Journal of Asian and African Social Science and Humanities, Vol. 1, No. 1, 2015, Pages 8-26

AN APPRAISAL OF THE INSTITUTIONAL FRAMEWORK FOR DATA PROTECTION IN THE UK, USA, CANADA AND NIGERIA

Bernard Oluwafemi Jemilohun[1]

1. *Ekiti State University, Department of Private Law, Faculty of Law, P.M.B 5363.Ado-Ekiti. Nigeria*

Keywords:
Data protection, supervisory agency, personal information, privacy

ABSTRACT

The protection of personal privacy on the internet is a contemporary issue and several nations have made legislation to secure same. With the need for regulation arises the need for better institutions to protect the same since it has become obvious that traditional law enforcement agencies like the police may not be best to handle such technology based matters. The paper observes that data protection agencies have become a common feature in democracies though agency powers vary from country to country. This paper looks at the institutional framework for data protection in Europe, the United Kingdom, the United States of America and Canada and by comparison appraises some institutions in Nigeria that have some data protection functionality either by the nature of their duties or the laws creating them. The paper by comparison concludes that Nigeria does not yet have a data protection agency compared to the European standard even as the legal framework is not fully developed and thus there is the need for a strong institutional approach to the issue.

To Cite This Article: Jemilohun, B. O. An Appraisal of the Institutional Framework for Data Protection in the UK, USA, Canada And Nigeria. Journal of Asian and African Social Science and Humanities, 1(1): 8-26, 2015

Journal of Asian and African Social Science and Humanities, Vol.1, No. 1, 2015, Pages 8-26

INTRODUCTION

Sequel to legislations and regulations governing new, emerging and serious issues like data protection, governments have continually found out that the traditional law enforcement system like the police may not be the appropriate body to be saddled with such a technologically-driven issue as data protection in an online environment. Thus, new institutions have been created to give effect to the new legislations and enforce the laws and provide appropriate remedies where possible. Data protection agencies have become a common feature in democracies though agency powers are often specific to each country[1]. Some countries established regulatory enforcement agencies and licensing boards, while others adopted an ombudsman position.

The rationale for this is that people conceived of data protection as a unique political right in need of state protection especially in the European block and thus for effective protection requires new institutions to oversee. This paper attempts to discuss the institutional framework for data protection in Nigeria and some selected countries like the United Kingdom, the United States, Canada and India.

EUROPE GENERALLY

The established practice of creating a dedicated supervisory agency for data protection has become a somewhat defining element of the European approach towards the protection of informational privacy. Though this was not initially a requirement of the Council of Europe Convention, the Data Protection Directive mandates each member state to create an independent supervisory agency to monitor the application of data protection laws and to investigate violations.[2] The Council of Europe Convention merely required signatories to 'designate one or more authorities who will, at the request of another designated authority, furnish information on national laws and administrative practices, provide factual information related to specified automated files, and undertake any investigations related to the request in conformity with national legal provisions'. It seems the intention of this provision was that the agencies should be concerned solely with transborder data flow issues.[3] However, as legislative patterns manifested, it became almost universally acceptable within Europe that specialised data protection agencies should be established. The specific authority so appointed is not saddled with the responsibility of seeing to the compliance of the directive but the national law for data protection.

The Data Protection Directive specifies in Recital 62 that the establishment of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of

[1] Reidenberg, Joel R, *Resolving Conflicting International Data Privacy Rules in Cyberspace* 52, Stanford Law Review 1315
[2] Article 28 of the Directive
[3] Lloyd, Ian J. (2011) *Information Technology Law*, Oxford University Press, 6th Ed.

personal data and provides that: "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them"[4]. Except for Germany, all the European Union states have established single agencies. Germany, probably due to the federal nature of its constitution, has about 20 supervisory agencies working in the area of data protection.

The Treaty of Amsterdam, which made significant changes to the treaties establishing the European Union, provided that an independent supervisory agency was to be established in respect of the data processing activities of the European institutions. It was based on this that Regulation 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the free Movement of such Data' was adopted, entering into force at the end of January 2001. The Regulation provided for the appointment of a European Data Protection Supervisor[5] and contains other provisions which are similar and equivalent in scope to those contained in the Data Protection and Electronic Communications Privacy Directives which applies to processing carried out by the European institutions. After two years, Decision 2004/55 announced the appointment of Peter Hustinx as the first supervisor for a five-year term of office. His appointment was continued for a second term in 2009.[6]

Though the language of the Directive is clear on the need for a supervisory agency[7], one of the key issues that may concern lawmakers is the form that this agency should take. Should it be the appointment of a single regulator (though supported by what maybe a substantial staff strength) or vesting the authority in a multi-membered commission or authority. The relative merits of single or multiple regulators cannot be overlooked. Lloyd[8] is of the opinion that a single regulator may be able to bring a more focused and consistent approach to regulation, although much will obviously depend upon the personality and abilities of the post holder. With a collegiate body, there is more likelihood of internal dissent, but it is also possible that a wider range of interests and expertise may be represented with the consequence that decisions reached carry greater weight.

