Computer and Telecommunications Law Review

2011

Registration of SIM cards in Tanzania: a critical evaluation of the Electronic and Postal Communications Act 2010

Alex B. Makulilo

Subject: Telecommunications. **Other related subjects:** Constitutional law. Human rights

Keywords: Constitutional rights; Interception of communications; Mobile telephones; Privacy; Registration; Tanzania

Legislation: Electronic and Postal Communications Act 2010 (Tanzania)

Constitution of Tanzania art.16

*C.T.L.R. 48 Abstract

This article sets out to evaluate the constitutionality of the provisions of the Electronic and Postal Communications Act 2010 (EPOCA) regulating the registration of SIM cards in Tanzania. Particular focus is cast on the legal implications this law has over the constitutional right to privacy. It is the author's argument that the Act, being broadly and loosely framed, has legalised the secret interception of our private communications by the state rather than achieving its principal aims. For such reason, EPOCA contravenes the constitutional right to privacy.

Introduction

In January, 2009 the Tanzania Communications Regulatory Authority (TCRA) announced that all existing and future subscribers of pre-paid SIM cards must be registered.[1] This public notice required mobile service providers to maintain databases of information of their subscribers. Included in such databases is information on the phone number, name, date of birth, gender, address, alternative phone numbers (if available), the number on ID card, passport, driving licence, student card, voter registration card or a letter from a local government official. The deadline for registration was initially set to six months, i.e. from July 1, 2009 to December 31, 2009. This time-limit was extended for another period of six months to June 30, 2010[2] and subsequently for half a month to July 15, 2010.[3]

As is the case with countries which have implemented mandatory registration of SIM card schemes in Africa such as Botswana, Kenya, Nigeria, Zimbabwe, Sierra Leone, South Africa, Ghana, Cameroon (to name a few), TCRA advanced four reasons in support of registration of pre-paid SIM cards: (1) to protect consumers from misuse of communication services; (2) to enable consumers to be identified as they use value added services, such as mobile banking, mobile money transfer, electronic payments for services such as water, electricity, pay-TV, etc.; (3) to enhance national security; and (4) to enable network operators to promote “know your customer”.[4] It is worthwhile noting here the fact that the TCRA's directive to service providers to collect personal information from their subscribers was merely administrative.[5] The directive was not backed by any statutory law. Legislation on mandatory registration of SIM cards only came into force towards the end of the registration exercise.

This article evaluates the law governing mandatory registration of SIM cards, namely the Electronic and Postal Communications Act (EPOCA) 2010 from the constitutional right to privacy perspective. The first part introduces the article. The second part reviews the legislative history for registration of SIM cards in Tanzania. The objectives and reasons for enacting this law are presented here. The third part deals with the presentation of the law itself, highlighting the main parts of the legislation. The fourth part outlines the constitutional right to privacy and when such right can *C.T.L.R. 49 be derogated. This part basically tests the constitutionality of the provisions of EPOCA on registration of SIM cards against the right to privacy. The final part concludes the article with two remarks: first, EPOCA is an interception of communication law. Being framed broadly, and without adequate safeguards, the law falls below the constitutional standards. Secondly, while the objectives of EPOCA with regards to registration of SIM cards may still be valid, the Act needs to be significantly amended ahead of any possible constitutional petition.

Legislative history for registration of SIM cards

Prior to July 1, 2009 no mobile phone network subscriber in Tanzania was obliged to register his or her SIM card with the service provider. Registration was only required where a pre-paid subscriber needed service added value for mobile money transfer such as Vodafone M-PESA, Z-PESA, etc., and in the case of post-paid services. At this particular time a potential subscriber could purchase a SIM card from a street vendor and activate it immediately. He could also transfer it from one cell phone handset to another. Moreover, a subscriber could give a cell phone handset to a friend as a gift or transfer it to any other person in return for some money. As there was no registration of SIM cards or cell phone handsets, thieves could steal cell phone handsets, throw away the SIM cards and sell them to people on the black market. Some people could also purchase SIM cards and use them to call or send anonymous life-threatening or defamatory text messages to other people.

