IS CYBER SEARCH AND SEIZURE UNDER THE CYBERCRIMES AND CYBERSECURITY BILL CONSISTENT WITH THE PROTECTION OF PERSONAL INFORMATION ACT?

1 Introduction

The use of the internet, computers and information and communication technologies has become the revolutionary means of communication that proffers unlimited access to a library of information. Information and communications technologies refers to "technologies that pertain to the new science of collecting, storing, processing and transmitting information whereby information, computing and telecommunications are converging" (Ajakaiye and Wangwe "Introduction to the Special Issue ICTs and Economic Transformation in Africa: A Synthesis" 2011 3 *African Journal of Science, Technology, Innovation and Development* 11). Juristic and natural persons alike have increasingly become dependent on the use of the internet for various purposes, such as conducting e-commerce (e-commerce can be defined as "commercial activities which are carried on by means of computers interconnected by telecommunications lines" Schulze "Electronic Commerce and Civil Jurisdiction, with Special Reference to Consumer Contracts" 2006 *SA Merc LJ* 31), e-business, accessing and storing information, communication and forging of new relations. With the dawn of each day, new and improved devices and applications (commonly known as "apps") are constantly designed to adapt to the sophisticated lifestyles prevalent in the information age. For cavalier individuals, the internet presented itself as pristine ground to develop new means of committing crime. Use of the internet, information and communication technologies introduced new forms of offences that were not previously known or defined, neither in terms of common law nor statute (Snail "Cyber Crime in the Context of the ECT Act" 2008 *JBL* 63). Such crimes include activities like hacking (hacking is the unlawful access and interception of data: Buys *Cyberlaw @SA 11 The Law of the Internet in South Africa* (2004) 447), cracking (producing anti-security circumventing technology: Snail 2008 *JBL* 66), phishing (when a fraudster sends an email impersonating another: *Nashua Mobile (Pty) Ltd v GC Pale CC t/a Invasion Plant Solutions* 2012 (1) SA 615 619 A–B), dissemination of malicious code (includes the dissemination of destructive programmes and codes, like virus, worms and Trojan horse: Snail 2008 *JBL* 64) and denial of service (denial of service is the inability of a website or other server to respond to legitimate connections, and is used to block access to a target-internet site: Etsebeth "The Growing Expansion of Vicarious Liability in the Information Age (Part 1)" 2006 *TSAR* 564 565), collectively known as cybercrimes (cybercrime has been defined as including any crime carried out primarily by means of a computer on the internet: Cassim "Formulating Specialised Legislation to Address the

Growing Spectre of Cybercrime: A Comparative Study" 2009 12 *PER* 36). At the same time, the use of the internet has facilitated the commission of previously defined crimes or traditional crimes, like forgery or theft in ways that are much easier for criminals, yet difficult for investigators to prove (Snail 2008 *JBL* 63).

The bulk of traditional laws governing crime investigations and crime prosecutions were to some extent incongruous with technological advances, making it extremely difficult to combat cybercrimes. Firstly, computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the legitimacy and feasibility of laws based on geo-political boundaries (Johnson and Post "Law and Borders – The Rise of Law in Cyberspace" 1996 48 *Stanford LR* 1367). The internet debilitated and disregarded geographical boundaries that previously served as a jurisdictional link for governments to assert power over any criminal activity. The other effect of the internet on jurisdiction was that in some instances no state could claim jurisdiction over a cybercrime, and in other instances several states claimed jurisdiction at the same time (Brenner and Kroops "Approaches to Cybercrime Jurisdiction" 2004 *Journal of High Technology Law* 1 3). Owing to the different cybercrime statutes, or the absence of cyber-security laws, the diverging jurisdiction clauses and failure to establish jurisdiction, either by exercising physical control or imposing sanctions, cyber-criminals had loopholes to evade prosecution. Another hurdle that was faced by the criminal-justice system was the anonymity enjoyed by criminals. Criminal anonymity involves the use of sophisticated rerouting techniques and hacking incidents which remain anonymous, making it extremely difficult if not impossible for the criminal justice system to unmask a cybercriminal for purposes of crime adjudication and prosecution (Cassim 2009 *PER* 39).