Alongside the requirement that member states establish independent supervisory agencies, with complete independence in exercising the

[4] Article 28
[5] Article 1
[6] http://ec.europa.eu/justice/policies/privacy/eusupervisor/index_en.htm
[7] Article 28 (1)
[8] Lloyd Ian J. s*upra* note 3 above

functions entrusted to them, the Data Protection Directive also prescribes the basic powers to be vested in these agencies. The powers are as follows:

(a) Investigative powers: These are powers of access to the data forming the subject matter of the processing operations and also powers to collect all the information necessary for the performance of its supervisory duties;

(b) Effective powers of intervention: These are powers such as for delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure, or destruction of data; powers of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions. (This is the power presently in exercise by the data protection authorities of France, the UK, Germany, Spain, Italy and the Netherlands over Google's alleged refusal or failure to fall in line with data protection rules. The six authorities will take enforcement action under their national laws which are all based on European data protection rules. The EU is working on a revision of the rules that would allow one data-protection authority to take action instead of multiple cases. In this instant case of Google, that would be in Ireland, which is where the company has its European headquarters.)[9]

(c) Power to institute legal action: This is where the provisions of the national laws adopted in pursuance of the Directive have been violated or to bring those violations to the attention of the judicial authorities.[10]

It is further provided by the Directive that "each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedom in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim".[11] It is only the courts that have power to entertain appeals from the decisions of the supervisory agencies.

At the national level, the designation varies from country to country thus we have them as follows:

UK – Information Commissioner's Office;
Hungary – Data Protection Ombudsman;
Austria – Austrian Data Protection Commission;
Belgium – Commission for the Protection of Privacy;
Finland – The Data Protection Ombudsman;

THE UNITED KINGDOM

[9] "Data-Protection Agencies Target Google" *European Voice.com* 3rd April, 2013. Available at http://www.europeanvoice.com/article/2013/april/data-protection-agencies-target-google-/76846.aspx
[10] Article 28 (3)
[11] Article 28 (4)

Following the recommendation of the Data Protection Directive, the Data Protection Act, 1998 places the duty of supervising and ensuring compliance with the Act on the office of the Information Commissioner[12]. The Information Commissioner's Office is the sole authority that is empowered to oversee the operation of the UK Data Protection Act. Presently, in the United Kingdom, the Information Commissioner's Office is responsible for the administration of both the Data Protection Act and the Freedom of Information Act[13]. In summary, the Information Commissioner is the United Kingdom's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.[14] It rules on eligible complaints, gives guidance to individuals and organizations and takes appropriate actions when the law is broken.

The Data Protection Act stipulates the terms and conditions under which the Commissioner is appointed.[15] The Commissioner is normally appointed for a fixed term of five years,[16] renewable for another five years. Within the period of his tenure, he may be removed from office by the Crown at his own request[17] or in pursuance of an Address from both Houses of Parliament.[18] The Act further provides that the Commissioner and his officers and staff are not to be regarded as servants or agents of the Crown.[19] The Information Commissioner's Office in the United Kingdom is a substantial one. Apart from the Commissioner himself, three separate offices headed by an Assistant Commissioner have been created for Scotland, Wales and Northern Ireland and as at 2011, some 262 staff are employed.[20]

By the provisions of the Data Protection Act, 1998, every data controller who processes personal data in the United Kingdom is required to inform the Information Commissioner's Office so that their processing of personal data may be registered and made public[21]. The Act expressly prohibits the processing of personal data without registration. In order to register, the data controller shall give a notification accompanied by the

[12] This office was created as the Data Protection Registrar under the 1984 Data Protection Act. When the 1998 Act came into operation, it was change to Data Protection Commissioner. Schedule 5, para. 1. It was the enactment of the Freedom of Information Act and the placing of the supervision of the Act under the office that necessitated the change of name to Information Commissioner.
[13] Section 18 of the Freedom of Information Act, 2000
[14] About the ICO available at http://www.ico.org.uk/about_us
[15] Schedule 5
[16] Schedule 5 para 2 (1)
[17] Schedule 5 para 2 (2)
[18] Schedule 5 para 2 (3)
[19] Para 1 (2)
[20] Lloyd, Ian J. *Information technology Law*
[21] Section 19 (1). Further, Section 17 (1) of the Act expressly prohibits the processing of data by any controller except an entry about the controller has been made in the register maintained by the Commissioner.

registrable particulars[22] and a general description of measures to be taken for the purpose of complying with the seventh data protection principle which deals with appropriate security measures to be put in place to secure data. Section 19 (7) provides that the Commissioner shall on the payment of a prescribed fee, supply any member of the public with a duly certified copy in writing of particulars contained in any entry on the register. This provision gives the public direct access[23] to the list of data controllers in the United Kingdom and thus no organization or company may process data secretly except such organization is exempt by the provisions of the Act. Presently there are over 370,000[24] data controllers in the United Kingdom and it is the job of the Information Commissioner's Office to ensure that each of them complies with the provisions of the appropriate legislation by remaining within the scope of their entries on the Register and that in general, processing complies with the substantive requirements of the Act.