Against the above backdrop, the need for registration of SIM cards first occupied the Tanzanian parliamentary debates on August 18, 2008.[6] In that parliamentary session, legislators were concerned with three issues. First of all, most legislators who contributed to the need of a law on registration of SIM cards raised concerns over cell phone theft. It was their view that if SIM cards were registered, once a cell phone is stolen the owner could easily make a report of the theft to the service provider who would then block it. Arguably, this view was too simplistic, since a service provider could block a stolen cell phone even where the same was not registered.[7] In fact, it used to be the practice by service providers to block stolen cell phones in the early days when mobile phones were first put into use in Tanzania.[8] However this practice was abolished by the service providers presumably for commercial reasons. This is so because, when a service provider blocks a particular cell phone, it automatically affects sales of credit vouchers and also reduces customers.[9] However, when a stolen cell phone is transferred to another person it does not affect a service provider in any significant way because it is less important to them who owns a cell phone but how much the owner spends in making calls, texting messages, subscribing to various services marketed by the service provider, etc. There is also another explanation behind the abolition of the practice. Sometimes people abused this practice by making malicious reports to service providers for their own concealed reasons.[10] As a result, when service providers blocked such cell phones, owners would come and complain and sometimes threatened the service providers with litigation. Secondly, most legislators were concerned about anonymous defamatory calls and text messages. They associated use of unregistered SIM cards with the commission of various offences. While this view is partly true, the claim had been overestimated. This is so because, even after registration of SIM cards, doubts have been cast on the effectiveness of the said registration in combating the increasing crime involving use of cell phones.[11] The last concern, raised during the parliamentary session, was on the protection of subscribers' right to privacy. It is interesting to note that only one legislator raised concern over the right to privacy. Even though this was raised, no discussion took place on privacy. However, outside Parliament, some people aired their views over the privacy concern about the registration of SIM cards.[12]

Based on concerns about cell phone theft as well as cell phone misuse generally, TCRA issued a public notice on January 28, 2009 directing all service providers to register their subscribers' SIM cards within a period of six months effective from July 1, 2009.[13] However, it was not until January 27, 2010 that the Government introduced in Parliament the Electronic and Postal Communication Bill 2009 for its first reading. This Bill was passed into law two days later, i.e. on January 29, 2010. Interestingly, no legislator raised concern over the individual's right to privacy, not even the only legislator who warned of the potential breach of the right to privacy on August 18, 2008 created by such a law on the registration of SIM cards.

Overview of EPOCA

EPOCA was passed by the Tanzanian Parliament on January 29, 2010 and assented to by the President on March 20, 2010. The Act came into force on May 7, 2010.[14] It repealed and replaced[15] two pieces of legislation in the Tanzanian communication sector: the Broadcasting Services Act[16] and the Tanzania Communications Act.[17] It also amended[18] the Tanzania Communications Regulatory Authority Act[19] and the Fair Competition Act.[20] However, it saved all regulations made under the repealed laws to the extent that they are not inconsistent with EPOCA and not expressly revoked.[21]

EPOCA was enacted with three fundamental objectives.[22] The first was to address the challenges posed by modern technologies, especially the convergence of technologies. The second was to harmonise and consolidate communication laws in order to overcome regular conflicts in their implementation, and the third was to introduce the Central Equipment Identification Register (CEIR)

and registration of SIM cards. The Act has nine parts. Part I covers preliminary provisions. This part has three sections providing for the name of the Act, its commencement date and application as well as interpretation of key terms and phrases. Part II is titled Electronic Communications. It has 28 sections. It governs licensing, interconnection and access issues. Part III bears the title Postal Communications. It also has 28 sections. This part regulates all matters pertaining to provision of postal services. Part IV deals with competition issues and conduct. This part is the longest of all. It has 55 sections. The most prominent part in Pt IV covers ss.84 to 102 which deal with the establishment of CEIR and registration of SIM cards. This part is prominent because it introduces significant development in the communications sector in Tanzania. It is this part which this article is devoted to address. Part V deals with enforcement issues. It has only two provisions. Part VI is the next longest part. It has 44 sections. This part deals with offences and penalties under EPOCA. However, of particular importance in relation to this article are those sections which touch privacy of communications arising from registration of SIM cards. Part VII deals with miscellaneous provisions. It has seven sections. Part VIII deals with transitional matters with only one section and Pt IX deals with amendments and repeals. It has 18 sections.

