AUSTEN-PETERS & Co.

Business Law Digest

December 2015 ISSN 0795 -1124

BRIDGING THE GAP BETWEEN E-COMMERCE AND THE NEED FOR CONSUMERS' DATA PRIVACY

By – **Michael Dugeri**

E-commerce means the buying, selling, and exchange of products, services, and information via computer networks, primarily through the Internet. E-commerce penetration in Nigeria is still relatively low by global standards; however, the number of 'online consumers' is on the increase, making Nigeria a significant e-commerce force in the West African region.

Whenever a consumer shops online or engages in biometric registration, he/she hands over vital personal information such as their name, address, telephone number, and debit or credit card number, even intimate details like fingerprint, blood type, etc. What happens to this data if it falls into the wrong hands? What rights does the consumer have regarding the use of the data? Attempts to answer these questions show the gap that exists between e-commerce and consumers' personal data protection in Nigeria, which is due to inadequate legal and regulatory framework for personal data privacy and protection.

The benefits of e-commerce are immense. However, e-commerce also brings challenges, one of which is the need to protect the personal data of consumers. Most consumers want low-risk, maximum-security e-transactions that preserve the confidentiality of any private information. However, even as the use of personal data are becoming increasingly complex, and not fully disclosed to consumers, a personal data breach could have significant impact on the consumer involved and may lead to significant financial loss or inconvenience. Data privacy, in this context, means that consumers should be able to determine for themselves when, how and to what extent information about them is communicated to others. The difficulty in meeting this demand is compounded by the inter-connected nature of the e-transactions, which involve many parties in different locations/jurisdictions.

Companies and government agencies routinely collect personal data of consumers in e-commerce without deference or recourse to the National Identity Management Commission (NIMC). NIMC is the government agency statutorily charged with the responsibility to collect and store personal data of citizens. Yet, many other government agencies and companies are engaged in biometric registration of consumers, which entail the collection and storage of personal data on a large scale.

What is the safety of the data collected and what is the capacity of the collectors to safeguard it from unauthorized use? The NIMC Act does not contain sufficient safeguards on data privacy. The penalties for data breaches under the Act are weak and targeted mainly at third parties (hackers) than on the Commission and its staff in who are entrusted with the immediate care of enormous personal data.

Section 37 of the *Constitution of the Federal Republic of Nigeria 1999* (as amended) provides that 'the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications are hereby guaranteed and protected'. Beyond this general constitutional provision, the Central Bank of Nigeria (CBN) issued *Guidelines on Electronic Banking,* which enjoin banks and other financial institutions to safeguard customers' personal data in e-banking transactions. The obligation of Banks on customers' data privacy can also be inferred from the general duty of confidentiality, which exists between the bank and its customers. A banker owes his customer a legal duty of confidentiality not to disclose information to third parties, and any breach of this duty could give rise to liability in damages, if any loss results from the breach.

The above legal provisions on data privacy are limited in scope and application, and leave much to be desired. For instance, the CBN Guidelines are silent on the mandatory nature of its provisions, and curiously, they are silent on the penalty to be imposed by CBN on a bank that breaches its customers' personal data. As regards the common law duty of confidentiality, it is clear from a long line of cases on the principle that the duty of secrecy only arises from the contractual relationship between the banker and the customer. However, what happens where a third party bank or intermediary is involved, as is often the case with e-transactions? In such cases, issues of privity of contract and conflict of laws are bound to arise.

Governments in other jurisdictions adopt either of the two following approaches in addressing online data privacy issues: (a) promote a market-driven, self-regulatory approach, or (b) enact comprehensive data protection legislation. It is recommended that Nigeria should adopt the second approach, given its peculiar need to balance citizens' privacy needs and national security.

Data privacy and protection laws in most common law countries are modelled after the Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*. The basic principles of the Guidelines include the following:

The benefits of e-commerce are immense. However, e-commerce also brings challenges, one of which is the need to protect the personal data of consumers. E-consumers should be able to determine for themselves when, how and to what extent information about them is communicated to others.

a. *Collection Limitation* – personal data should be obtained by lawful and fair means.
b. *Data Quality* – personal data should be relevant to the purposes for which they are used, accurate, complete and kept up-to-date.

c. *Purpose Specification* – purposes for which the data are to be used should be specified and subsequent use should not be incompatible with these purposes.
d. *Use Limitation* – personal data should not be disclosed or used for purposes not specified unless consent is given by the data subject or under the authority of law.

Government in Nigeria needs to pay close attention to the manner business organisations collect and use personal data given its peculiar security challenges.

Government in Nigeria needs to pay close attention to the manner business organisations collect and use personal data given its peculiar security challenges. We need laws on data protection and privacy to protect on-line consumers and increase trust and confidence in e-commerce.

e. *Security Safeguards* – personal data should be protected by reasonable safeguards against loss, destruction or disclosure.
f. *Openness* – general policy of openness about developments with respect to personal data.
g. *Individual participation* – individuals have certain rights with respect to personal data controllers; and
h. *Accountability* – data controller is responsible for complying with these principles.

With respect to trans-border data flows, the Guidelines permit the restriction of free flow of data to countries without data protection laws. These basic principles are applicable to e-commerce, and can be embedded in a data protection and privacy law in Nigeria.

It is pertinent to note that some countries with peculiar security concerns have enacted data localization laws, in addition to data protection laws. Such legislation oblige businesses collecting the data of citizens, including on the Internet, to record, systematize, accumulate, store, update, change, and retrieve such in databases located within the country.

Nigeria should make laws on data protection and privacy to protect on-line consumers and increase trust and confidence in e-commerce. Such legislation must be effective, flexible, and efficient; and should balance the rights of consumers on the one hand and the economic interests of e-merchants, banks and other third parties on the other hand. Specifically, the law should provide that personal data can only be gathered legally under strict conditions, and for a legitimate purpose. Furthermore, persons or organisations, which collect and manage consumers' personal data should be required to protect it from misuse and to respect the rights of the data owners which are guaranteed under the law.

The consumers on their part must note that the e-transactions that give rise to the exchange of personal data are contractual, an integral part of which involves the manner the data is to be used. Even though these 'contracts' are standard form and drafted by the collectors, the consumers have a choice in entering them and in some cases, to negotiate the terms. Professional advice is also available to consumers in respect of real or potential data breach.

Editor's Note

The Federal Government has presented the 2016 budget proposal of N6 trillion to the National Assembly for approval. While the increased budgetary provision for capital expenses is meant to reflate the economy, there are funding concerns amidst dwindling oil revenue.

Meanwhile, the National Electricity Regulation Commission (NERC) has unveiled a new tariff regime for electricity with an increase of about N9.00 for all classes of consumers. NERC has also abolished the contentious fixed charges for all electricity consumers. These changes are meant to balance the commercial interests of the investors and consumers in a nascent competitive electricity market in Nigeria.

W: http://www.austen-peters.com/
Lagos: Penthouse Floor, Foreshore Towers, 2a Osborne Road, Ikoyi, Lagos, Nigeria. T: +23418990901, F: +23412713240
Abuja: Suite 06, 3rd Floor, Obum Plaza, Plot 1140, Adetokunbo Ademola Crescent, Wuse 2, Abuja. T: 234 (9) 870 2139