In South Africa there has been a long wait for articulate laws which were congruent with technological developments in identifying and defining offences committed in cyberspace, and providing penalties for such crimes. As cybercriminals changed from being nerdy loners to being criminal syndicates, there was a call to formulate specialized legislation to combat these new criminal behaviours (Cassim 2009 *PER* 37). Some of the notable statutes which provided a partial recourse to issues surrounding cybercrimes included the Criminal Procedure Act (51 of 1977 (CPA)) and the Electronic Communications and Transactions Act (25 of 2002 (ECT Act)). The two pieces of legislation had to be read together when addressing the overlapping issues of cybercrime (s 82(4) of the ECT Act). However, the Acts had their own inadequacies as they were not precisely tailor-made to regulate offences committed in cyberspace, and had difficulties in establishing jurisdiction where offences were committed by a faceless or nameless criminal.

The main challenge with the existing legal framework was its inability to provide properly defined parameters of what could be searched and seized during a cybercrime investigation (Musoni *Revisiting Cyber Search and Seizure in the Context of the Electronic Communications and Transactions Act and the Criminal Procedure Act* (unpublished Master's thesis, Witwatersrand University 2013). Information and communication technologies by nature have the ability to store elephantine personal and

confidential data which cannot ordinarily be retrieved under a traditional search in terms of the CPA (Musoni *Revisiting Cyber Search and Seizure* 6). For instance, computers and cellphones act as access portals / doorways into cyberspace and store unlimited amounts of personal data like photographs, personal memoirs, private thoughts and conversations, videos and audios (Park "Traffic Ticket Reasonable, Cell Phone Search Not: Applying The Search-Incident-To-Arrest Exception To The Cell Phone As "Hybrid" 2012 60 *Drake LR* 429 444). In addition, they provide access to the internet where one can access sensitive and confidential financial information, like banking details and various personal communications. The use of the internet leaves trails of digital footprints or electronic evidence (Electronic evidence is "information that is stored electronically and which can be presented as evidence in a legal action"; Basdeo "The Legal Challenges of Search and Seizure of Electronic Evidence in South African Criminal Procedure: A Comparative Analysis" 2012 *SACJ* 195 198), which can prove the commission of cybercrimes and such evidence can be found on a computer, computer network, cellphone, *etcetera*. The wealth of information readily available from one source can be a treasure trove of evidence to crime investigators. The knowledge that evidence can be easily obtainable at the click of a button is tempting bait for crime investigators as they might end up exceeding the bounds of the search and seizure. Searching throughout a person's computer, computer network and cellphone is tantamount to searching through a person's home or workplace and incidentally homes or workplaces of their friends and colleagues, and this elusively infringes on the constitutional right to privacy (Bertron "Home is Where your modem is: An Appropriate Application for Search and Seizure Law to Electronic Evidence" 1997 34 *American Criminal LR* 163 181–182; the author draws an analogy that an internet user's account is equivalent to his/her real home because through this account they can conduct various activities only previously conducted in the real/physical world such as banking, shopping and communicating with friends).

The other problematic challenge with information and communication technologies and the internet is its ability to disseminate personal data at incredible speed to an unlimited number of people across the globe (Roos "Privacy in the Facebook Era: A South African Legal Perspective" 2012 *SALJ* 375 377). This poses as a problem to peace officers in the sense that they cannot control the number of participants in the commission of a crime, neither would they be able to stop the furtherance of such a crime. Cyber investigators also risk the loss of evidence of the commission of crime, as skilled cybercriminals could easily destroy the evidence at the click of a button. Since different networking systems could be remotely accessed without the knowledge of the owner of the network, it is tempting for investigators to conduct such searches without tipping off a suspect (a good example of investigators bypassing the normal procedure to obtain evidence was in the United States case between the FBI and Apple Inc which will be discussed below in the last paragraph preceding the conclusion). Owing to all these challenges surrounding cybercrimes, crime investigators can be lured to conduct the search of electronic evidence without the requisite search warrant, or end up exceeding the bounds of their search warrant.

The focus of this note is to analyze whether the Cybercrimes and Cybersecurity Bill provides a harmonization between search and seizure and the constitutional right to privacy. This will be achieved by discussing the State powers of search and seizure in cyberspace *vis-à-vis* the right to privacy as envisaged in the Protection of Personal Information Act. Further, this note investigates whether the Cybercrimes and Cybersecurity Bill achieves the purpose of combatting cybercrimes without the infringement of the right to privacy. Subsequently, the article provides plausible recommendations on how the State should lawfully conduct searches and seizures of articles related to cybercrimes.

