect to communication between journalists and

[1] 2016 *Cost of Data Breach Study: Global Analysis* - accessible at:https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF

[2] 70 of 2002.

[3] Section 16(1)(a) and (b) of the Constitution.

their confidential sources.[4] In the matter of *Khumalo and Others v Holomisa*[5], the Constitutional Court emphasised that the Constitution asserts to protect the media and that the media -

> "*...bears an obligation to provide citizens with information and with a platform for the exchange of ideas which is crucial to the development of a democratic society*."[6]

8.3. Furthermore, section 16(2) of the Constitution specifically limits the right to freedom of expression in very narrow circumstances and does not extend it to "*propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender or religion, and that constituters incitement to cause harm.*"[7] It is important to take note that the constitutional terminology used has a specific connotation and is in line with international law on this topic. Terminology used in the Bill in relation to the prohibition of "*malicious communications*" has to be in line with this section in order to ensure certainty and avoid confusion.

8.4. The right to privacy in section 14 of the Constitution extends to the right not to have your property searched or seized and everyone is specifically granted the privacy not to have "*the privacy of their communications infringed*".[8] It is crucial that the measures proposed in the Bill impacting on the right to privacy are narrowly tailored considering the importance of this right and will pass the limitation of rights query as set out in section 36 of the Constitution, especially with reference to the surveillance powers of the State.[9]

8.5. In the matter of *Minister of Police v Kunjana*[10], the Constitutional Court emphasised that the closer the "*inner sanctum*" of a person's home is infringed the higher the justification has to be -

> "*In Gaertner, this Court held that 'the right to privacy embraces the right to be free from intrusions and interference by the state and others in one's personal life'. How closely one infringes on the 'inner sanctum' of the home is a consideration that must be borne in mind when considering the extent to which a limitation of the right to privacy may be justified*."[11] (own emphasis)

8.6. Section 34 of the Constitution specifically affords everyone the right to have a dispute resolved by "*application of law decided in a fair public hearing before a court...".* The failure of the Bill to provide a person with a legal mechanism to dispute the lawfulness of the manner the State intercepted data and shared information to this extent, is a glaring omission. In the matter of *Zondi v MEC for Traditional and Local Government Affairs and Others*[12], it was reaffirmed that -

> *''The right of access to court is indeed foundational to the stability of an orderly society. It ensures the peaceful, regulated and institutionalised mechanisms to resolve disputes…"*[13]

---

[4] See media report regarding the interception order granted against *Sunday Times* journalist Mr Wa Afrika - www.iol.co.za/the-star/hawks-listened-to-journalists-telephone-calls-1148988.
[5] 2002(5)SA 401.
[6] At para 24 of the Judgment.
[7] Section 16(2)(a) - (c) of the Constitution.
[8] Section14(d) of the Constitution.
[9] Section 36 of the Constitution - "*Limitation of rights*" and stipulates the justifying factors to determine whether a limitation of a right in the Bill of Rights is justified.
[10] 2016 (9) BCLR 1237 (CC).
[11] At para 18 of the judgment. See above footnote for case reference.
[12] 2005 (3) SA 509 (CC).
[13] At para 61 of the judgment.

8.7. Last, above all the Rule of Law must be adhered to. The Rule of Law is a foundational value of a constitutional democracy and it requires that legislation must be "*written in a clear and accessible manner*" which exactly stipulates to the public what is required of them, as was stated in the matter of *Affordable Medicines Trust and Other v Minister of Health*.[14]

8.8. Various provisions in the Bill are currently vaguely stipulated and of special concern to the CFCR is the extent to which this causes confusion with the regulatory measures provided for in RICA and unintentionally creates a parallel system of surveillance. This needs to be clarified in order to be in line with the Rule of Law. This vagueness further creates potential for abuse of the legal process.

8.9. The CFCR will briefly set out international principles the Committee should take note of in this instance, in order to guide the Committee, especially in consideration of South Africa's international obligations and in line with section 39 of the Constitution.[15]

9. International principles

9.1. South Africa is a signatory to both the *Universal Declaration of Human Rights*[16] and the *International Covenant on Civil and Political Rights*[17], which amongst other international treaties to which South Africa has assented, reinforces South Africa's commitment to the upholding of the right to freedom of expression, access to courts and especially the right to privacy.