Registration of SIM cards and protection of privacy

There is no general data protection law in Tanzania. Nevertheless the Tanzanian Constitution[23] generally guarantees the right to privacy. The relevant provision is art.16(1). It states:

“Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.”

However this right is not absolute. It is limited in art.16(2). This provision states:

“For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.”

Further limitations to the enjoyment of the constitutional right to privacy are generally provided in art.30(2) of the Tanzanian Constitution.[24] Construing the latter provision, the High Court of Tanzania has over and again held:

“A law which seeks to limit or derogate from the basic right of an individual on the grounds of public interest, will be saved by Article 30(2) of the Constitution, if it satisfies two requirements: firstly, such law must be lawful in the sense that it is not arbitrary. That means it should make adequate safeguards against arbitrary decisions and provide effective controls against abuse of those in authority when using the law. Secondly, the limitation imposed by such a law must not be more than is necessary to achieve the legitimate object. This is also known as the principle of proportionality.”[25]

***C.T.L.R. 51** In the subsequent parts of this article the author evaluates the provisions of EPOCA regulating registration of SIM cards in the light of the above-cited constitutional principles.

EPOCA places obligations on every person who owns or intends to use a mobile telephone to register his or her SIM card.[26] At the same time it places obligations on every service provider to obtain information from buyers of SIM cards which identify them before activating such SIM cards in their networks.[27] The list of information that a potential subscriber must give to the service provider on his or her identity includes: in the case of a natural person, full name of the potential subscriber, identity card number or any other document which proves the identity of the potential subscriber, and residential, business or registered physical address, whichever is applicable.[28] In the case of a legal person, the certificate of registration or incorporation, business licence, tax payers' identification number certificate and where applicable value added tax will be required for registration purposes.[29] In addition, a service provider may obtain “any other information” from potential subscribers which it deems necessary.[30] In effecting registration, a service provider is put under obligation to verify all the information from a potential subscriber before he or she proceeds to register him or her.[31] Once registered, the information obtained from a potential subscriber will be retained in hard copy documents or electronically.[32] Where the information is obtained on behalf of a service provider, such person who acted on his or her behalf is obliged to submit such information to the service provider within 15 days.[33] A service provider, on the other hand, is required to submit all subscribers' information collected by himself or herself together with those by its agents to TCRA once in every month.[34] The latter preserves this information in the subscribers' database.[35] As rightly argued by

Froomkin, once personal information is collected in a database the person from whom such information was collected has significantly less control over his or her personal information.[36] This loss of control over one's personal information leads to a potential lack of the subscriber's knowledge of data flows and blacklisting.[37] In the same vein, Clarke posits that databases create a prevailing climate of suspicion and repressive potential for a totalitarian government.[38] In line with Froomkin and Clarke, Sutherland argues that if the government knows your SIM card details, then it can monitor your calls and text messages.[39] Because of this, s.98 of EPOCA lays a duty on service providers to ensure that the information collected from subscribers is kept secure, confidential and not tampered with. This section states:

“98(1) a person who is a member, employee of application service licensee, or its agent, shall have a duty of confidentiality of any information received in accordance with the provisions of this Act.”

It proceeds to state:

“98(2) no person shall disclose the content of information of any customer received in accordance with the provisions of this Act, except where such person is authorised by any other written law.”

