# State-on-nationals' electronic communication surveillance in South Africa: A murky legal landscape to navigate?

Murdoch Watney
University of Johannesburg
mwatney@uj.ac.za

***Abstract*—The discussion concerns itself with state-on-nationals' electronic communication surveillance in South Africa. The 2013 Snowden revelations of collaboration between the United States National Security Agency and the United Kingdom Government Communications Headquarters conducting bulk surveillance of all people as well as the 2015 South African spy cable disclosures involving communications between the South African State Security Agency and other foreign intelligence agencies confirmed that surveillance technology provides for covert, mass and undiscriminating government surveillance of nationals and states. Although the latter surveillance was conducted for national security purposes, government agencies also conduct surveillance for law enforcement purposes. The question pertaining to this discussion is whether information of South African nationals is lawfully accessed and/or retained in terms of a legal framework. This should include effective checks and balances, accountability and transparency to ensure that the information gathered is effectively protected against abuse such as its utilization for means other than the original purpose for which it was accessed and/or retained. Another concern is whether different thresholds apply to the purposes in conducting state electronic communications' surveillance. The aim of the discussion is not to vilify government surveillance practices as governments carry the onerous task of protecting nationals against threats within the ever-advancing electronic communication technology medium. The aim is rather to establish whether there exist voids and/or deficiencies and if affirmative, how it could be addressed to ensure an open and transparent surveillance landscape aimed at striking a balance between security and human rights protection.**

***Keywords: state-on-nationals surveillance, electronic communication, legal framework, law enforcement, state security, South African surveillance landscape***.

## I. INTRODUCTION

Catchphrases such as "Orwellian society" and "big brother state" abound today and reflect the warning of George Orwell in his book, *Nineteen Eighty-Four*, in which he warned of a state ever-watching citizens. It may be premature to assume it has happened or that states such as South Africa are moving in that direction before the topic at hand has been fully addressed.

The 2015 espionage revelations involving the South African State Security Agency (SSA) catapulted nationals into scrutinizing the South African government's electronic information gathering practices, unlike the 2013 Snowden WikiLeaks allegations which did not evoke much debate regarding state-on-nationals' surveillance. This may be ascribed to the fact that the so-called "spy cable scandal" directly affected the South African legal surveillance landscape and was not merely a European Union (EU) and/or United States (US) government-on-nationals' surveillance issue.

It is relevant for purposes of this discussion to briefly review the 2013 revelations in which Snowden, a former US National Security Agency (NSA) contractor disclosed that the US NSA in collaboration with the UK Government Communications Headquarters (GCHQ) had conducted secret and mass surveillance on national and international level. Information was gathered on people irrespective of whether they were suspects, allegedly in the interest of national security [1]. These revelations were followed by various human rights discussions and a re-evaluation in the EU and the US of state surveillance practices and a debate on the challenges facing state surveillance of electronic communication in a globalized world. This is of relevance to South Africa as the country forms part of a globalized world and it should therefore take cognisance of global legal developments within a legal comparative context.

The discussion focuses on re-examining state-on-nationals' surveillance practices of electronic communication in South Africa. Many inter-related legal issues will be addressed such as:

- A brief explanation of the meaning of the term, state surveillance which serves as a background to the discussion;
- An overview of the legal framework governing state-on-nationals' electronic communication surveillance in South Africa; and
- An outline of legal developments in other countries that may be of interest pertaining to the South African surveillance landscape.

Although controversial and in some instances, problematic, a debate on the inter-related legal issues is long overdue. This should be seen against the background of the Snowden revelations, the ever-increasing impact of communication technology on people's daily lives, the government's role in ensuring the safety and security of its nationals, the criminal and extremist abuse of communication technology to infringe user rights and the difficulties in ensuring a balance between protecting the human rights of users and ensuring security and safety in cyberspace.

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

## II. UNDERSTANDING THE TERM "STATE SURVEILLANCE" OF ELECTRONIC COMMUNICATIONS

### A. Introduction

The term "state surveillance" of electronic communications serves as a starting point and provides the necessary background to understand the legal framework governing state-on-nationals' surveillance discussed hereafter at paragraph III. The legal framework as illustrated hereafter consists of legislation and regulations. The primary legislation applicable to surveillance is the *Regulation of Interception of Communications and Communication-related Information Act* 70 of 2002 (referred to as RICA).

