
***Data Protection under the
Nigerian Mobile Phone
Subscriber Registration
Scheme***

Content:

Abstract

Background

Right to Privacy

Overview of NCC Draft Regulation

Conclusion

Abstract

The Nigerian Communications Commission (“NCC”) recently adopted a scheme to register all users of the Subscriber Identity Module (SIM) Cards in Nigeria. This newsletter examines the legal issues surrounding the scheme; specifically, it examines Nigerian privacy rules and the NCC Draft Regulation in comparison with European privacy rules and data protection framework.

Background

In December 2009, NCC announced plans to embark on a registration of all SIM Card users (mobile phone subscribers) and directed telecommunications companies in Nigeria to put arrangements in place for a smooth takeoff of the scheme.¹ NCC said that the registration scheme became necessary following the spate of criminal activities in Nigeria, especially those perpetuated through mobile phones. It said that registration would assist Nigerian Law Enforcement Officers to address the rate of crime, as opposed to the current inability to directly link individual subscribers to particular phone numbers. Pursuant to powers conferred on it by sections 1(i) and 70 of the Nigerian Communications Act 2003 (“NCC Act”), NCC has published a Draft Regulation to regulate the scheme.² The registration is in two phases; the first phase of the process, which is currently ongoing, involves the registration of all subscribers acquiring new SIM Cards before the SIM Cards could be activated. NCC has said that the

¹ Chris Uba, “Telecom operators, subscribers rebuff SIM Card registration,” available at <http://www.itnewsafrika.com/?p=7813> (last accessed 10 December 2010).

² Available at <http://www.ncc.gov.nig/> (last accessed 10 December 2010).



second phase of the scheme (registration of existing subscribers) will commence at a date to be subsequently announced.³ It warned that once a deadline is set for registration, unregistered numbers would be suspended at the end of the exercise.

While NCC believes that registration of mobile phone subscribers would check the spate of criminal activities in Nigeria, other stakeholders have expressed fears over the exercise. Telecommunications operators believe that the scheme portends loss of profit, as Nigerians would be less likely to purchase new SIM Cards for fear of supplying their personal information to the wrong people.⁴ Subscribers also fear that the scheme may result in undue exposure of subscribers' personal information, resulting in loss of privacy.⁵ The latter forms the focus of this newsletter.

Right to Privacy

The new registration scheme requires mobile phone operators in Nigeria (defined under the NCC Draft Regulation as "Licensees") to register new subscribers,⁶ while SIM Card Registration Solution Providers (SCRSPs)⁷ are

required to provide solutions to facilitate registration of existing subscribers. To register, subscribers are required to provide the designated organizations with biometrics (finger prints and facial photographs) and other personal information.⁸ Reports have also revealed that a number of other documents are required for identification during the registration process, including E-passports, company or work place identity cards that contain pension identification/tax numbers, student identity cards from recognized institutions, as well as drivers' licenses issued by the Federal Road Safety Commission and E-Tax cards.⁹

This information has relevance on the privacy of subscribers, and in the age of identity theft and cybercrime (most prominent in Nigeria), recording and storing such information in a private or public database without appropriate legal frameworks may expose subscribers to significant risks. Presently, the only cushion against invasion of privacy of individuals seems to be the Constitution of the Federal Republic of Nigeria 1999 ("the Constitution" or "the 1999 Constitution"),¹⁰ which provides that:

*The privacy of citizens, their homes, correspondence, telephone conversations, telegraphic communications is guaranteed and protected.*¹¹

³ There are indications that registration of existing subscribers has already commenced.

⁴ Ikechukwu Osodo, "SIM card registration in Nigeria triggers hot debates" available at <http://www.itnewsafrika.com/?p=3493> (last accessed 10 December 2010).

⁵ Toyin Willoughby Muiy, "How secure is this SIM registration," available at <http://www.tribune.com.ng/sun/index.php/front-row/2583> (last accessed 10 December 2010).

⁶ Registration is currently ongoing.

⁷ Defined in the NCC Draft Regulation as "companies contracted by the Commission for the conceptualization, design, development, and delivery of SIM Card Registration Solutions covering all licensees, and providing detailed

Subscriber information in a manner facilitating seamless integration into the central database."

⁸ Defined by NCC Draft Regulation as "Subscriber Information," Part 1(1) of NCC Draft Regulation.

⁹ Chris Uba, "Telecom operators, subscribers rebuff SIM Card registration," available at <http://www.itnewsafrika.com/?p=7813> (last accessed 10 December 2010).

¹⁰ The Constitution of the Federal Republic of Nigeria 1999; section 37.