From this provision, it is clear that s.98 applies only to three categories of persons: a member of a service licensee, an employee of a service licensee and an agent of a service licensee.[40] Surprisingly under s.91(1) and 91(2) of EPOCA, TCRA is also a custodian of the subscribers' information, yet there is no provision in EPOCA which places upon it a duty of confidentiality. Although such a duty may be implied under s.99 of EPOCA, it is still not adequate to bring TCRA within its ambit.[41] And the duty of confidentiality imposed under this provision is limited to “any information” received in accordance with the provisions of EPOCA. Unfortunately the phrase “any information” as used in s.98(1) of EPOCA ***C.T.L.R. 52*** is not defined. However, viewed narrowly, the information referred to here may be that which reveals the identity of a subscriber which was submitted by a subscriber and obtained by a service provider during registration of SIM cards. This is because, when reading ss.93 and 94 of EPOCA, reference is only made to this type of information. However, when one reads s.98(1) in conjunction with s.98(2), which prohibits disclosure of the “content of information” of any customer received in accordance with the provision of EPOCA, it definitely appears that the phrase “any information” as used in s.98(1) is broad enough to encompass “content of information”. The latter is sometimes referred to as “content of communication”. Section 3 of EPOCA defines the term “content” as information in the form of speech or other sound, data, text or images whether still or moving, except where transmitted in private communications. This type of information is not the one submitted during registration of SIM cards but the actual messages or conversations transmitted over service providers' networks when one makes a call to another person. One could therefore argue that EPOCA is an interception law as it authorises interception of subscribers' content of communication, because it would be illogical for the Act to prohibit disclosure of the content of information which was not intercepted and retained in the first place.

As has been indicated above, s.98(2) of EPOCA permits disclosure of content of communication where persons who disclose such information are authorised by “any other written law”. The phrase “any other written law” is open-ended. This article attempts a non-exhaustive analysis of such laws in order to determine if they incorporate adequate safeguards for the protection of individuals' right to privacy. The Prevention of Terrorism Act[42] is one such law which authorises interception of communication. Section 31 of this Act empowers a police officer[43] to intercept communications in connection with the investigation of terrorist offences.[44] However, before the police officer intercepts such communication he must apply ex parte to the High Court of Tanzania[45] and obtain a warrant of interception of communications order. A police officer may only make an application for interception of communication order with prior consent of the Attorney General.[46] The High Court, if satisfied that there are reasonable grounds to believe that material information relating the commission of a terrorist offence or the whereabouts of a suspect of terrorist offence is contained in that communication or communications of that description, may make an order requiring a service provider to intercept and retain specified communication(s) received or transmitted, or about to be received or transmitted by the service provider.[47] Alternatively, the court may authorise the police officer to enter any premises, and to install on such premises any device for the interception and retention of a specified communication(s), and subsequently to remove and retain it.[48] While s.31 of the Prevention of Terrorism Act seems to have fulfilled the procedural requirement of art.16(2) of the Tanzanian Constitution, it is doubtful if the same has satisfied the proportionality test under art.30(2) of this Constitution. This is because s.31 does not state a limitation period for the order which the High Court may grant. Because of this, a person who is a target of the said interception may find his communication intercepted throughout, under the justification of an interception order of the High

Court even when such investigation fails to reveal any material information linking him or her with the alleged terrorist offence. Apart from that, this section is silent on what will happen to the communication tapped by the police officer if it is not sufficient to warrant prosecution of the suspected person. Closely similar to the Prevention of Terrorism Act is the Tanzania Intelligence and Security Service Act.[49] Section 15(1) of this Act empowers the Tanzania Intelligence and Security Service (TISS) to investigate any person or body of persons whom it has reasonable cause to consider a risk or a source of risk of a threat to the state security. In the course of investigation, TISS can institute surveillance of any person or category of persons.[50] It is worth noting that the Tanzania Intelligence and Security Service Act contains the term “intercept” in the definition section but the term is not found in any other provision of the Act. According to s.3, the word “intercept”, in relation to any communication not otherwise lawfully obtainable by the person making the interception, includes to hear, listen to, record, monitor or acquire the communication, or acquire its substance, meaning or purport. And the word “interception” has a corresponding meaning to the word “intercept”. However, the Act uses the term “surveillance” in its substantive provisions instead of “interception”. Unfortunately, the former term is not defined in the definition section of the Act. However, surveillance simply means the monitoring of the behaviour, activities or other changing information, usually of people and often in a surreptitious manner.[51] The former includes interception of electronically transmitted information.[52] It is arguable that although the Tanzania Intelligence and ***C.T.L.R. 53** Security Service Act has avoided using the term “interception”, it still authorises interception under the umbrella of surveillance. Moreover, since under s.28(2) of the Prevention of Terrorism Act, a police officer also includes a member of the Tanzania Intelligence Security Service, the latter may still enforce interception under that law. Be that as it may, the Tanzania Intelligence and Security Service Act, when measured against the provision of art.16 of the Tanzanian Constitution, falls below the constitutional protection of the right to privacy. This is because the Act does not prescribe any procedure for such interception. The interception is warrantless. Moreover, this Act broadly and loosely defines grounds for authorising interception. It simply provides state security as a blanket ground for interception.

