

Data Protection Legislation for Nigeria, The Time is Now! **Franklin F Akinsuyi (LL.B, B.L, MSc, LL.M) ¹**

Over the last decade, identity theft has become one of the fastest growing global crimes².

This can be attributed to a number of reasons:

- Huge margins for little effort and risk on the part of criminals
- Inadequate legislation or punishment to deter identity thieves
- Organisations not deploying appropriate security measures
- People not being aware of the value of their personal information

It had for a while been thought that the only victims of identity theft were individuals whose personal information has been obtained illegally. Evidence has however shown that organisations, which obtain and sell personal information, have fallen prey to sophisticated criminals.

For example:

- Customers of financial institutions have been tricked into handing their personal data through phishing scams³,
- Personal information brokers have had their systems breached by identity theft criminals. This can be illustrated with Choicepoint and Lexisnexis⁴ both of which have been hit by large scale identity theft of personal information stored on their databases
- Internal staff have colluded with criminals to illegally sell personal information, which is then used to purchase goods without the knowledge of the individual.
- The U.S. Attorney's Office has prosecuted approximately ten individuals for being involved in the use of financial institution computers to obtain customer information, and using that information to commit fraud. The prosecutions have included financial institution employees, and impostors who assumed the identity of account holders to commit bank fraud and fraud on the Internet. As part of each plea agreement, the financial institution employees agreed to be statutorily barred from employment at any federally insured financial institution for ten years following the date of conviction, pursuant to 12 U.S.C. § 1829(a). According to court documents, some convictions have included:
 - Kimberley Molette Smart, 27, of Sacramento, was sentenced on December 5, 2002, to serve one year and one day in prison, and given a three-year term of supervised release, in connection with using her

¹ Franklin F Akinsuyi is the Founding partner of DataLaws an information technology law consultancy based in the United Kingdom. He specialises in Information Technology Contract Negotiations, Information Security Law, Data Protection, Electronic Commerce and Identity Theft. He can be reached at fakinsuyi@datalaws.com

² See Combating Identity theft article by Franklin Akinsuyi available at www.datalaws.com/common/pdf/Combating%20Identity%20Theft.pdf

³ The act of sending an [e-mail](#) to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for [identity theft](#) see also www.webopedia.com/TERM/p/phishing.htm

⁴ See Security breach at LexisNexis now appears larger: Article by Heather Timmons and Tom Zeller JR NewYork Times April 13, 2005

financial institution position to obtain customer account information from the financial institution computer, and provide it to others who caused an intended loss of approximately \$121,146.63.

- Lynn Booker, 34, of Sacramento, a former credit union employee, pled guilty to committing a check "kite" through unauthorised computer access to customer account information from a financial institution. On January 21, 2003, Booker was sentenced to a five-year term of probation and ordered to pay restitution in the amount of \$25,510.97.⁵

In realising that personal information has value and that it can be used to obtain false documents which in turn can be used to commit criminal activity, data protection legislation has been enacted to identify the responsibilities of organisations that collect, transmit, store and process personal information. These legislations also have provisions, which provide for redress in the event that the organisation breaches data protection provisions in the handling of personal information.

What is Personal Data?

A good definition can be derived from the UK Data Protection Act⁶ which defines personal data as follows, "Data that relates to a living individual who can be identified from such data, or and other information which is in the possession of, or is likely to come into the possession of, the data controller⁷ and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual⁸."

What is data protection?

Data protection involves the implementation of administrative, technical or physical measures to guard against unauthorised access to such data.

It stems from legislative requirements such as the European Convention of Human Rights, and has with the advancement in automated processing of data been influenced by new legislations such as the European Data Protection Directive⁹ and the Directive on Privacy and Electronic Communications¹⁰.

It involves the protection of personal data, which covers both facts and opinions about an individual.

An instance of data protection legislation can be illustrated with the European Convention on Human rights, which provides for the right of respect to private and family life¹¹. It further provides that there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety

⁵ For more information see <http://www.usdoj.gov/criminal/cybercrime/thomasIndict.htm>

⁶ Data Protection Act 1998

⁷ A person who allow or jointly with others determines the purpose for which and manner in which personal data is to be processed

⁸ Section 1(1) Data Protection Act 1998

⁹ 95/46/EC

¹⁰ Directive 2002/58/E.C OJ L201/37

¹¹ Article 8 (1) European Convention On Human Rights

or the 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 freedoms of others¹².