¹¹ Section 37



The Constitution further provides that there shall be no interference with any of the rights conferred in section 37 among others, except in accordance with:

... any law that is reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom of other persons.¹²

One question that comes to mind, therefore, is whether the NCC scheme can sufficiently come under any of the exceptions in section 45(1) of the Constitution to justify the invasion of the privacy of mobile phone subscribers, most of whom are Nigerian citizens? One clear fact is that the Draft Regulation cannot be classified as a "law" under section 45(1) of the Constitution, as such, it cannot confer legitimacy on acts performed thereof. However, NCC could rely on section 1(i) of the NCC Act for legitimacy of its registration scheme.¹³

Outside the shores of Nigeria, the European Convention on Human Rights (ECHR)¹⁴ provides an illustration of how an individual's data is protected from invasion. It recognizes that:

¹² Section 45(1) 1999 Constitution

¹³ Section 1(i) of the NCC Act confers on the NCC the right to inter alia, ensure efficient registration and use of scarce national resources in the communication sub-sector, and also promote and safeguard national interests, safety, and security in the use of the scarce national resources.

¹⁴ Article 8

everyone has the right to respect for his private and family life, his home and his correspondence, as such there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety and economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.

This piece of legislation amply specifies the circumstances in which an individual's data may be processed or transmitted in order not to breach guaranteed rights, and is similar in many respects to the provisions of sections 37 and 45(1) of the Nigerian Constitution. However, while Nigeria appears to stick to the provision of the 1999 Constitution without more, ECHR has influenced a couple of other data protection legislation within the European Union and its Member States.¹⁵ The European Data Protection Directive¹⁶ provides the basic principles for collecting, processing, transmitting and transferring personal data legitimately to avoid misuse. The Directive defines "personal data" as *any information relating to an identified or identifiable natural person ('data subject')*. It defines "processing of personal data" to mean *any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage,*

¹⁵ See for instance the UK Data Protection Act of 1998.

¹⁶ Directive 95/46/EC



adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. It further defines "processor" to mean *a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.*¹⁷

The Principles require that personal data must be:

- a) processed fairly and lawfully;¹⁸
- b) collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;¹⁹
- c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;²⁰
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purpose for which they were collected or for which they are further processed, are erased or rectified;²¹
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed;²²

¹⁷ "Controller" is defined as a person within the classification (i.e. natural or legal person, public authority, agency or any other body) which alone or jointly with others determines the purposes and means of processing of personal data.

¹⁸ Article 6(1)(a)

¹⁹ Article 6(1)(b)

²⁰ Article 6(1)(c)

²¹ Article 6(1)(d)

²² Article 6(1)(e)

- f) data subject to be given right of access to personal information held by the controller in accordance with the provisions of the Directive;²³ and
- g) appropriate technical and organizational measures to be taken to protect personal data against accidental or unlawful destruction, or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves transmission of data over a network, and against all other unlawful forms of processing.²⁴

In recognition of the protection guaranteed under ECHR, the Directive specified circumstances when Member States may restrict the scope of the obligations and rights specified above, as when such restriction constitutes a necessary measure to safeguard:

- a) national security;
- b) defense;
- c) public security;
- d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- e) important economic or financial interest;
- f) monitoring, inspection or regulatory function connected, with the exercise of official authority in cases referred to in (c), (d) and (e) herein; and
- g) the protection of the data subject or of the rights and freedom of others.²⁵

Overview of NCC Draft Regulation

²³ Article 12

²⁴ Article 17(1)

²⁵ Article 13



As noted earlier, the provisions of sections 37 and 45(1) of the 1999 Constitution seem to be the only cushion against invasion of subscribers' privacy in Nigeria. However, since announcing its plans under the SIM Card registration scheme, NCC has attempted to put additional rules in place. Notwithstanding that the scheme has already commenced, these rules are still in draft forms. The provisions of the Draft Regulation, however, suggest a resolve on the part of NCC to protect the privacy of subscribers in accordance with the provisions of the Constitution. Some of the provisions of the Draft Regulation are as follows:²⁶

- a) NCC is charged with care, control and management of all subscriber information received from Licensees and SCRSPs.²⁷
- b) Licensees and SCRSPs are prohibited from dealing, duplicating or making copies of subscriber information for any purpose other than those stipulated under the Draft Regulation or other law in Nigeria.²⁸
- c) Licensees and SCRSPs are prohibited from retaining subscriber information on their database, and shall cause same to be deleted upon transmission to a central database which NCC shall designate; Licensees are permitted to retain information on subscribers who hold at least one SIM card on their networks on the date of registration.²⁹
- d) Licensees shall use such information retained pursuant to the Draft Regulation³⁰ solely for their operations

and shall not release the information to third parties without the prior written consent of the relevant subscriber;

- e) The Draft Regulation stipulates that subscribers' information shall be held on a confidential basis,³¹ However, such subscribers' information may be provided to a security agency on a written request of a high ranking official of the agency (Assistant Commissioner of Police or its equivalent in any other security agency),³² unless where the release of such information to the security agency would constitute a breach of the 1999 Constitution, or any other law in force in Nigeria, or be a threat to national security.³³

The Draft Regulation further mandates Licensees to take all precautions to preserve the integrity and prevent any corruption, loss or unauthorized disclosure of subscriber information retained pursuant to paragraph 9(5). In addition, such Licensees must take steps to restrict the unauthorized use of subscriber information by its employees who may be involved in the capture and or processing of such information.