Besides the interception and disclosure of information under “any other written law” clause, EPOCA itself authorises interception and disclosure of communication. Section 99 states:

“A person shall not disclose any information received or obtained in exercising his powers or performing his duties in terms of this Act except -- (a) where the information is required by any law enforcement agency, court of law, or other lawfully constituted tribunal; (b) notwithstanding the provision of this section, any authorized person who executes a directive or assist with execution thereof and obtains knowledge of information of any communication may -- (i) disclose such information to another law officer to the extent that such disclosure is necessary for the proper performance of the official duties of the authorised person making or the law enforcement officer receiving the disclosure; or (ii) use such information to the extent that such use is necessary for the proper performance of official duties.”

As can be noted from this provision, the grounds for interception and subsequent disclosure of communication is only the need of such information by a law enforcement agency, court of law or tribunal. There are no other criteria. In effect therefore, when there is no specific provision in “any other written law” authorising a person to intercept and retain the content of communication or other type of personal information, such person may still fulfil the requirements of s.98(2) by resorting to s.99 of EPOCA. He can just come forward and tell the service provider he wants certain information relating to a specific person by merely introducing himself as a police officer carrying out an investigation related to that person. Assessed from the constitutional right to privacy in art.16 of the Tanzanian Constitution, it obviously appears that s.99 of EPOCA fails to pass the proportionality test. This is because the provision does not safeguard in any way subscribers' personal information held in the subscribers' database. Moreover, no one is placed in a position to scrutinise whether the need for intercepted information is justifiable in any way. Because of this, subscribers' personal information is unsecured. Moreover, their communication can be intercepted at any time without any appropriate remedy. Although EPOCA makes it an offence for any unauthorised person to intercept and disclose any information,[53] or for an authorised person, having intercepted such communication, to unlawfully disclose it,[54] it is difficult to enforce these provisions given the broad and loose drafting of ss.98 and 99 of EPOCA. Moreover, the Commission for Human Rights and Good Governance,[55] which is ordinarily vested with powers to deal with complaints arising from breach of the Bill of Rights, is not well placed to make enforcements in relation to breaches of the constitutional right to privacy. This is because the Commission cannot impose any binding determination. It can only make an investigation of complaints and offer recommendations to the appropriate authority or a person in authority.[56]