Electronic communication is defined in the *Electronic Communications and Transactions Act* 25 of 2002 (ECT Act) and referred to in RICA as indirect communication. It constitutes communication for example by means of a website such as online banking or booking airplane tickets or Google searches or social media communication by means of tweets, YouTube, Instagram, Facebook and emails which may be accessed either by means of a so-called smart phone or a computer. Smartphone usage in South Africa is expected to top 23,6 million users this year, up from 19 million in 2014 [2]. The growth in smartphone usage is boosting South Africa's internet population. The number of internet users in South Africa is predicted to reach 18,5 million during 2015 and increase to 24,5 million by 2020 [2]. Electronic communication is borderless, instant and available 24 hours 7 days a week and can target a wide audience simultaneously.

### B. Meaning of state surveillance

State surveillance of electronic communication refers to the government gathering different types of electronic information for law enforcement and/or national security purposes. Surveillance has been referred to as spying or espionage, but this does not reflect the legal meaning of the term, surveillance.

State surveillance is an umbrella term that includes various surveillance methods which are employed in the collection of information (evidence). The information collected may either be:

- Content information which refers to communication that includes information concerning the substance, purport or meaning of that communication (as defined in section 1 of RICA); and
- Traffic data (also referred to as metadata and archived communication-related information in RICA) refers to the records of transactions kept by ISPs when a user engages in online activity. ISPs must retain the following traffic data that identifies the source of a communication: the destination, date, time, duration and the type of communication.

The type of information collected may violate human rights for example the right to privacy. However, human rights are not absolute and may be infringed in accordance with the limitation clause in the South African Constitution (108 of 1996) (constitution) if the limitation is reasonable and justifiable in an open and democratic society. Rights can only be limited in terms of a law of general application.

### C. State surveillance methods

For purposes of this discussion, cognizance should be taken of the methods employed in gathering information, such as [3]:

- Monitoring which includes the listening to or recording of the content data at the time of the communication;
- Interception which is applicable to the collection of content data of communication in the course of its transmission. This entails the acquisition of the communication by someone other than the sender or the receiver;
- Traffic data retention which is the retention of traffic data of all users for a period of time;
- Data preservation (quick freeze) which is the preservation of specific traffic data of an identifiable Internet user for a specific criminal investigation for a limited period of time. RICA does not provide for data preservation; and
- Decryption of encrypted communication.

### D. Motivation for state surveillance

Vast amounts of information is communicated electronically daily. The characteristics of this medium challenges governments who wish to protect their nationals against crime and extremism. The purpose of state surveillance is to collect information in the interest of:

i. Law enforcement in order to detect, prevent, investigate and/or prosecute serious crimes outlined in RICA. In these instances prosecution would most probably follow; and

ii. National security in order to detect, prevent and investigate any security threat such as for example extreme (radical or fanatical) communication that canvasses support and/or incites and/or encourages terrorism or sabotage. National security is defined in the *General Intelligence Law Amendment Act* 11 of 2013 (GILAA). "National security" includes the protection of the people and the territorial integrity of the Republic against for example the threat of or actual use of force as well as terrorism, terrorist-related activities, espionage, sabotage or the exposure of a state security matter with the intention of undermining the constitutional order. Prosecution will not always be instituted.

Different government agencies will be responsible for collecting the information (evidence or intelligence) but in some instances interests may overlap. What has to be established is whether different thresholds apply pertaining to the different purposes for information gathering by means of state surveillance and it is relevant whether criminal prosecution will be instituted or not.

### E. Liability for conducting state surveillance

The internet and cellphone service providers are responsible for conducting surveillance on behalf of the state agency. Direct access to information by government agencies should be discouraged as it may result in surveillance abuse.

At paragraph 3 reference will be made to the Office of Interception Centre (OIC) and the National Communications Centre (NCC).

### *F. State surveillance and censorship*

It is important to distinguish between surveillance and censorship. Both are methods of state control of information, with censorship being a more severe form of government control of electronic communication. Surveillance does not affect access to information and/or freedom of expression whereas censorship is the restriction of access to information.

Censorship may be used as a national security measure imposed to protect society as a whole, keeping in mind that such measures seriously restrict the rights and freedom of nationals. The suppressing of cellphone signals by government resulting in attendees not being able to access the Internet at the South African State of the Nation Address (SONA) on 12 February 2015 cannot be considered as a national security measure as such an approach falls short of the constitution. This cannot be compared to for example prohibiting and/or blocking of access to child pornography as the latter constitutes a crime in South Arica and many other countries and the criminalization serves to protect the interests of the vulnerable, namely children. When Facebook banned a South African atheist group called Atheist Republic in 2014 for contravening the social network's terms of use and accused the 54 000 members of "hateful, threatening and obscene behaviour", Facebook was compelled to reverse its decision to provide for religious tolerance and freedom of expression which are guaranteed in the constitution [4]. The communication could not be considered extreme.