9.2. Furthermore, South Africa is also a signatory to the *Convention on Cybercrime of the Council of Europe*[18] (the Budapest Convention), which provides a guideline for national legislation to be adopted in combatting cybercrime and provides a framework for international cooperation in the fight against cybercrime.

9.3. 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.[19]

9.4. 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*." (own emphasis)

9.5. It is submitted that a revision of RICA together 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.[20]

9.6. Furthermore, it is submitted that the *International Principles on the Application of Human Rights to Communications Surveillance*[21] (commonly known as the "Necessary and Proportionate Principles")

---

[14] 2006(3) SA 247 (CC).
[15] Section 39(1)(b) states that "*on interpreting the Bill of Rights, a court, a tribunal or forum must consider international law*".
[16] Which was adopted by the General Assembly of the United Nations on 10 December 1948.
[17] Which was adopted by the General Assembly of the United Nations on 16 December 1966.
[18] ETS 185 - Convention on Cybercrime, 23.XI.2001.
[19] Article 21 of the Convention.
[20] Stakeholder Report Universal Periodic Review 27th Session - South Africa "The right to privacy in south Africa". Submitted by Right2know campaign and Privacy International.
[21] See - https://necessaryandproportionate.org/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.

9.7. The Necessary and Proportionate Principles were adopted after global consultation with various stakeholders and international experts in communication-surveillance and was officially launched by the United Nations Human Rights Commission in September 2013.

9.8. The Necessary and Proportionate Principles in essence clarify how international human rights law applies to the ever-changing digital environment, and stipulates 13 principles to measure current and proposed communication-surveillance laws. The Necessary and Proportionate Principles serve as a guidance framework and are endorsed by over 600 organisations worldwide. The CFCR will specifically consider how the proposed measures in the Bill measure against certain of these principles.

10. ***Ad clause* 16, 17 and 19 of the Bill: *Malicious Communications* as provided for in Chapter 3 of the Bill - Concerns on inconsistent use of terminology and unintentional consequences**

10.1. At the outset, it is suggested that clauses 16 and 17 in their current format be removed not only for the more detailed reasons as set out below but also careful consideration of the alignment of proposed offences created in both the *Films and Publication Amendment Bill* (Films Bill)[22] and the *Prevention and Combatting of Hate Crimes and Combatting of Hate Speech Bill (Hate Crimes Bill)*[23], to ensure it is aligned with the Constitution.[24]

10.2. As previously stated, the constitutional right to freedom of expression can only be limited in very narrow circumstances as set out in section 16(2) of the Constitution. It is important to emphasise that unless the offences created in both clause 16 and 17 fall within these narrow categories of "(*a) propaganda for war ;(b) incitement of imminent violence; or (c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm*" it will infringe protected expression and can only be justified if it meets the limitation threshold as set out in section 36 of the Constitution[25].

10.3. Clause 16 in 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.

10.4. Furthermore, 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 matter of *Brandeburg v Ohio*[26] *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.

[22] B 37-205. It appears the Bill is currently under further deliberation.

[23] B-2016.

[24] The CFCR made extensive submissions on both the Films Bill and the Hate Crimes Bill in this regard.

[25] As was confirmed in the matter of *Islamic Unity Convention v Independent Broadcasting Authority* 2002(4)SA 294 (CC) para 13.

[26] 395 US 444 (1969).As referred to in the 5th Edition of *The Bill of Rights Handbook* by I Currie and J de Waal.

10.5. It is noted that the previous controversial offence of "*prohibition of data message which advocates, promotes, or incites hate, discrimination or violence*"[27] has specifically been replaced with a "*data message which is harmful*" at clause 17. It is submitted that the current clause 17 is extremely vague. It is unclear whether the intention of the drafters was to align it with the *Protection from Harassment Act* of 2011 (Harassment Act)[28] as it echoes certain sentiments, such as the application for a protection order pending criminal proceedings, at clause 19 of the Bill.