Conclusion

The analysis of the provisions of EPOCA regulating registration of SIM cards has revealed that EPOCA is an interception law. Because of that, the Act was supposed to comply with the provisions of art.16 of the Tanzanian Constitution which guarantees the right to privacy. As it is now, EPOCA fails to provide adequate safeguards to privacy of personal information held in the subscribers' database as well as the content of communications. The Act broadly and loosely defines grounds for authorising interception and disclosure of the content of communication as well as personal information revealing the identity of subscribers. Moreover, it fails to provide clear and adequate procedures for interception and disclosure of communications. Where EPOCA permits interception and disclosure of information through ***C.T.L.R. 54** authorisation of other written laws, assuming that such laws provide grounds for interception and safeguards, it has been revealed that such laws also fall short of the required constitutional standards. Similarly, the permission of interception and disclosure of information within EPOCA itself is problematic. Where a law enforcement agency such as the police, a court of law or a tribunal needs any information including content of information of a particular subscriber, this is a sufficient ground to require a service provider to make a supply. There is no warrant required from a judge to initiate such a supply. Because of these loopholes, the author recommends that EPOCA be amended immediately to put in place a harmonised procedure for interception of communications. A warrant for interception from a judge is highly recommended. In the same vein, a court of law should not be one of the institutions which may require intercepted information, as is now the case. Also, the grounds for interception must be clearly defined in the said amendments. The current and the only ground for supply of intercepted information which is based on the mere need of a law enforcement agency, a court of law or a tribunal, should be repealed. Finally, there should not be double standards in different laws. For example, while interception of communications under the Prevention of Terrorism Act requires the warrant of a judge, interception under the Tanzania Intelligence and Security Service Act does not require such a warrant from a judge. The reasoning behind this recommendation is that, in both cases, interception of communication is an ultimate result; hence compliance with the provisions of art.16 of the Tanzanian Constitution is mandatory.

C.T.L.R. 2011, 17(2), 48-54

---

1. See Tanzania Communication Regulatory Authority, “Public Notice: SIM Card Registration”, at *http://www.tcra.go.tz/headlines/simcardRegEng.pdf* [Accessed December 29, 2010]; see also Daily News, January 29, 2009, p.3.

2. See Tanzania Communication Regulatory Authority, “Press Release: SIM Card Registration”, at *http://www.tcra.go.tz/headlines/SimRegPublicNoticeEn.pdf* [Accessed December 29, 2010].

3. See *The Guardian,* July 1, 2010, pp.1-2; See also *The Citizen,* July 1, 2010, p.2.

4. These reasons were explained in the subsequent notices for extension of SIM registration. However, the initial public notice indicated only security as the reason for SIM card registration.

5. TCRA's directive, being administrative in nature, would not satisfy the requirements of art.16(2) of the Tanzanian Constitution which requires that any derogation to the constitutional right to privacy enshrined in art.16(1) of the Constitution must lay down legal procedure for that derogation. Moreover it must pass the proportionality test. Further discussion on this aspect is provided later in this article; see also M. Murungi, “Registration of Mobile Phone Users: Easier said but carefully done” (July 25, 2009), at *http://kenyalaw.blogspot.com/2009/07/registration-of-mobile-phone-users.html* [Accessed December 29, 2010].

6. See BUNGE LA TANZANIA, MAJADILIANO YA BUNGE, MKUTANO WA KUMI NA MBILI, Kikao cha Arobaini na Saba -- Tarehe, August 18, 2008.

7. What a subscriber is required is just to report the theft to the service provider and his or her mobile phone number. The service provider may trace the IMEI and block it. See also *http://virgintech.org/how-to-block-lost-mobile-phone-by-imei-number.html* [Accessed December 29, 2010].

8. For example, in a bid to fight against cell phone theft, the East African mobile phone service providers in 2003 signed a memorandum of understanding (MoU) binding them to offer reciprocal stolen phones blacklisting services on their networks. Tanzania's Celtel, Vodacom, Mobitel and Zantel as well as Uganda's MTN, UTL and Celtel Uganda, and Kenyan Safaricom and KenCell activated their equipment identification registers (EIR) in that regard without having any requirement for registration of SIM cards in place for their respective subscribers; see *http://www.cellular.co.za/news_2003/122003-african_gsm_operators_create_mob.htm* [Accessed December 29, 2010].

9. This is according to the author's interviews with some employees working in the marketing departments of the service providers in Tanzania. The author carried these interviews between July 2010 and September 2010. None of the interviewees allowed their names to be disclosed because of preserving their job security.