This has implications relating to information about data of individuals in respect to how it is kept, processed and transmitted, this is so especially since misuse can lead to a breach of the aforementioned right.

Why do we need Data Protection?

Advances in technology has led to easier ways of carrying out daily routines, indeed, many activities which in the past required physical presence before a purchase could be made of a product, now only need the supply of personal details. While this is convenient, and has led to faster means of conducting business, it has also led to a rise in identity theft.

It is also to be noted that with the proliferation of business activity in relation to customer information, a number of organisations have sprung up which have identified the fact that information about a person can be of value to other organisations. This has led to a number of underhanded means of collecting personal information in what appear to be promotional information leaflets. Victims tend to fill these leaflets in only for this information to be collated and then sold to marketing companies. It is this type of activity that has led to the call and development of data protection laws leading to stiff penalties for organisations and individuals that breach them. Indeed, under the UK 1998 Data Protection Act it is an offence for a person, knowingly or recklessly, without the consent of the data controller, to obtain personal data¹³. To buttress this point further an individual named Alistair Fraser, trading as Solent Credit Control¹⁴, pleaded guilty to offences of unlawfully obtaining and selling personal information in breach of the Data Protection Act 1998. Mr Fraser had obtained the personal information of certain individuals by deception from the Department for Works and Pensions. He then sold the information to third parties. He was found guilty and fined. A feature of this case is the fact that it was brought to court by the Information Commissioner, thus showing that the Commissioner is prepared to use enforcement powers to combat and discover agencies that illegally obtain and sell personal information.

In the United States organisations that violate data protection legislations relating to privacy of information are severely punished. In the case between United States of America (for the Federal Trade Commission) v. Hershey Foods Corporation: Mrs. Fields Cookies and Hershey Foods Corporation each agreed to settle Federal Trade Commission charges that their Web sites violated the Children's Online Privacy Protection Act (COPPA) Rule by collecting personal information from children without first obtaining the proper parental consent. Mrs. Fields are to pay civil penalties of \$100,000 while Hershey will pay civil penalties of \$85,000. The separate settlements also bar the companies from violating the Rule in the future. The COPPA Rule applies to operators of commercial Web sites and online services directed to

¹² Article 8 (2)

¹³Section 55 (1&3) Data Protection Act 1998

¹⁴ See www.csa-uk.com/news-facts-press_index/newsletters/autumn202002.pdf page2

children under the age of 13 and to general audience Web sites and online services that knowingly collect personal information from children under 13. Amongst other things, the Rule requires that Web site operators obtain verifiable consent from a parent or guardian before they collect personal information from children¹⁵.

Data Protection and Financial institutions

With the introduction of online services, financial institutions have made it more convenient for customers to access their accounts. It is to be noted however that prior to online accounts being created, customers need to provide these institutions with their personal information such that they can process, transmit and store such information in the order to utilise the information to uniquely identify the customer. It has been well documented however that many financial institutions have had systems containing customer personal information breached from both internal; and external sources as illustrated above.

Data Protection and Telecommunications:

The telecommunications industry has seen a large uptake in subscription to the services that are being offered. Indeed this can be seen with the radical changes from the previously limited fixed line services in the earlier years to the introduction of the mobile telephone. The advent of the Internet along with the integration of voice, video, data and communications via a single stream¹⁶ has led to cheaper and faster ways of communicating. New services rendered by mobile phone companies have indeed led to the introduction of 3rd generation mobile phone networks, making it possible for subscribers to send pictures and video clips to each other using these services.

It is to be noted that while the technology is changing, attitudes and an understanding that personal data needs to be kept secure and confidential have not.

Technology makes it much easier to infringe on the rights of individuals especially when it comes to their personal data. Numerous organisations¹⁷ have identified this situation and have for years been championing the call for greater awareness to make sure that the individual's fundamental human rights are not infringed.

It is a well-known fact that convergence of these technologies makes it easier for marketing companies to process data to profile people. Like wise it is also possible for criminals to easily gather information about others in their quest to forge identities¹⁸ in their pursuit to commit crimes.

In recognition of the risks that can accrue to an individual, privacy laws have been enacted to act as a cushion to define what constitutes legal and illegal activity when it

¹⁵ See www.ftc.gov/opa/2003/02/hersheyfield.htm

¹⁶ Also called convergence

¹⁷ For example electronic privacy information centre www.epic.org and Electronic Frontier Foundation www.eff.org

¹⁸ See Internet fraud watch www.fraud.org and Internet fraud centre www1.ifccfbi.gov

comes to the protection of an individual's data when it is being transmitted over telecommunication streams.