2 Background

2 1 The Criminal Procedure Act

Before the advent of the internet and information and communication technologies, the Criminal Procedure Act was the principal law on search and seizure. Peace officers conducted searches and seizures within clearly defined prisms without unlawfully infringing on the privacy rights of suspects. It was commonplace that privacy rights could be limited if it was reasonable and justifiable in an open and democratic society, by weighing up of competing values (Basdeo "A Constitutional Perspective of Police Powers of Search and Seizure: The Legal Dilemma of Warrantless Searches and Seizures" 2009 *SACJ* 403 406) in terms of section 36 of the Constitution of the Republic of South Africa, 1996 (the Constitution). But the same analogy is difficult to draw when dealing with cybercrimes. The inimitable nature of information and communication technologies lies in their ability to store vast amounts of data belonging to different persons, which can be shared with any third parties anywhere in the world at the blink of an eye. This makes it extremely difficult to delineate the bounds of a search without unnecessarily and unlawfully invading a suspect's private space, or that of a third party that is not a part to the crime.

Section 27(a) of the Cybercrimes and Cybersecurity Bill provides that laws relating to search and seizure are an addition to chapter 2 of the CPA, thus retaining the CPA as the default position for a search and seizure. Section 20 of the CPA lists articles that may be seized. These articles include anything concerned / or on reasonable grounds believed to be concerned with the commission of an offence whether within the Republic or elsewhere. It also includes anything which may afford evidence of the commission or suspected commission of an offence, whether in the Republic or elsewhere. Furthermore, it includes anything which is intended to be used in the commission of an offence. If any one of the grounds is satisfied, then a search can be conducted.

It has been argued that the definition of "entity" was restrictive to physical entity, and as such chapter 2 of the CPA does not apply to the search of a computer and the seizure of information located on that computer (Basdeo 2012 *SACJ* 205). The Law Commission was also of the view that chapter 2 of the CPA would not apply to the search of a computer, although it would allow for seizure of a particular computer (Buys *Cyberlaw @SA* 330). As

would be discussed below, the definition of article in the Cybercrimes and Cybersecurity Bill includes a computer/information system. For brevity purposes, the CPA will be discussed further in the discussion.

2 2 The Electronic Communications and Transactions Act

The ECT Act was previously the principal legislation on search and seizure in cyberspace. To conduct a lawful search and seizure, a cyber-inspector had to be in possession of a section 83-search warrant. Section 83(3)(a) of the ECT Act provided that a warrant to enter, search and seize may be issued at any time and must identify the premises and information system that may be entered and searched. A cyber-inspector could only search and seize property under the authority of a warrant and enter, or access the information system that had a bearing on an investigation (section 82 of the ECT Act). Also the cyber-inspector could perform his/her functions without notifying the person against whom the search is to be conducted. Any statutory body with powers of search and seizure (like South African Police Services) could apply for assistance from a cyber-inspector to assist it in an investigation (section 81(2) of the ECT Act).

The problem with this Act was that it created unnecessary administrative processes likely to circumvent the ends of justice (Musoni *Revisiting Cyber Search and Seizure* 16). Cyber-inspectors could only search and seize articles if they were in possession of a search warrant. Conversely, where a cyber-inspector witnessed the commission of a cybercrime in his presence, he could never conduct a search without possession of a search warrant. In such cases the object of the search will be defeated since the evidence could easily be removed, destroyed or lost. When cyber-inspectors came across incriminating evidence, they could not search or seize such information, but rather had to report to the South African Police Services. Alternatively, as members of the South African Police Services lacked the technical know-how, it was imperative to apply to the Director-General to deploy the services of a cyber-inspector. This joint process between cyber-inspectors and South African Police Services could cause unnecessary delays in the investigation of crime (Musoni *Revisiting Cyber Search and Seizure* 16). Chapter 6 of the Cybercrimes and Cybersecurity Bill provides a meticulous structure to deal with cybercrimes- and cybersecurity- related matters. The Cyber Response Committee coordinates activities aimed at improving cyber-security by all key-role players (such as the 24/7 Point of Contact, the Cyber Security Centre, Cyber Crime Response Centre *etc*) which includes strengthening of intelligence collection and improved state capacity to investigate, prosecute and combat cybercrime, as well as deal with cyber threats. This proper coordination and centralization ensures a painstaking investigation and regulation of cybercrimes.