## III. LEGAL FRAMEWORK GOVERNING STATE-ON-NATIONALS ELECTRONIC COMMMUNICATION SURVEILLANCE IN SOUTH AFRICA

### *A. Introduction*

State-on-nationals' surveillance must be conducted within a legal framework to ensure legal certainty and to prevent government abuse for purposes that may not fall within law enforcement and / or national security.

The constitution is the benchmark against which all legislation and regulation as well as behaviour is measured. It may protect nationals against state abuse of surveillance powers, but the protection can only be invoked if the infringement is in the public arena and not conducted in secret. Although state surveillance abuses were suspected prior to the 2013 Snowden revelations, it was only after the disclosures were made that states and nationals could debate it. As will be illustrated hereafter, specific legislation need to give effect to the rights guaranteed in the constitution.

### *B. RICA*

RICA is the primary legislation governing surveillance for both law enforcement and national security purposes. Other legislation that may be relevant for purposes of surveillance will be briefly referred to. For purposes of this discussion only the most relevant provisions in RICA will be highlighted.

RICA provides in section 2 that monitoring and/or interception of electronic communication (referred to as indirect communication) is prohibited and therefore no one may listen in (eavesdrop) on a cellphone conversation or read someone else's email or SMS unless the communication falls within the ambit of sections 3 – 11. These sections provide for exceptions where communication may be intercepted in certain instances. Interception (which includes monitoring) may for example be conducted in respect of serious crimes or threats to national security (section 7) or to determine location in case of emergency (section 8) or where other legislation provides for it (section 9). Interception is strictly regulated and is carried out by means of a court order issued by a judge which will be presented to the telephone, cellphone or internet service provider [4]. Section 30 provides *inter alia* for the retention of the traffic data (communication-related information) by the internet service provider of all users for a period not less than 3 years.

Chapter 3 of RICA provides for the Office for Interception Centre (OIC). A distinction should be drawn between the OIC and the National Communications Centre (NCC). The OIC serves the state's intelligence agencies and National Prosecuting Authority (NPA). The NCC provides for bulk monitoring and interception of all signals with its main target foreign signal intelligence that falls outside the borders of South Africa or passes through or ends in South Africa [6].

Chapter 7 provides that cellphone owners must register their SIM card with a telecommunications service provider who must obtain information on their cellphone customers. If a cellphone or SIM card is used in a crime, then the person involved may be subjected to surveillance which could include being tracked.

For crimes that fall outside RICA, the law enforcement agency (police) may obtain a subpoena in terms of section 205 of the *Criminal Procedure Act* 51 of 1977 before accessing for example cellphone or telephonic records or cellphone tracking information.

The practical implementation and enforcement of RICA is of specific importance. The aim of the discussion is not to vilify government surveillance practices, but to establish whether there exist shortcomings and/or voids that should be addressed without undermining government surveillance powers in protecting nationals against threats posed by crime and/or radicalism. The following aspects may be noted:

- As surveillance affect users' rights, transparency is important to ensure trust in government surveillance practices and therefore the Joint Standing Committee on Intelligence (JSCI) should regularly release public oversight reports [7]. The Right2Know campaign indicated that prior to the April 2014 intelligence committee public oversight reports, no reports had been released for a period of three years [7]. The *Promotion of Access to Information Act* 2 of 2000 (PAIA) provides for example that any person may request records from a public body and receive a response within 30 days, but compliance has been slow [8]. In 2013 the *Protection of Personal Information Act* 4 of 2013 (POPI) amended PAIA to make provision for an information regulator which will act as

an ombud with legal powers to enforce compliance with information requests [8]. Right2Know also indicated that the April 2014 reports appear to be flawed [7]. The 2014 report indicated that about three million interceptions had been carried out in 2010, but only 882 RICA warrants were authorized. Right2Know opined that either each warrant represented thousands of interceptions or surveillance may be conducted without a court order [7] and that lack of public oversight of surveillance capacity remains vulnerable to abuse [8]. Other authors [5], [6], have expressed similar views. Where information is for example not needed for criminal prosecution, it may happen that it is gathered without judicial authorization as the question of admissibility in a subsequent criminal trial will not arise. It may be that doubts regarding the strength of a criminal case exist and that information is gathered to determine the strength of the criminal case which may then be followed by an application for a court order [6].

