

CAMBRIDGE ANALYTICA SCANDAL: WHY NIGERIA NEEDS A DATA PROTECTION LAW

Background

Across the globe, many countries, including China, South Africa and member states of the European Union have taken steps in recent years to tighten the legal framework for the protection of data and personal information within their respective jurisdictions. Quite glaringly, the Nigerian Government has taken very little steps towards implementing a coherent legislation on data protection. Our data protection framework consists largely of legal provisions littered across numerous laws and regulations.

The recent scandal involving the unauthorized and unethical exploitation of data of Facebook users by Cambridge Analytica during the United States presidential election campaign in 2016 has once again brought to the fore issues of user privacy and protection of personal information across the global web community. Citizens of different countries desire protection from their respective governments against the violation of their personal information rights. Whilst the debate and discourse rage on, no legislative action has been taken in Nigeria to expedite the promulgation of a national framework for protection of personal information.

This article considers the current state of data protection regulation in Nigeria, highlights some deficits within the current regulatory framework and proposes legislative action to tighten the regulatory regime for the protection of personal information in the country.

State of Data Protection in Nigeria

Nigeria does not currently have a framework for the protection of information of persons whose personal information is collected (Data Subjects). Though there are diverse legislations that contain privacy protection



Image courtesy techspot.com

regulations, very few have general application, with most of the regulations targeted at specific sectors.

The few regulations, which have general application include:

- I. **The NITDA Guidelines on Data Protection (2017).** Issued by the National Information Technology Development Agency (NITDA) for the protection of Data Subjects who are residents and citizens of Nigeria, the Guidelines are applicable to the public and private sectors. Specifically, they are applicable to federal, state and local government agencies and institutions as well as data collectors, data custodians, data administrators, data systems auditors and data security organizations. They define the minimum data protection requirements for the collection, storage, processing, and management of personal information in Nigeria.

- II. **The Cybercrimes Act (2015).** This contains provisions on the retention and protection of data by public and private institutions in Nigeria. The Act requires internet service providers to keep traffic data information and subscriber information of Data Subjects for a period of two (2) years. Although service providers may release such information to law enforcement agencies, the privacy rights of the Data Subject must be considered, and the data may not be used illegally (Section 38 Cybercrimes Act).
- III. **The Constitution of the Federal Republic of Nigeria (1999).** This provides for the protection of the fundamental right of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications (Section 37 of the Constitution of the Federal Republic of Nigeria).

Other targeted regulations that provide for the protection of personal data of persons in Nigeria include:

- I. **Freedom of Information Act (2011).** This contains provisions that protect personal information of persons and information that is subject to professional privilege. The Act requires that applications for information, which includes personal information of Data Subjects, should be denied by public institutions unless consent of the Data Subject is obtained, or where such information is publicly available (Section 14 of the FOI Act). Furthermore, public institutions may deny applications for disclosure of information that is subject to professional privilege conferred by law (such as attorney-client privilege) (Section 16 of the FOI Act).
- II. **Credit Reporting Act (2017).** This grants Data Subjects rights to the privacy, confidentiality and protection of their credit information, except permitted disclosures such as disclosure to a credit bureau or where the Data Subject is involved in a financial or credit related malpractice (Section 9 of the CR Act).

- III. **Consumer Code of Practice Regulations (2007) and the Registration of Telephone Subscribers Regulations (2011).** Issued by Nigerian Communication Commission, both regulations provide for the protection of subscriber information by telecommunication service providers operating in Nigeria.
- IV. **National Identity Management Commission Act (2007).** This prevents access to data or information of citizens contained in the database of the National Identity Management Commission (NIMC). The exceptions would be under permitted circumstances such as where the provision of such information is in the interest of national security, or necessary for the prevention or detection of crime or any other purpose specified by the NIMC (Section 26 of the NIMC Act).

Lapses in Nigeria's Current Data Protection Framework

Whilst Nigeria currently has a plethora of regulations that touch on data protection, a comparison with the data protection frameworks in other jurisdictions reveals that there are several lapses, which need to be remedied if the country is to achieve comparative levels of personal information protection. Some of the noticeable gaps in the current data protection framework include:

- I. **Multiple Loopholes in the Current Regulatory Framework:** Several loopholes currently subsist in the existing data protection regime, and these include the absence of: (a) a mandatory legal requirement to report data security breaches or losses suffered by Data Subjects to law enforcement agencies; (b) a compensation framework for Data Subjects who have suffered a violation of their data rights; (c) a requirement for the registration of Data Controllers and databases; and (d) absence of specific data protection regulations in critical sectors such as e-commerce, services, human capital, healthcare, education, utilities, etc.