The EU Directive on Privacy and Electronic Communications provides that communication service providers should adopt adequate security measures both from a technical and organisational point of view that are commensurate with the risks that can accrue. With the spate of recent high profile security breaches that have occurred it is paramount that telecommunications providers implement adequate logical and physical security measures to ensure data under their control is safe from unauthorised access, which may lead to loss of privacy. It goes further to provide that users should be made aware of risks that are beyond the control of the service provider¹⁹.

Data Protection Laws

National data protection laws have developed as electronic commerce has boomed. Indeed, with more coverage being given in the media relating to infringement of privacy, it is no wonder that countries have been more active in ensuring people know what their rights are in relation to these issues and also that data controllers ensure data under their custody is processed in line with data protection legislations. The European Union has developed a Framework for Data protection; this can be seen in the Data Protection Directive and the Directive on Privacy and Electronic Communications (2002/58/EC), which replaces the Telecommunications Data Protection Directive.

Data protection principles

Data protection laws provide protection of the individual with regards to their personal data, however the question is how does one ensure from the onset that personal data is collected, processed, transmitted and transferred legitimately? Data protection laws have basic principals that need to be adhered to. Indeed if one analyses for example the European Union Data Protection Directive one will notice that there are a number of principles that form the body of data protection laws worldwide.

These principals can be summarised as follows:

- Personal data shall be processed fairly and lawfully²⁰
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes²¹.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed²².
- Personal data shall be accurate and, where necessary, kept up to date²³.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes²⁴.

¹⁹ Article 4 (1&2) Directive on Privacy and Electronic Communications

²⁰ Article 6(1a) Data Protection Directive 95/46/EC

²¹ Article 6(1b)

²² Article 6(1c)

²³ Article 6(1d)

- Personal data shall be processed in accordance with the rights of data subjects under this Act²⁵.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data²⁶.

Alongside these worldwide principles, the European Union in an attempt to protect personal data processed within its environs has an additional principle relating to transfer of data to third party countries, which covers countries outside the European member states. This provision states that the transfer of data should not be carried out to such countries if they do not have similar data protection laws and measures such as the European Union²⁷.

As has been mentioned, The European Union has also adopted a new Directive on the processing of personal data in the electronic communications sector this Directive repeals and replaces the Telecoms Data Protection Directive. It also addresses various issues in relation to the services of electronic communication service providers and their retention of user data.

Data Protection in Europe

The European Directive also has significant implications for those that have made a business out of the sending of direct marketing e-mails where it states that they may only be sent where the subscriber has given their consent²⁸. The main aim of this Directive is to harmonise the provisions of Member States laws in relation to electronic communications to ensure an equivalent level of protection of fundamental rights and freedoms, particularly the right to privacy, processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the community.

It is to be noted that the Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the community.

The Directive in providing for subscriber protection has laid out a number of articles to which public communication service providers must adhere: An analysis of the salient points reveal the following in the Directives aims in ensuring the fundamental human rights and freedoms particularly the right to privacy for subscribers of electronic communications:

In its attempt to maintain privacy of personal information, the Directive requires service providers ensure confidentiality of communications. This the Directive states can be attained by making sure that communication over public telecommunications lines are free from interception and tapping save on the instance of lawful

²⁴ Article 6(1e)

²⁵ Article 12

²⁶ Article 17

²⁷ Articles 25 and 26

²⁸ Article 13 Directive on Privacy and Electronic Communications

interception²⁹. The article also provides that where communication networks are used in the processing of data, the data subject shall be informed why this is being carried out. The data subject has a right to refuse such processing³⁰.

Further privacy rules can be seen in relation to caller and connected line identification. Here the directive states that subscribers must be issued with the possibility of withholding the identification of their telephone numbers when making a call along with being able to reject incoming calls where the incoming caller has refused showing their number³¹.

Location data is a valuable tool that can be used to identify especially in the mobile phone sector where an individual is located³² its use can be illustrated where recently in the UK a case involving the hunt for a missing child in the UK identified that calls purportedly from the girls phone to her uncle (later convicted for her murder) were in fact being made by her uncle from one location³³.

The Directive in recognising the importance of location data provides that location data can be processed only if it is made anonymous or with the consent of the subscriber for a value added service but only for the duration that is necessary for the processing³⁴. The subscriber must also be given the possibility to temporarily refuse such processing of location data information³⁵.