10.6. However, the terminology used in clause 17 of the Bill is much wider than that used in the Harassment Act and, in fact, it replicates terminology used in section 10 of the *Promotion of Equality and* Prevention *of Unfair Discrimination Act*[29] of 2000 (Equality Act) regarding the "*prohibition of hate speech*".

10.7. Clause 17(1) specifically stipulates that the 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*".

10.8. However, "*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 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*".[30]

10.9. 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*[31] and defamation[32]. Furthermore, clause 17 is also silent on defences available to an accused in this instance.

10.10. It is submitted that clause 17 is not only in contravention of the Rule of Law regarding the vagueness of the terminology used and possible conflict with the Harassment Act as set out above but it will also impact protected expression, which can only be justified in terms of section 36 of the Constitution. Considering the importance of the right to freedom of expression in a democratic society, the limitation to this right will in this instance need to be narrowly defined with clear use of terminology, which makes it explicitly clear what the purpose of this limitation is.

10.11. Last, it is also noted that 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

[27] Clause 17 of the 2015 Draft Bill.
[28] 17 of 2011.
[29] 4 of 2000.
[30] Clause 17(d) of the Bill.
[31] *Crimen injuria* is a common law crime and the essential elements to the crime is the "*unlawfully, intentionally and seriously impairing of the dignitas of another*".
[32] Which is the wrongful and intentional publication of defamatory material of a person.

service provider without notice. This is specifically 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 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.

11. ***Ad clause 38*** **of the Bill as read with various other provisions in the Bill: Concerns on the surveillance power of the interception-powers of the State in addition to RICA and the echoing of serious shortcomings in RICA**

11.1. It is submitted that clause 38 of the Bill, which provides for the interception of "*indirect communication, obtaining of real-time communication-related information and archived related information*" infringes on the constitutional rights to privacy and especially the right of access to courts with reference to RICA.

11.2. Clause 38 not only provides additional and unclear obligations to electronic communications service providers in conflict with RICA, but it also expands the State's interception powers in relation to the amendment of the definition of "*serious offence*" as set out in section 1 of RICA. Finally, clause 38 also echoes and relies on serious shortcomings of RICA, which are currently the matter of a constitutional challenge in the North Gauteng High Court.[33]

11.3. RICA sets out procedure for the lawful State interception of "*communication*" and "*communication-related information*" of a person, without their knowledge, in terms of chapter 3 of RICA. This includes the interception of "*direct communication*" and "*indirect communication*".

11.4. In terms of section 1 of RICA, "*indirect communication*" includes the "*transfer of information, including a* message *or any part of a message*" in various forms such as "*data*" in this instance, "*that is transmitted in whole or in part by means of a postal service or a telecommunication system*". Section 16 of RICA furthermore sets out the manner and information that needs to be provided for the granting of an "*interception-order*" by a "*designated judge*" as defined in RICA.

11.5. 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.

11.6. However, "*data*" in terms of clause 1 of the Bill is defined as "*electronic 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*[34] has been abused to obtain "*real-time*" or "*archived communication-related information*" outside the procedure of RICA. [35]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.[36]

---

[33]*AmaBhungane Centre for Investigative Journalism NPC and Sole Stephen Patrick/ Minister of Justice and Constitutional Development and 9 Others*. Case nr 25978/17 - North Gauteng High Court - filed 2017/04/11. Matter has not been set down at date of submission.

[34] 51 of 1977. Section 205 provides that - "*Judge, Regional Court magistrate or Magistrate may take evidence as to alleged offences*" .

[35] In this regard see specific questions raised by Adv Breytenbach to the Minister of Justice and Correctional Services on 5 June 2017 and his reply. This can be accessed on: https://pmg.org.za/committee-question/5651/

[36] Especially section 15 of RICA.

11.7. It is also of concern that the procedure for interception-orders and other related order in terms of RICA which is relied on in clause 38(1) currently forms the basis of a constitutional challenge by amaBhungane Centre for Investigative Journalism (amaBhungane).[37] The constitutional challenge follows various serious concerns of interception of communication between journalists and their sources.[38] Even though the matter is under judicial consideration at time of making the submission, it is submitted that these concerns of RICA are also further replicated in the Bill.