- The NCC is a matter for concern. The *General Intelligence Law Amendment Act* 11 of 2013 (GILAA) does not specifically refer to the NCC and presumably the NCC and its functions are incorporated in the SSA [10]. Commentators [7], [10], [11] report that the workings of the NCC are conducted in secret and that it is not possible to establish how much surveillance is conducted on diplomats (state-on-state surveillance) and ordinary citizens and how much thereof is justifiable [10]. As it targets foreign communication that emanates outside the South African borders, it could be argued that it does not fall within the ambit of RICA [6], [10], [11]. However, Nathan [9] makes a valid legal point by stating that as the NCC is not subjected to RICA, the NCC is acting unconstitutionally as the limitation of human rights must be done in accordance with a law of general application. Nathan [9] made valuable recommendations in this regard that might not have been considered prior to the implementation of the GILAA.
- Information should only be accessed for law enforcement and national security purposes and no one else should be able to gain unauthorized access to information. Cellphone service providers must allegedly divert all calls to the OIC. Von Solms [11] observes that it is not clear whether the information is used to profile a user or whether it may possibly be used for crime commission such as "identity theft." Interestingly Von Solms [10], who is an information security expert, clearly sees cellphone usage for online banking as a security risk when he remarks that he would only consider using his computer for online banking.
- "Identity theft" is not a crime in South Africa as it does not fall within the ambit of the common law definition of theft. Such behaviour will have to be regulated by means of legislation [12]. The damaging impact of "identity theft" on a person's life should not be under-estimated [13]. Hate speech is also not a crime in South Africa, but its criminalization may be considered. "Hate speech" is defined in the *Promotion of Equality and Prevention of Unfair Discrimination Act* 4 of 2000 (referred as the Equality Act) as words that are communicated based on race, gender, ethnic or social origin and colour; objectively considered to be hurtful, harmful, incite harm or propagate hatred and the words do not fall within artistic creativity, academic and scientific inquiry [14]. At present the victim of hate speech may claim damages for hurt, humiliation and degradation suffered in the Equality Court [14]. Criminalization would not curtail freedom of expression as the latter would then similarly be applicable to the common law crimes, *crimen iniuria* and defamation. Behaviour that amount to hate speech affect the constitutional rights of others. Following the xenophobic attacks in April 2015, the Ministry of Telecommunications and Postal Services called on South Africa's Internet service providers to exercise a mandate to respond to take-down notices lodged for content that is deemed racist or xenophobic on social media [15]. Section 77 of the ECT Act provides for a take-down notification pertaining to unlawful activity.
- A member of the public may lay a complaint with the Office of the Inspector General of Intelligence (established in terms of the *Intelligence Services Oversight Act* 40 of 1994) if she suspects that the state is unlawfully monitoring and/or intercepting her information. However, where surveillance is implemented covertly, it will only become known if it is disclosed as happened with the 2015 spy cable disclosures [16]. It was for example reported that the South Korean National Intelligence Service requested the SSA to conduct a security assessment on Naidoo, a South African national and head of Greenpeace (a non-governmental organization) who as an activist opposes nuclear power development. This request was issued prior to Naidoo's 2010 visit to South Korea where a meeting for G20 leaders was held [17]. Had it not been disclosed, Naidoo would not have known that he was perceived as a threat to the South Korean government.

### *C. Conclusion*

RICA provides a strict legislative framework, but these provisions are nevertheless challenged by advances in surveillance technology. Harmonization of terminology would have been welcomed. Traffic data retention (referred to as archived communication-related information) may have to be revisited taking into consideration the global legal developments referred to in paragraph IV.

As indicated above, the current application of RICA leaves room for improvement and it may be debatable whether sufficient safeguards (checks and balances) are in place to prevent the unlawful accessing of information. The challenge that presents itself does not only relate to the unlawful accessing of information but also whether information is sufficiently protected against abuse. Von Solms [10] also questions the high prevalence of cybercrime in South Africa. The *Protection of Personal Information Act* 4 of 2013 (POPI) may assist against the unlawful collection, retention, dissemination and use of personal information [18]. The aim of POPI is to protect personal information processed by public and private bodies and in order to achieve this aim, POPI provides for a number of offences.

If the application of national security laws and powers are not subject to good governance, the rule of law and effective checks and balances, there is a risk that national security may serve as a pretext for suppressing for example unfavorable

political and/or social views. It may appear that different thresholds apply to the purposes for which surveillance is conducted [10].