An exception to the privacy of caller line and location data is provided for in article 10 where the elimination of calling line identification and location data is sanctioned to trace nuisance calls and in relation to location data for it to be revealed on a temporary basis only to emergency services.

In order to protect user data and information provided in directories, the directive instructs that where directory services are provided in printed or electronic form subscribers must be informed free of charge of the directories purpose³⁶, it further states that subscribers must be given the opportunity to ascertain the possibilities of use of further use of search functions based on the data about them in that directory.

The Directive in recognising the harmful effects of Spam this provides that there shall be no automated communication using electronic mail or faxes for the purpose of direct marketing without the consent of the data owner³⁷.

²⁹ Article 5 (1)

³⁰ Article 5 (2)

³¹ Article 8

³² See Location Data is as sensitive as content data Alberto Escuardo Pascual Royal Insitute of Technology

³³ See bbc.news.co.uk/2/low/technology/2593653.stm

³⁴ Article 9 Directive on Privacy and Electronic Communications

³⁵ Article 9(2)

³⁶ Article 12 (1)

³⁷ Article 13 Directive on Privacy and Electronic Communications

The Directive also enables for legislative restrictions of rights and obligations in relation to certain articles³⁸ where national security is at risk and where criminal investigations are being carried out. This legislation also allows for data to be retained for limited periods of time during the investigation of such situations³⁹.

Data Protection in the United States

In the United States Data Protection legislation does not stem from a central law as do the Data Protection Directives in Europe, rather one finds sectoral laws, which affect certain sectors and industries. As such due to this state of affairs it is to be noted that as advanced as the United States is on data protection issues, the European Union still regards its data protection regime as one that requires special provisions such as the Safe harbour rule when it comes to the transfer of data from EU member states to the United States.

Even though there is no general law on data protection the Supreme Court case of *Whelan v Roe*⁴⁰ illustrated the recognition of the right to privacy of information. It is to be stated at this point however that while it may seem that due to the sectoral nature of data protection legislation there does not appear to be a coherent data protection framework in the United States, this could not be further from the truth. Indeed what we find is a situation where the proliferation of privacy laws for various sectors leads to heavier regulation and tighter controls as is evidenced from the number of cases that have been brought to trial.

An example of such laws is seen with the following federal legislations which all have an element of data protection featured in them:

Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code 6501 et seq.

The aim of this Act is to place parents in control over what information is collected from their children online. With limited exceptions, the related FTC Rule requires operators of commercial websites and online services to provide notice and get parent's consent before collecting personal information from children under 13.

Fair Credit Reporting Act (FCRA) - 15 USC 1681-1681u

This federal law is designed to promote accuracy, fairness, and privacy of information in the files of every consumer reporting agency, the credit bureaus that gather and sell information about consumers to creditors, employers, landlords and other businesses.

Federal Identity Theft Assumption and Deterrence Act of 1998 - 18 USC 1028

The Act makes it a federal crime to use another's identity to commit an activity that violates Federal law or that is a felony under State or local law. Violations are investigated by federal agencies including the Secret Service, the FBI and the Postal Inspection Service and prosecuted by the U.S. Department of Justice.

Federal Privacy Act of 1974 - 5 U.S. Code 552a

³⁸ Notably articles 5,6 8 (1,2,3&4) and Article 9

³⁹ Article 15 (2) Directive on Privacy and Electronic Communications

⁴⁰ *Whelan v Roe* 429 US reports (February 1977) 589-604

This law applies to the records of federal government executive and regulatory agencies. It requires such agencies to apply basic fair information practices to records containing the personal information of most individuals.

Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule - 15 USC 6801-6827

The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies.

Health Information Portability and Accountability Act of 1996 (HIPAA)

This Act includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the security and confidentiality of patient information.

Video Privacy Protection Act of 1998 - 18 U.S.C. 2710

The Act strictly limits the conditions under which a video rental or sales outlet can disclose information about its clients. The Act also requires such an outlet to give its clients the opportunity to opt out of any sale of mailing lists, it also allows consumers to sue for money damages and attorney fees if they are harmed by a violation of the Act.

Personal Data Privacy and Security Act 2005

The aim of this Act is to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

In relation to data protection and telecommunication laws in the United States one can look to the Electronic Communication Privacy Act.

Data Protection in Nigeria

In Nigeria, Part 10 of the draft Computer Security and Critical Information Infrastructure Protection Bill 2005⁴¹ deals with identity theft while Part 11 deals with records retention and data protection.