11.8. One of the specific constitutional challenges in the amaBhungane matter is the fact that RICA prohibits "*user notification*" of the interception order even after the fact and after the sensitivity of the investigation has passed. This seriously threatens the right to privacy and access to courts.[39] The lack of "*user notification*" is also replicated in the Bill. This is not only seen in the fact that clause 38(1) of the Bill does not address this constitutional concern of RICA but electronic-communications service providers are specifically prohibited in terms of clause 37(1) of the Bill to "*disclose <u>any information</u> which he or she has obtained in…the performance of his duties*" in this regard unless it falls within exceptions as provided for.

11.9. This means that electronic-communications service providers are not only prohibited to inform their customers of the interception-order but they are even strictly prohibited to inform the public and their customers of the extent they have been requested to comply with interception-orders, the type of request, the prevalence of specific data requests and different categories of data request for instance.

11.10. Principle 8 of the Necessary and Proportional Principles specifically requires "*user-notification*" of interception-orders in order for the user to challenge the decision in a competent Court. It is understandable that user-notification at time of the application will in all probability make the provision of interception-orders futile.

11.11. However, it is not clear what justification there is to not inform the 'person' or 'customer' of an interception-order after expiry of such order or after an investigation in order for the person to consider the lawfulness of the interception-order.[40] This would provide a person or customer with the opportunity to review the legality of the order and give effect to the constitutional right to access to courts. It appears in other jurisdictions such as Germany for instance, "*user notification*"

---

[37] See reference to case law at footnote 32.

[38] As set out in the Founding Affidavit, the second applicant, Mr Sole, a journalist who was investigation the Arms Deal matter in 2008, specifically became aware that telephone communications between him and the lead prosecutor in the Arms Deal matter were intercepted as suspected and extracts of the conversation formed part of court papers in 2015. Despite various requests to the State Security Agency, it appears Mr Sole is yet to see a full transcript of the intercepted communications or the documents that served before the "designated judge" to justify the interception-order.

[39] Page 12 and 13 of the Founding Affidavit of the amaBhungane matter stipulates the constitutional challenges. In brief: Lack of user notification of interception orders, lack of procedure to be followed regarding storing and destroying of documents intercepted, period for which communication relation information has to be retained, lack of civilian oversight and lack of protection for journalists and attorneys. AmaBhungane also argues that RICA is under-inclusive regarding mass surveillance. In relation to the lack of "*user notification*" sections of RICA being challenged in this regard are: Sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7).

[40] This is specifically a grief concern in relation to media-reports of interception-orders having been granted against two *Sunday Times* reporters in 2010 on false information provided to the 'designated judge' by the police official. The two reports apparently had sources who informed them of these interception-orders. See http://m.news24.com/news24/SouthAfrica/News/spy-nation-journalists-challenge-government-snooping-20170420

of interception orders in terms of criminal law is made possible after the order has lapsed and the sensitivity of the investigation has ceased.[41]

11.12. In terms of section 36 of the Constitution, regarding the limitation query of the rights in Bill of Rights, the "*importance of the purpose of the limitation*"[42] limiting the right to access to Courts needs to be clear. In this instance it is not clear how the infringement can be justified when the purpose for the interception order has specifically lapsed.

11.13. Furthermore, the wide prohibition on the disclosure of information as provided for in clause 37(1) of the Bill in relation to clause 38(1), even for objective statistical purposes, not only undermines the principle of "*transparency*" as provided for in the Necessary and Proportional Principles[43] but it is difficult to see "*the relation between the limitation and its purpose*" which would justify such a limitation in terms of section 36 of the Constitution.[44]

11.14. Furthermore, 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*".[45] This would now mean that if on the low threshold of a "*reasonable belief*" any of 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[46].

11.15. Not only is the scope of RICA considerably widened 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,[47] it creates potential for abuse. This is worsened by the fact that the legality of the interception-order cannot be reviewed.

11.16. Furthermore, the fifth principle of the Necessary and Proportional Principles relates to "*proportionality*" and specifically states that there must be a "*high probability*" that a serious offence has been committed.

11.17. It is submitted that it would be crucial to review the lack of independent civilian oversight on the granting of interception orders in terms of RICA and the prohibition for user-notification, especially considering the further widened scope of "*serious offences*".