A brief comparison between the NCC Draft Regulation and the European Data Protection Directive reveals a number of gaps in the Draft Regulation as follows:

- a) The Draft Regulation failed to define what constitutes processing of personal data or subscriber

²⁶ Part 5 NCC Draft Regulation

²⁷ Paragraph 9(3) NCC Draft Regulation

²⁸ Paragraph 9(4) NCC Draft Regulation

²⁹ Paragraph 9(5) NCC Draft Regulation

³⁰ Permission to retain subscriber information was contained in Paragraph 9(5) of Draft Regulation.

However, the Draftsman wrongly referred to paragraph 9(7) as the source of retained subscriber information.

³¹ Paragraph 9(4) NCC Draft Regulation

³² Paragraph 9(7) NCC Draft Regulation

³³ Paragraph 9(10) NCC Draft Regulation



- information. A broad meaning should be given to this definition so far as is necessary to protect subscribers;
- b) The Draft Regulation failed to identify the subscribers' right to privacy or other rights that may accrue to such subscribers, including right of access to personal information;
 - c) The Draft Regulation failed to clearly and explicitly state the purpose for which subscriber information may be processed, so as to exclude processing for illegitimate purposes. This is a very important requirement, without which legitimacy cannot be conferred on the process;
 - d) There is no provision in the Draft Regulation to ensure regular update of information entered in the database after the first entry. This is closely related to the issue of accuracy of information held in the central database and may defeat the purpose of the scheme where information becomes inaccurate or incomplete due to change in circumstances of subscribers, for instance change of address;
 - e) The Draft Regulation failed to recognize that the NCC itself or its officers may breach subscribers' right to privacy, as such it failed to confer any obligations on NCC or its employees to prevent misuse of information contained in the central database; and
 - f) Finally, the Draft Regulation failed to specify the technical and organizational measures to be taken to protect personal data against accidental or unlawful destruction, or accidental loss, alteration, unauthorized disclosure or access.

It is pertinent to note that the privacy of mobile phone subscribers is severely exposed and may be breached each day any information is processed without adequate guidelines to regulate the activities of the Licensees, SCRSPs, and even the NCC itself. There is therefore the need to finalize and implement the Draft Regulation especially as it relates to privacy obligations and data protection.

Conclusion

Much as we applaud the ingenuity of the NCC under the Draft Regulation wherein it sought to provide guidelines for registration under the scheme, we must not fail to point out that only a comprehensive Data Protection legislation in Nigeria, in line with international standards and best practices, would consolidate the legal framework and provide the necessary guidelines for processing subscribers' information. In most jurisdictions where mobile phone registration exercises were conducted in recent times,³⁴ efforts were made to implement Data Protection Legislation to confer legitimacy and regulate activities of processing organizations prior to commencement and conclusion of the exercises. NCC may need to liaise with the National Identity Management Commission³⁵ to sponsor a Data Protection Bill, which should be fast tracked given that the registration exercise has already commenced.

In addition, the objective of the scheme needs to be clearly defined. NCC may need to clearly specify (in the Draft Regulation or other

³⁴ For instance Kenya.

³⁵ A body created by the National Identity Management Commission Act 2007 to register and issue Multipurpose Identity Cards to Nigerian citizens, permanent residents and non-citizens who have resided in Nigeria for two years or more.



legislation to be drafted) the purpose for which information may be processed, so as to exclude processing for illegitimate purposes.

There is also need for continuity, so as not to defeat the purpose of the scheme. NCC would need to make provisions for regular update of personal information in the central database to accommodate circumstance that may occur after the first phase of registration, including change of address or loss of SIM Cards. NCC may also need to put in place a plan of action that would ensure sustainability beyond the registration deadline to ensure subsequent registration of subscribers (new entrants).

Care should be taken in the engagement of Consultants to ensure that NCC is properly guided throughout the process. It is therefore imperative for NCC to have on its retainer qualified Consultants with relevant expertise to provide effective guidance throughout the process.

Disclaimer: This document serves merely as a note and is not intended to provide legal advice to any person or group of persons whether natural or corporate regarding the issues discussed herein. All persons desirous of legal advice should therefore contact a lawyer. Aina Blankson LP shall not be liable for any breach or loss resulting from reliance on any part of this newsletter.

For further information, please contact:

- *Abayomi Alabi* a.alabi@ainablankson.com
- *Chinonyelum Uwazie* c.uwazie@ainablankson.com
- *Kanayo Okoye* k.okoye@ainablankson.com
- *Paul Okonji* p.okonji@ainablankson.com