10. Author's interviews.

11. For example, in September 2010 there was a wide circulation of a hoax text message in Tanzania warning people that they would die if they received calls whose numbers were in red. The message raised fear and panic among most Tanzanians. Some people challenged the registration of SIM cards which aimed at enhancing security from misuse of mobile phones; see *The Guardian,* September 6, 2010, pp.1-2; *The Guardian,* September 7, 2010, pp.1-2; *The Guardian,* September 12, 2010, pp.1-3, 18; *The Citizen,* September 6, 2010, p.8; *Daily News,* September 9, 2010, p.1; *Dar Leo,* September 8, 2010, pp.1 and 4; *Uwazi,* September, 14-20, 2010, pp.1 and 3; and *Sani,* September 11-14, 2010, pp.1-2. There were also defamatory and hateful text messages circulated to millions of Tanzanians in the political campaign for the last October 31, 2010 general elections, attacking presidential candidates for Chama cha Demokrasia na Maendeleo (CHADEMA) and the Civic United Front (CUF), two opposition parties; see *The Guardian* (October 17, 2010), at *http://www.ippmedia.com/frontend/index.php?l=22119* [Accessed December 29, 2010].

12. See JamiiForums, "SIM Card Registration in Tanzania Now a Must", discussions held on January 28, 2009, at *http://www.jamiiforums.com/jukwaa-la-siasa/23569-simcard-registration-in-tanzania-now-a-must-2.htm* [Accessed December 29, 2010]; see also allAfrica.Com, "Tanzania: SIM-Card Registration Now Viewed As Spying Move" (November 8, 2009), at *http://allafrica.com/stories/200911091473.html* [Accessed December 29, 2010].

13. This period was extended twice. First, from December 31, 2009 to June 30, 2010 and from July 1, 2010 to July 15, 2010.

14. See *Government Gazette,* No.19 of May 7, 2010.

15. See Electronic and Postal Communications Act 2010 s.186.

16. Cap. 306 R.E 2002.

17. Cap. 302 R.E 2002.

18. See Electronic and Postal Communications Act 2010 ss.169-185.

19. Cap. 172 R.E 2002.

20. Cap. 285 R.E 2002.

21. See Electronic and Postal Communications Act 2010 s.168(2).

22. See Electronic and Postal Communications Bill 2009 "Objects and Reasons" at p.115.

23. Cap. 2 R.E 2002

24. These restrictions will be discussed when considering case law developed by courts in Tanzania.

25. See for example, *Kukutia Ole Pumbun v Attorney General*[1993] T.L.R. 159; *Julius Ishengoma Francis Ndyanabo v Attorney General* , Civil Appeal No.64 of 2001, Court of Appeal of Tanzania, at Dar es Salaam (Unreported); *Legal and Human Rights Centre v Attorney General,* Miscellaneous Civil Cause No.77 of 2005, High Court of Tanzania, at Dar es Salaam (Unreported); *Christopher Mtikila v Attorney General,* Miscellaneous Cause No.10 of 2005, High Court of Tanzania, at Dar es Salaam (Unreported).

26. EPOCA s.93(1). However it is doubtful if this obligation extends to persons who had acquired SIM cards prior to the coming into force of EPOCA. This is because on July 1, 2009 when registration of SIM cards in Tanzania commenced, there was no legal obligation in its support. TRCA only issued a public notice requiring all service providers to register SIM cards for their subscribers. Part of this notice reads: "Pre-paid subscribers who have up to now not been registered shall be registered by their respective telecommunication service providers within a period of six months from 1st July, 2009 … With effect from 1st July, 2009 any new pre-paid subscribers shall be registered by their respective telecommunication service providers as soon as they start using a new SIM-card … Appropriate legislation is in the process through which registration of every person desiring to own and use a SIM-card shall be mandatory." Worse still, EPOCA has no provision for the retrospective operation of the Act in order to take into account previous registered and unregistered SIM cards.

27. EPOCA ss.93(2) and 94(1).

28. EPOCA s.93(2)(a).

29. EPOCA s.93(2)(b).

30. EPOCA s.93(2)(c).

31. EPOCA s.93(3)(b); practically no verification has ever been done prior to registration of SIM card. Stakeholders raised concern over lack of national IDs in the registration process (see *Daily News,* June 27, 2010, p.3), as such subscribers would come with various sorts of identification cards and get registered. It is therefore doubtful if the information submitted was accurate in the first place. This, in the author's view, will still complicate the ability of the database to trace criminals because of the possibility of false information with which criminals might have been registered. See also E. Sutherland, "The Mandatory Registration of SIM cards" [2010] C.T.L.R. p.61.