11.18. It is submitted that clause 38(3)(b)(ii) to (iv) will not muster constitutional scrutiny. It provides vague additional obligations in relation to "*archived-communication-related information*" to be provided by categories of electronic-communication service who are specifically excluded in terms of section 30(2) of RICA to store "*communication-related-information*". In its current format it creates confusion as to the period applicable to "*archived-communication-related information*" and the obligation on these electronic-communication-service providers. This is in clear contravention with the Rule of Law.

---

[41] In this regard it appears section 101(5) of the German Code of Criminal Procedure specifically deals with notification and it states that "*notification shall take place as soon as it can be effected without endangering the purpose of the investigation*…".

[42] Section 36(1)(b) of the Constitution.

[43] Principle 9.

[44] Section 36(1)(d) of the Constitution.

[45] Sections 8, 9(1), 9(2) and 10, 11(1), 11(2) or 12 are specifically included in the definition of a serious offence in terms of RICA. See schedule to the Bill.

[46] Section 16(5) of RICA.

[47] Reference to "*unlawfully*" in section 8, 9, 10 and 11 is not defined in the Bill.

11.19. Section 30(2) of RICA is also currently being challenged in the amaBhungane matter on the ground that the minimum-data retention period of three years and maximum of five years imposed on telecommunication-providers is impermissibly long and unduly infringes the right to privacy.[48] RICA also provides no oversight mechanism to ensure that the manner in which the data is retained or handled is protected and this is also specifically being challenged in the amaBhungane matter.

11.20. The above lack of oversight concern in RICA is also reflected in the additional obligations provided in clause 38(3)(b)(i) and (iv) of the Bill, in that no information is provided on how the data should be retained and stored. The Bill is also silent on whether the information has to be destroyed after such an order. It is submitted that this limitation on the right to privacy considering the nature of "*communication-related information*", which gives a great deal of personal information of an individual, cannot be justified.

11.21. Furthermore, it is also submitted that the relationship of clause 38 of the Bill to clause 27 of the Bill is not clearly stipulated. A real risk exists that despite the Deputy Minister of Justice and Correctional Services' reassurance that clause 27 does not increase the State's "*surveillance powers*", it does appear to conflict with RICA and perhaps unintentionally creates a parallel surveillance system.[49]

11.22. 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.

11.23. 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.[50]

11.24. 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*" for instance 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.

11.25. This search warrant in terms of clause 27(2) may include the authority to enter such premises, for instance, and the use of any "*instrument*" or "*device*", for instance 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.

11.26. On the current reading of clause 27 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 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

[48] Page 47 of the Founding Affidavit.
[49] http://www.gov.za/speeches/cybercrimes-and-cybersecurity-bill-19-jan-2017-0000%20
[50] Section 22(4) of RICA.

ensuring that the process to gain access to premises in order to intercept data cannot be circumvented.

11.27. Lastly, the CFCR is also concerned that 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.[51] 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 that examines the manner this information is shared between these new structures, poses a real threat to the right to privacy.

12. ***Ad clause 39*** **read with clause 38(1) and (2) - Expedited preservation of data direction**

12.1. 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.

12.2. 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.

12.3. Furthermore, the interception-order granted under clause 38 is supposed to be justified on 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 catchment area of the interception is in fact much wider and this raises a serious threat to the right to privacy.

12.4. Clause 39(2) makes it clear that clause 39(1) also applies to "*archived communication-related information*" 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.

12.5. Furthermore, it is submitted that 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*,[52] for instance, only refers to the request for a preservation order of property which on reasonable belief is an "*instrumentality of an offence*".

13. **Conclusion**

13.1. We hope our submission on the provisions of "*malicious communication*", as well as the interception-powers of the State as read with RICA, has been of assistance to the Committee. We wish to emphasise that it is crucial to ensure that the constitutional rights to freedom of expression,

[51] Clause 37(1)(d) of the Bill.
[52] 121 of 1998.

privacy and access to courts are not unduly infringed upon, especially in relation to the worrisome extent this Bill relies on serious flaws of RICA that currently forms the basis of a constitutional challenge.

Yours sincerely

Ms Christine Botha
LEGAL OFFICER : CENTRE FOR CONSTITUTIONAL RIGHTS