It should also be borne in mind that any surveillance oversight body must have the requisite independence and political will to ensure that government agencies do not break the law [5].

## IV. A CONCISE OVERVIEW OF LEGAL DEVELOPMENTS POST 2013 SNOWDEN'S REVELATIONS

Reference will only be made to aspects that may be of relevance to South Africa:

- As indicated, RICA provides for traffic data retention. However, in April 2014 the Traffic Data Retention Directive 2006/24/EC was declared invalid stating that although the purpose of investigation to combat serious crimes and international terrorism was compatible with the European framework, the directive was disproportionate and contrary to some fundamental rights protected by the EU Charter of Fundamental Human Rights [19]. National courts in several EU member countries have followed suit by declaring national traffic data retention laws unconstitutional. Traffic data retention is a valuable pro-active investigation tool and this may explain why Mexico in 2014 and Australia in 2015 implemented traffic data retention legislation. The RICA traffic data retention provisions may have to be re-visited to ensure safeguards are in place to protect the information gathered.
- Extremism (radicalism) has steadily increased since 2013 and countries such as the US, UK, France, Nigeria, Kenia and Tunisia have fallen foul of terrorism which affect western and non-western countries. Pressure may be exerted on internet communications providers to pro-actively monitor the content of all communication although such a legal duty would have serious human rights implications.

Cognisance must be taken of the brutal killing of UK soldier, Rigby by Islamic extremists in 2013. It transpired that one of the perpetrators discussed on Facebook in 2012 with a foreign-based extremist, known as "Foxtrot" that he wished to carry out a public execution of a British soldier. Although this communication amounted to anti-British hate speech, Facebook did not refer the information to British intelligence as it had in all probability not monitored the content. At the end of 2014 the British Intelligence and Security Committee concluded that the killing of Rigby could have been averted if Facebook had reported the communication to intelligence agencies [20].

According to Fidler [21] the release of online videos of the murder of captured persons by the self-proclaimed Islamic State (IS) represent a method of communicating with supporters, radicalizing new adherents, recruiting fighters, humiliating adversaries and spreading terror. Fidler [21] is of the opinion that the online distribution is an act of terrorism directed against persons protected by the International Humanitarian Law (IHL). The IS uses these violent videos to send messages about what happens to those who oppose IS.

The Islamic State (IS) has already started its' recruitment of supporters in South Africa [22]. It has been reported that South Africa is becoming an attractive destination to terrorist organisations for funding and training [23].

Unfortunately the Internet, due to its' characteristics, may be used by extremists for the purpose of propaganda and/or recruiting. The role of service providers in assisting government agencies against extremism may in future be under pressure. How the South African and other foreign governments are going to deal with cyberspace extremism is open to speculation.

## V. CONCLUSION

Although several aspects referred to require a more comprehensive analysis, this paper aims to provide an overview of the relevant issues at hand.

It is apparent that the old adage "I have nothing to hide" may have a hollow ring if a government is not only able to willy-nilly gather information but also no safeguards exist to protect the gathered information from ending up in the wrong hands [11]. A citizen needs to know when, how and why information is gathered and how the information is safeguarded. The latter should not only be clearly outlined in legislation to ensure legal certainty, but existing safeguards for oversight and transparency should be applied.

In *No Place to Hide* O' Harrow [16] remarks that "(y)ou are being watched. Government agencies and private corporations know where you live, how much you earn, what you buy, and sometimes even what you read. And increasingly, this information is being leaked (or sold) to identity thieves. In a surveillance society out of control, there is no place to hide" [13]. The question is whether surveillance in South Africa is out of control or moving in that direction.

State surveillance must be employed to protect nationals against the abuse of electronic communication, such as crime and extremism and to ensure a safe, reliable and secure electronic medium, but at the same time surveillance must be conducted in a transparent and controlled manner which safeguard nationals against abuse by those who gather the information. State surveillance should aim at striking a balance between human rights protection and securing the electronic medium and/or information gathered.

Singer and Friedman [24] states that "… the technical community that understands the workings too often sees the world only through a specific lens and can fail to appreciate the broader picture or non-technical aspects. Critical issues are thus left misunderstood and often undebated."

As technology continues to seep into our daily lives and the possible abuse of surveillance technology becomes more prevalent, a debate on state-on-nationals' electronic communication surveillance is important as it presents a muddy legal landscape to navigate.