3 The Protection of Personal Information Act

The Protection of Personal Information Act 4 of 2013 (POPI) gives effect to the constitutional right to privacy (s 14 of the Constitution). The Act represents a significant advancement in data-security standards in South

Africa by imposing stringent requirements pertaining to the processing of personal information (Gill and Bokhari "Cyberspace – The World's Largest Crime Zone. Why it is Essential for South Africa to Implement Cyber Security Measures and Legislation" 2016 *Technology and Sourcing Alert* 1 4). The Act purports to protect personal information processed either by public and private bodies, as well as establishing minimum requirements for the processing of personal information. It outlines eight data-protection principles that must be adhered to when processing personal information (Visser "The Protection of Personal Information in Broadcasting: The Effect of the Protection of Personal Information Bill on Freedom of Expression" 2011 *SAJHR* 331 340). Before processing of data, a data subject must consent to the processing of its personal information (s 10 of POPI). This consent must be obtained directly from the data subject and the processing must be lawful and reasonable (s 8–11 of POPI). The processing must still be relevant and in line with the purpose for which the information has been processed. This goes hand-in-glove with the requirement that the personal information must be obtained for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party (s 12–14 of POPI). Also the data subject must know the purpose for the processing of the personal information and has a right to object, on reasonable grounds, to the processing of its personal information.

The Cybercrimes and Cybersecurity Bill uses the same definition for personal information found under POPI. Part of the definition of personal information is information that can be linked to an identifiable living, natural person. Such information includes "any identifying number, symbol, email address, physical address, telephone number and correspondence sent by the person that is implicitly or explicitly of a private / confidential nature or further correspondence that would reveal the contents of the original correspondence". In cyberspace, personal information in the form of correspondence would include communications *via* an array of social networking sites, such as Facebook (an application platform that allows interactions between individuals online; McClard and Anderson "Focus on Facebook: Who are we Anyway?" 2008 3 *Anthropology News*), MySpace (a platform for self-representation, self-promotion and content sharing through user-generated content; McClard and Anderson 2008 3 *Anthropology News*), WhatsApp messenger (an instant-messaging application for smartphones that can be used to send each other videos, images and audio-media messages, http://en.wikipedia.org/wiki/WhatsApp (accessed 2013-10-15)), Blackberry messenger (an internet-based instant-messenger application on Blackberry devices that allows messaging between Blackberry users, http://en.wikipedia.org/wiki/Blackberry Messenger and http://appworld.blackberry.com (accessed 2013-09-13)), short-message services (an sms is a service that allows for short-text messages to be sent from one cellphone to another cellphone; Fendelman "definition of sms text messaging: what is sms messaging, text messaging" http://cellphones. about.com/od/phoneglossary/g/smstextmessage.htm (accessed 2013-08-12)), telephone conversations, Skype conversations (is an IP telephony-service provider that offers free calling between subscribers and low-cost calling to people who don't use the service; Rouse "Skype" http://search unifiedcommunications.techtarget.com/definition/Skype (accessed 2013-12-

04), emails, and any other kinds of social networking. The type of information typically contained in social networking sites like Facebook and Myspace profiles includes the user's photograph along with the user's name, country, gender, sexual orientation, marital status and date of birth (Papadoupoulos "Revisiting the Public Disclosure of Private Facts in Cyberworld" 2009 30 *Obiter* 30 32). The profile also includes a list of friends, a list of groups to which the user is affiliated, interests, personal photographs, favourite music, *etcetera*. (Papadoupoulos 2009 30 *Obiter* 32). Contents of private correspondence *via* social-networking sites are thus protected in terms of both POPI and the Cybercrimes and Cybersecurity Bill as personal information.

POPI allows the State to process personal information without complying with the data-protection principles if it's in line with a crime investigation (s 6(1)(c) of POPI). However, there is a *proviso* which states that "there must be adequate safeguards in specific legislation for the protection of such personal information" (s 4(c)(ii) of POPI). The specific legislation with the adequate safeguards on processing of personal information during a search and seizure, is going to be the Cybercrimes and Cybersecurity Bill.