- II. Absence of Codified Data Protection Framework:** Nigeria currently lacks a defined regulatory framework for the protection of personal information and sensitive consumer data. Unlike the codified data protection regime established under recognized national legislations such as the Data Protection Act 2012 of Ghana and the Federal Data Protection Act 2017 of Germany; Nigeria continues to rely on various targeted data protection regulations. Consequently, data use and protection in many critical sectors remain largely unregulated.
- III. Lack of Centralized Data Protection Authority:** There is currently no single authority charged with the protection of data and enforcement of existing data protection laws and regulations. Contrary to what obtains in Nigeria, South Africa established the Office of the Information Regulator under the Protection of Personal Information Act 2013 with widespread powers on the protection of personal information, though the country's laws on protection of personal information are also currently straddled across multiple regulations.
- IV. Absence of State and Local Data Protection Laws:** Whilst Nigeria's current regime is similar to what obtains in the United States of America (USA), there is a marked difference., Nigeria currently does not have data protection laws at the state level. Unlike the USA and Germany, the gaps created by the absence of sufficient data protection laws at the federal level is not remedied at the state level. In Germany for instance, every state has its own Data Protection Authority that is responsible for data enforcement within its territory.
- V. Failure to Criminalize Illegal Use of Data:** The national criminal code, which is markedly out of date, fails to recognize or criminalize the illegal use of data. This is dissimilar to the practice in other jurisdictions. The criminal laws of China recognize the sale, illegal provision, or illegal access to personal information of the citizens as a crime, whilst the German Criminal Code recognizes violation of private secrecy as a criminal offence.

Recommendations

In order to address some of the regulatory lapses identified, there is a need to strengthen the existing framework for the use, collection and processing of personal information in Nigeria. We recommend that a single, consolidated federal legislation on data protection be passed, which should, at a minimum, contain provisions covering the following matters:

- I. The establishment of a national body charged with the powers to enforce data protection laws in Nigeria, as obtainable in countries such as Germany, South Africa and Ghana;
- II. Mandatory registration of Data Controllers operating within Nigeria and publication of details of data controllers in publicly accessible registers per the practice in the United Kingdom and Ghana;
- III. Mandatory disclosure and reporting of unauthorized access to or disclosure of personal information of data subjects, as is the practice in Ghana and Germany where such breaches must be reported to the data protection authorities and the Data Subjects;
- IV. Civil and criminal liabilities for persons, natural and legal, who illegally access, use, collect or dispose of personal information in Nigeria, such as those prescribed under the Data Protection Act 2012 of Ghana, and the Federal Data Protection Act 2017 of Germany;
- V. Recognition of the right of Data Subjects to request for information on the collection and use of their personal information, as recognized under the laws of other countries such as Germany;
- VI. Recognition of compensation of Data Subjects for the breach of the data protection obligations of Data Controllers, such as those recognized under the data protection laws of Ghana and Switzerland; and

VII. Mandatory and continuous sensitization of members of the public on their rights in relation to personal information, grievance procedure in relation to unauthorized use of data and remedies for breach of privacy.

In addition, it is recommended that the States of the Federation take steps to promulgate laws for the protection of personal information within their respective jurisdictions to compliment the federal law on protection of personal information.

Conclusion

As the data protection regimes of most advanced economies continue to evolve to match the ever-evolving technology landscape, Nigeria needs to take legislative actions, urgently, to improve its framework on protection of privacy and personal data of residents and citizens, in order to set in motion a process to catch up with internationally acceptable practices.



Image courtesy telegraph.co.uk

Detail Commercial Solicitors is distinct as Nigeria's first commercial solicitor firm to specialize exclusively in non-courtroom practice. Based in Lagos, Nigeria's business capital, DETAIL is totally committed to its clients' business objectives and reputed for dealing with the minutiae. Email: info@detailsolicitors.com

Detail

Detail Commercial Solicitors
DCS Place, 8, DCS Street,
Off Remi Olowude Way
Lekki Phase 1, Lagos, Nigeria
+234(0) 12771400-5
www.detailsolicitors.com