## REFERENCES

[1] R.A. Clarke and R.K. Knake, *Cyber War*. New York: HarperCollins Publishers, 2012, pp. 2, 279 – 283.

[2] G. van Zyl, 19 March 2015, “Digital tsunami to hit SA workplace,” http://www.fin24.com/Tech/News/ Digital-tsunami-to-hit-SA-workplace-20150319

[3] M. M. Watney, “The use of electronic surveillance in conducting criminal investigations of the Internet” in Jahankhani, H., Watson, D.L., Gianlugi, M., and Leonhart, F. Handbook of Electronic Security and Digital Forensics, World Scientific Publishing Co.Pte.Ltd, Singapore, 2010, pp. 525 – 551.

[4] D. Alfreds, Janury 12, 2015, “Facebook does U-turn on atheist group ban”, http://www.fin24.com/Tech/News/Facebook-does-U-turn-on-atheist-group-ban-20150...

[5] P. De Vos, June 23, 2011, “RICA: Is it unconstitutional?” http://constitutioinallyspeaking.co.za/rica-is-it-constitutional/

[6] H. Swart, October 14, 2011, “Secret State: How the government speis on you,” http://mg.co.za/article/2011-10-14-secret-state/

[7] S. Writer, September 11, 2014, “Rica – what is the point?” http://businesstech.co.za/news/general/68246/rica-what-is-the-point/

[8] S. Writer, September 9, 2014, “SA govt secrecy getting worse: report, “ http://businesstech.co.za/news/government/-67990/sa-govt-secrecy-getting-worse-report/

[9] L. Nathan, March, 16, 2012, “A critique of the General Intelligence Laws Amendment Act” http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page72308?oid=29385

[10] P. De Wet. June 21, 2013, “Spy wars: South Africa is not innocent.” 2013 http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent

[11] L. George, March 2, 2015, “Wat word regtig alles afgeluister?” http://www.netwerk24.com/nuus/2015-03-02-wat-word-rgtig-alles-afgeluister

[12] M. M. Watney, “Identity theft: the mirror reflects another face,” 2004 (3) TSAR pp. 511 – 519.

[13] R. O’Harrow, No place to hide. New York, Free Press Publishers, 2006, pp. 10, 95 – 96, 300 – 304.

[14] P.Williams, March 2015, “Hate speech is a crime: Equality Court rules in favour of domestic worker,” De Rebus March 2015, issue 550, pp. 26 – 28; also available at http://www.myvirtualpaper.com/doc/derebus/de-rebus---march-2015/2015021801/28.html

[15] News24Wire, April 2015, “Govt targets xenophobic content,” http://businesstech.co.za/news/internet/86152/govt-targets-xenophobic-content-online/

[16] J. Heard, March 2, 2015, “Parliament must restore public trust after spy cable scandal,” http://www.news24/com/SouthAfrica/Politics/Parliament-must-resore-public-trust-aft...

[17] D. Smith, February 26, 2015, “Greenpeace head kumi Naidoo saddened at spying revelations, “ http://www.theguardian.com/world/2015/feb/26/greenpeace-head-kumi-naidoo-sadde....

[18] A. Hamman,“Nowhere to Hide – Big Brother is Watching You: Non-communiative Personal Cellphone Information and the Right to Privacy,“ 2010 (1) Speculum Juris pp. 70 – 95.

[19] R. Corbet, O. Mullooly and E. Dunne, April 16, 2014, “Data Retention Directive Declared Invalid by EU Court of Justice“, http://www.arthurcox.com/publications/data-retention-directive-declared-invalid-eu-c....

[20] M Jackson,. November, 25, 2014, “UPD Commons Intelligence and Security Committee blames ISPs for murder”, http://www.ispreview.co.uk/index.php/2014/11/commons-intelligence-security-comm...

[21] D. Fidler, April 8, 2015, “ISIS is committing war crimes on the Internet,” http://natiionalinterest.org/blog/the-buzz/isis-commiting -war-crimes-the-internet-12581

[22] Z Khoisan, “Muslim clerics slate’murderous’ Islamic State,” Saturday Star, April 11, 2015, p. 1.

[23] C. Benjamin, February 1, 2015, “SA an attractive destination for terrorism funding networks,” http://mg.co.za/article/2015-02-04-sa-an-attractive-destination-for-terrorist-funding-...

[24] P.W.Singer and A. Friedman, Cybersecurity and Cyberwar, New York: Oxford University Press, 2014, p.7.