4 Cyber search and seizure under the Cybercrimes and Cybersecurity Bill

Section 28 of the Cybercrimes and Cybersecurity Bill empowers law-enforcement agencies or investigators to conduct a search or a seizure of any article, whether within the Republic or elsewhere. As indicated earlier, the CPA did not apply to the search of a computer and the seizure of information located on a computer. In order to address the inadequacies under the CPA, the Cybercrimes and Cybersecurity Bill extended the definition of "article" under section 20 of the CPA. Section 26 of the Cybercrimes and Cybersecurity Bill defines an article as "any data, a computer device, a computer network, a database, a critical database, an electronic-communications network or a National Critical Information Infrastructure or any part thereof or any other information, instrument, device or equipment which –

> "(a) is concerned in, connected with or is, on reasonable grounds, believed to be concerned in 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 in terms of this Act, or any other offence which may be committed by means of or facilitated through, the use of an article, whether within the Republic or elsewhere."

So the Cybercrimes and Cybersecurity Bill is in line with technological developments as it does not limit the definition of article in section 20 CPA to physical entities, but extended the meaning to include computer networks, databases and devices which are in connection with/provide evidence of the commission of a crime, or intended to be used in the commission of a crime.

4 1 Particularity in a search with a warrant

A search generally constitutes a serious encroachment on the right of the individual, so courts have a duty to scrutinize activities related to a search (*Minister of Justice v Desai* 1948 (3) SA 395 (A)). A search with a warrant is reasonable because a search warrant outlines the specific areas to be searched. The question of particularity of a search warrant becomes more remarkable in cyberspace. What kind of information should be searched on a person's computer or computer networks? Should a search warrant for electronic evidence specify the files on a computer or phone that must be searched? Does search on a computer extend to search through social networking profiles or emails?

To be valid, a search warrant must state the statutory provision in terms of which it is issued, identify the searcher, clearly mention the authority it confers upon the searcher, describe the person, container or premises to be searched, describe the article to be searched for and seized, with sufficient particularity, and specify the offence which triggered the criminal investigation and names of the suspected offender(s) (*Minister of Safety and Security v Van der Merwe* 2011 (2) SACR 301 (CC) par 55–56). If a search warrant specifies articles to be seized in broad and general terms, then such a warrant lacks particularity (*Smith, Tabata and Van Heerden v Minister of Law and Order* 1989 (3) SA 627 (E) 249). A valid search warrant is one that outlines the ambit of the search it authorizes to both the searcher and the searched (*Zuma v National Director of Public Prosecutions* 2006 2 All SA 91 (D)).

Section 29(2)(e) of the Cybercrimes and Cybersecurity Bill provides the investigator or member of a law-enforcement agency with the right to access and search any data, computer device, computer network, database, critical database, electronic-communications network, or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant. Section 29(2)(f) further provides that the investigator or member of the law enforcement agency may obtain and use any instrument, device, equipment, password, decryption key, data or other information that is believed, on reasonable grounds, to be necessary to access or use any part of any data, computer device, computer network, database, critical database, electronic-communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant. The Cybercrimes and Cybersecurity Bill clearly fails to outline the particularity expected in a search warrant. There is no obligation on the investigator or peace officer to know 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, computer files, etc. 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 (*Magobodi v Minister of Safety and Security* 2009 (1) SACR 355 (Tk) par 10–11).

The definition of article under section 26 part (a) and (c) of the Cybercrimes and Cybersecurity Bill 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 part (b) of section 26. The Cybercrimes and Cybersecurity Bill provides that an article may be searched if it may provide evidence for the commission of a crime. This provision empowers investigators to search any article without the need to prove that there are reasonable grounds that it will provide evidence for the commission of a crime. This provision gives the State unnecessary powers to pry into people's privacy as long as the investigator is of the opinion that the information will provide evidence of the crime. The Cybercrimes and Cybersecurity Bill must ensure that investigators have reasonable belief that every article searched is linked to, affords evidence and intended to be used in the commission of an offence. That way there will be no unnecessary intrusions into one's privacy.