32. EPOCA s.93(4).

33. EPOCA s.95.

34. EPOCA s.91(3).

35. EPOCA s.91(1) and (2).

36. M. Froomkin, "The Death of Privacy?" (2000) 52 *Stanford Law Review* 1464, at *http://personal.law.miami.edu/%EBfroomkin/articles/privacy-deathof.pdf* [Accessed December 29, 2010].

37. Froomkin, "The Death of Privacy?" (2000) 52 *Stanford Law Review* 1464, at *http://personal.law.miami.edu/%EBfroomkin/articles/privacy-deathof.pdf* [Accessed December 29, 2010].

38. See R. Clarke, "Information Technology and Dataveillance" (1988) 31 Commun. ACM 498, at *http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html* [Accessed December 29, 2010].

39. See above fn.31.

40. Under s.91(1) and (2) of EPOCA, TCRA is also a custodian of the subscribers' information, yet there is no provision in EPOCA which places upon it duty of confidentiality. Although such a duty may be implied under s.99 of EPOCA, it is not adequate to bring TCRA within its ambit.

41. The obligation of confidentiality of customers' content of communication is also repeated in reg.12 of the Tanzania Communications (Consumer Protection) Regulations 2005 (Government Notice No.271 of 2005).

42. Act 21 of 2002.

43. In this context, a police officer means a police officer of or above the rank of assistant superintendent, an immigration officer or a member of the Tanzania Intelligence Security Service; see s.28(2) of the Prevention of Terrorism Act 2002.

44. For what constitutes terrorist offences see s.4 of the Prevention of Terrorism Act 2002.

45. Prevention of Terrorism Act 2002 s.31(1); note also that for Zanzibar, the High Court of Zanzibar is responsible to authorise interception under the Prevention of Terrorism Act.

46. See Prevention of Terrorism Act 2002 s.31(2).

47. See Prevention of Terrorism Act 2002 s.31(3)(a).

48. See Prevention of Terrorism Act 2002 s.31(3)(b).

49. Cap. 406 R.E 2002.

50. Tanzania Intelligence and Security Service Act ss.5(1)(d) and (2) (b).

51. See *http://en.wikipedia.org/wiki/Surveillance* [Accessed December 29, 2010].

52. See *http://en.wikipedia.org/wiki/Surveillance* [Accessed December 29, 2010].

53. Section 120 of EPOCA states: “120, Any person who, without lawful authority under this Act or any other written law -- (a) intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept any communications; or (b) discloses, or attempts to disclose to any other person the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or (c) uses, or attempts to use the contents of any communications, knowingly having reason to believe that the information was obtained through the interception of any communications in contravention of this section, commits an offence and shall, on conviction, be liable to a fine of not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both.”

54. Section 121 of EPOCA states: “121(1), Any person who is authorized under this Act intentionally discloses, or attempts to disclose, to any other person the contents of any communications, intercepted by means authorized by this Act -- (a) knowing or having reason to believe that the information was obtained through the interception of such communications in connection with a criminal investigation; (b) having obtained or received the information in connection with a criminal investigation; or (c) improperly obstructs, impedes, or interferes with a duly authorized criminal investigation, commits an offence and shall, on conviction, be liable to a fine of not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both. (2) It shall be lawful under this Act for an officer, employee or agent of any network facilities provider, network service provider, application service provider or content service provider whose facilities or services are used in communications, to intercept, disclose, or use those communications in the normal course of his employment while engaged in any activity which is a necessary incident to the performance of his facilities or services or to the protection of the rights or property of the provider of the facilities or services, but the provider shall not utilize the facilities or services for observing or random monitoring unless it is for mechanical or service quality control or checks.”

55. See ss.5 and 6 of the Commission for Human Rights and Good Governance Act 2001(Act 7 of 2001).

56. Commission for Human Rights and Good Governance Act s.17(1).