Section 4 provides amongst other things that “Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act or pursuant to any regulation under this section, shall not be utilised except for legitimate purposes. Under this Act, utilisation of the data retained, processed or retrieved shall constitute legitimate purpose only with the consent of individuals to whom the data applies or if authorised by a court of competent jurisdiction or other lawful authority.”

This section raises a number of issues.

⁴¹ See www.cybercrime.gov.ng/site/index.php?option=com_content&task=view&id=20&Itemid=56

- The first being that part 11 is limited to personal data obtained from service providers only, as such it is restricted to communications service providers and not financial institutions or other industries
- Secondly, it is implying that in the event that an offence has been committed and needs to be investigated, the data subject will be required to give consent before it can be used, this amounts to saying that a suspect must give consent to data being used against him/her!
- Another lawful authority is too wide a scope and should be restricted otherwise it leads to room for abuse.

A brief comparison between Nigerian, European and US data protection legislations identifies a number of gaps in the Nigerian Bill. Notable of which are the following;

- No definition of what constitutes personal data;
- No identification of the right to privacy;
- No definition of what constitutes data subjects rights;
- No appointment of a regulatory body to redress breach (i.e. a Data Protection Commissioner);
- No identification of the fact that organisations can also breach data protection rules;
- No provision for circumstances where the personal data needs to be utilised without the consent of the data subject;
- No provision, definition, or mandatory requirement of technical measures to mitigate data protection breaches.

It is to be stated that in its current form the Bill does not adequately address Data Protection issues. For instance as we have seen in the United States and Europe, the legislations define what constitutes personal data, along with stating what the principles of data protection are. They also provide for adequate redress to persons that have had these principles breached. This is done through regulatory bodies that have appropriate power and are not afraid to use it.

In the United Kingdom, the Data Protection Commissioner has the right to fine and also stop organisations from processing personal information where they do not comply with the provisions of the data protection Act. In the United States the regulatory bodies also have the power to fine organisations that breach data protection legislation.

With these findings in mind, it is my recommendation that a stand-alone Data Protection legislation, which identifies the responsibilities of organisations, individuals and government in relation to obligations towards data protection, be written.

To Conclude,

With the consolidation of the Nigerian banking sector, it is necessary that customers personal data is kept confidential and private, the growing subscription of customers to online services offered both by the financial and telecommunications companies in Nigeria is all the more reason why now is as good a time as any for data protection legislation to be revisited and rewritten to international standards

In today's global economy more countries are waking up to the effects of identity theft and the need for organisations to protect customers personal information and as such are enacting effective legislation to deal with identity theft and the safeguarding of personal information.

We have seen the rise in outsourcing functions to Asian countries, which have recently enacted data protection legislation.

Not enacting appropriate legislation to cater for data protection and identity theft will not allow us to be in a position to partake in lucrative outsourcing deals which not only brings job opportunities but also the kudos that our legislative and technical services are up to scratch with the rest of the world. As long as Nigeria does not have adequate data protection legislation, it will be looked upon as country that does not take identity theft or Data Protection seriously and as such be excluded from these lucrative outsourcing opportunities

It is to be noted that the Eighth Data Protection principle provides that personal data shall not be transferred to a country outside of the European Economic Area if that country does not have adequate levels of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

To buttress the point further, in a recent article published in the Independent⁴², three African countries have been identified for outsourcing, these being Egypt, South Africa and Ghana. (Nigeria is notably missing)

Going forward, in order to appear on the radar as a country that understands the need for data protection, data protection awareness programs which highlight the importance and value of personal information must be devised, implemented and made available to Nigerian citizens.

A major disadvantage of not implementing the legislation is the fact that many Nigerians who legitimately wish to purchase goods online are barred from doing so due to credit card companies blacklisting Nigerian IP addresses. This can be attributed to a lack of evidence that appropriate technical and legislative measures are available to protect personal data.

It is also advisable that the current Computer Security and Critical Information Infrastructure Protection Bill is totally reworked to consist of separate legislations comprising of the following:

⁴² A UK based daily newspaper, see also www.independent.co.uk/

- Data Protection Legislation
- Computer Misuse Legislation
- Information Security Legislation
- Lawful Interception

These will then form the Nigerian Cyber Crime Legislative Framework to which we can be recognised as having appropriate legislature to combat computer related crime and Identity theft.

As a final note, when such legislation is being drafted, it is imperative that appropriately qualified individuals who have experience in this area are called upon to give their input.

Copyright 2007