It is the author's submission that, where the level of particularity cannot be met, a key-word search should be included in a search warrant. The key words could be for the names of suspected participants, important dates, place of events surrounding the crime under investigation and other words likely to be found in the relevant communications (Bertron 1997 *American Criminal LR* 176). Searches can be limited to messages sent, or received to or from particular individuals or during a particular time frame. So, for instance, where a person is suspected of committing a phishing scam and siphoning money from ABSA bank, the inspector can use the word "key search" and go straight to emails that mention ABSA bank (Musoni *Revisiting Cyber Search and Seizure* 19). The effect of the criteria is to limit the messages that can be read by officers, as well as avoiding irrelevant messages from being accessed (Bertron 1997 *American Criminal LR* 190). This search is a less restrictive means to achieve the objective of investigating cybercrime.

4 2 Warrantless search

As stated earlier, a cyber-inspector cannot search premises or information system without a search warrant. It is quite conceivable that circumstances may arise were the delay in obtaining a search warrant would defeat the object of the search, which thus justifies a warrantless search (Geldenhuys, Joubert, Swanepol, Terblanche, Van der Merwe and Iuris *Criminal Procedure Handbook* 10ed (2011) 155). A search without a warrant will usually result in a constitutional violation of privacy, unless it can be justified in terms of section 36 of the Constitution (the right to privacy includes the right to be free from intrusions and interference by the State and others in one's personal life, as well as unauthorized disclosures of information about one's life; Mason "Invasion of Privacy: Common Law v Constitutional Delict – Does it make a Difference?" 2000 *Acta Juridica* 227 250). Section 31 of the Cybercrimes and Cybersecurity Bill emphasizes the importance of consent as one of the fundamental principles of data protection. It provides that warrantless searches may only be conducted where the investigators obtained consent from the person with authority to do so. The Cybercrimes and Cybersecurity Bill does not provide provisions for urgent situations where a search or seizure has to be effected without a warrant. It is not clear

why the legislature failed to include such a provision in the Cybercrimes and Cybersecurity Bill.

A balance should be struck between private interests on the one hand, which demands the protection of a constitutional right to privacy and freedom and public interest, on the other hand, which in turn demands a protection against crime (Musoni *Revisiting Cyber Search and Seizure* 21). Where a search warrant could have been obtained in the absence of extraordinary exigent circumstances, it was maintained that a search of private dwellings without a warrant is an infringement of the constitutional right to privacy (Basdeo 2012 *SACJ* 195 198). Where such exigent circumstances are present, the interests of law enforcement override the need for judicious consideration of privacy rights (*S v Madiba* 1988 (1) BCLR 38 (D) 45). These exigent circumstances include the imminent danger of the loss, removal, destruction or disappearance of evidence if the search should be delayed to obtain prior authorization (Basdeo 2012 *SACJ* 195). Such circumstances are even more likely in cyberspace because of the easiness in destroying the evidence. However, it is the author's submission that the legislature might not have found the need to provide a warrantless search provision, since section 26(b) already empowers the State to search an article if it may provide evidence. It is the author's submission that in the presence of exigent circumstances and the seriousness of a crime (for instance, where an investigator has come across evidence of child pornography or plans for a terrorist attack), the right to privacy can be overridden in order to achieve national safety and security. In such circumstances, an investigator should be allowed to immediately seize an article and orally apply for a search warrant in terms of section 30 (1) of the Cybercrimes and Cybersecurity Bill.

4 3 Search incident to arrest

Section 32(1) of the Cybercrimes and Cybersecurity Bill provides that on the arrest of any person on suspicion that he or she has committed an offence under this Act or any other offence, a member of a law-enforcement agency may search the arrested person and seize any article referred to in section 28 which is in the possession of, in the custody of or under the direct control of, the arrested person. In terms of this provision, search will be limited to the arrested person. If the arrested person is carrying a section 28 article, such an article must be seized. However, section 32(2) of the Cybercrimes and Cybersecurity Bill appears to be a misnomer. It provides that a member of a law-enforcement agency or an investigator who is accompanied by a member of a law-enforcement agency, may access and search any article referred to in subsection (1). The author fails to understand the rationale behind searching for a section 28 article, where a person is arrested for an offence unrelated to cybercrimes. Where a person has been arrested for driving without fastening his/her seatbelt or driving without a licence, there is no justification for an investigator to access a section 28 article and go through a person's emails and social-networking profiles and messaging.

Section 32(2), when read together with section 32(1)(b) of the Cybercrimes and Cybersecurity Bill, is an unjustifiable infringement of the right to privacy. It is the author's submission that the Bill should be amended

to provide that, where a person has been arrested for a crime other than cybercrime, the investigator should only seize according to the section 28 article. Should the investigator, on reasonable grounds, believe that the evidence of the crime leading to the arrest is likely to be found on the article, thereafter he/she can apply for a search warrant to search the article. This way of operating will ensure that investigators do not rummage through a person's personal and confidential information upon a whim.

Section 38 of the Cybercrimes and Cybersecurity Bill prohibits investigators and members of the law-enforcement agencies from disclosing any information they would have acquired during their investigation. It is the author's submission that non-disclosure by investigators does not justify the infringement of privacy. Infringement of privacy can also occur when an outsider acquires knowledge of private and personal facts relating to a person, contrary to that person's determination and wishes (Neethling, Potgieter and Visser *Law of Personality* 2ed 2004 225–226). In cases where an unnecessary search of section 28 is conducted, such search will be unjustifiable regardless of the mandate on the investigators not to disclose the information.

In general, trans-border flow of information is restricted in terms of POPI (s 72(1) of POPI). Section 46, read together with section 48 of the Cybercrimes and Cybersecurity Bill allows the State to transfer data to a foreign state if the data relates to a cybercrime, and the data is necessary to prosecute offenders. The Cybercrimes and Cybersecurity Bill is in line with POPI which allows for the trans-border flow of information if the foreign state has effective laws that uphold principles for reasonable processing of information similar to South Africa. It has been argued that since the Cybercrimes and Cybersecurity Bill seeks to foster international cooperation on cybercrimes and other criminal activities, SA law-enforcement agencies could in future potentially be engaged by other states to bypass security and encryption features (Gill, Suliman and Makhubedu "Analysing the Cybercrime Bill and its Impact on Privacy in the Context of the Apple v FBI Controversy" 2016 *Technology and Sourcing Alert* 1 3). This line of argument came as a result of the US Government's request to Apple Inc to assist the FBI in developing an operating system that could unlock an iPhone belonging to Syed Farook who was responsible for the shootings in San Bernadino (Kharpal "Apple v FBI: All you Need to Know" 29 March 2016 *CNBC News*). Though the US Government requested the judge to drop the case after they had found other means to unlock the iPhone, the action taken by the US Government has left South Africans who use iPhones vulnerable as there is likelihood that their personal information could be accessed without their consent. It is the author's submission therefore that before the South African Government can transmit personal information to foreign states, it should investigate whether the foreign states uphold similar data-protection principles. This will ensure that regardless of personal data having left South Africa, there will be reasonable processing of that data.

5 Conclusion

The Cybercrimes and Cybersecurity Bill is a very important legislative development that is going to fill in the gaps and provide clarity to South Africa's legislative framework on cybersecurity. It serves to mend the bridge between technological advancement and the law to ensure that the law maintain its credibility. It has brought clarity to cybercrimes by succinctly defining different types of criminal activity as cybercrimes and allowing the prosecution of such cybercrimes. Only a few provisions of the Bill unlawfully infringe on the privacy rights of individuals. The provisions of a search warrant for a section 28 article should be very precise and particular. Since the Cybercrimes and Cybersecurity Bill is expected to be the principal law regulating conduct in cyberspace, it should set out clearly-defined parameters of what can be searched within information systems/computer networks/information and communication technologies, *etcetera*.

Part (b) of the definition of "article" under section 26 of the Cybercrimes and Cybersecurity Bill should be amended. The Cybercrimes and Cybersecurity Bill should make it a requirement that there should be a reasonable ground to believe that a section 28 article may provide evidence of a cybercrime or any other crime committed. A search warrant should be issued only if there is reason to believe that the article will provide evidence. The same reasonableness test is relevant in the case of a search incident to arrest. Section 32(1)(b) of the Cybercrimes and Cybersecurity Bill should be amended by inserting the *proviso* that search and seizure in respect of a suspect arrested for any other offence, should be effected only if there are reasonable grounds to believe that the evidence of this offence can be obtained from the section 28 article. This will avoid unnecessary searches and unlawful infringement of privacy where there is no reason to believe that the section 28 article will provide evidence.

Melody Musoni