POWERS OF THE INFORMATION COMMISSIONER

The Information Commissioner's Office has tremendous powers in the United Kingdom. The Commissioner is empowered to serve an information notice, requiring the supply within a fixed period of time of specific information relating to the matter under investigation.[25] An appeal against such a service of an information notice will lie to the Data Protection Tribunal which has the power to suspend the operation of the notice.[26] However, failure to comply with an information notice is an offence as well as reckless or intentional provision of false information in response to the information notice.[27] The service of an information notice may be on the Commissioner's own initiative or following a complaint from a data subject since the Act provides that anyone may contact the Commissioner to seek an assessment whether it is likely that personal data has been or is being processed lawfully.[28]

A second power that the Information commissioner has is the power of entry and inspection. Under the Data Protection Act, the Commissioner can approach a circuit judge seeking a warrant to enter and search any premises. Where the judge is satisfied that the data controller is in breach of any of the principle or has committed an offence under the Act, the warrant will be granted. The warrant will empower the Commissioner or his staff to "inspect, examine, operate and test any equipment found there which is intended to be used for the processing of

[22] Section 18 (2)
[23] The register is available on the Internet.
[24] Register of Data Controllers available at http://www.ico.org.uk/what_we_cover/register_of_data_controllers
[25] Section 43 (1)
[26] Section 43 (4) – (5)
[27] Section 47
[28] Section 42 (1)

personal data and to inspect or seize any document or other material found there."[29]

A third power of the Commissioner is the power to serve enforcement notice[30] on a data controller where the commissioner is satisfied that a breach of one or more of the data protection principles has occurred. This notice serves to identify the act or omission complained of and specifies the steps to be taken to put things right. Failure to comply with an enforcement notice is an offence.[31] Again, similar to the information notice, the data controller may appeal to the Data Protection Tribunal and this will serve to suspend the operation of the notice.

Another power that the Commissioner has is the power (with the consent of the data controller) to assess any processing 'for the following of good practice and shall inform the data controller of the results of the assessment.'[32] Lloyd is of the opinion that such action may provide the data controller with the reassurance concerning the legality of current or proposed processing, thereby minimizing the possibility that more formal enforcement measures such as service of an enforcement or information notice will be taken at some stage in the future.

Beyond the foregoing, the Commissioner is to disseminate information giving guidance about good practice under the Data protection Act, 1998[33]. Good practice is defined as "such practice in the processing of personal data as appears to the Commissioner to be desirable having regards to the interests of data subjects and others and includes (but is not limited to) compliance with the requirements of this Act"[34]

The Information Commissioner remains the United Kingdom agency responsible for liaison with other data protection agencies within the ambit of the Council of Europe Convention. He is also responsible for working with the various Committees and Working Parties established at the European Union level by the Data Protection Directive. Part of the roles of such bodies is to determine whether third countries provide adequate level of protection for personal data. It is the duty of the Commissioner to disseminate information about such findings and seek to implement them within the United Kingdom. More so, the Data Protection Directive also contains provision that require national supervisory agencies cooperating with each other.

Above the Information Commissioner is the Information Tribunal which has appellate powers over the operations of the Information

[29] Schedule 9 para 1 (3)
[30] Section 40
[31] Section 47
[32] Section 51 (7)
[33] Section 51 (1)
[34] Section 51 (9)

Commissioner. This tribunal was created under the Data Protection Act, 1984 and it consists of a chairman and a number of Deputy Chairmen who are barristers, advocates or solicitors of at least seven years standing. Under the 1984 Act, the sole function of the Tribunal is to hear appeal brought by data users against the decisions of the Registrar that were adverse to their interests. Under the 1998 Act, a data subject can bring a case directly before the tribunal. The Tribunal's decisions may be appealed against on point of law to the High Court.

THE UNITED STATES OF AMERICA

When the Privacy Act was enacted in the United States, the law originally proposed the creation of a privacy protection commission; however, then president, Gerald Ford was opposed to such a bureaucracy. He wrote "I do not favour establishing a separate Commission or Board bureaucracy empowered to define privacy in its own terms and to second-guess citizens and agencies. I vastly prefer an approach which makes Federal agencies fully and publicly accountable for legally-mandated privacy protections and which gives the individual adequate legal remedies to enforce what he deems to be his own best privacy interests".[35] As a compromise, central oversight was assigned to the Office of Management and Budget, and OMB has exercised relatively weak leadership in the implementation of the Privacy Act. The law also calls for the designation of Privacy Act officers within federal executive agencies to handle requests and insure compliance with the code of practice. Ultimately enforcement rests with the courts (as individuals bring suit to redress perceived grievances).[36] Schwartz has argued that the lack of a United States federal data protection agency and the paucity of comprehensive data protection legislation covering the United States private sector make a case for the perception by European nations that their legal regime is better.[37] He points out that a more general governmental body is needed to assist the public, social groups and the legislature in understanding strengths and weaknesses in the boundaries of existing information territories.[38]

Presently, the only authority that one may say is partially responsible for the protection of personal information and the prevention of data abuse in the United States is the Federal Trade Commission. The

[35] U.S. Congress. House. Committee on House Administration. Legislative History of the Privacy Act of 1974, S.3418 (Public Law 93-579): Source Book on Privacy. 94th Congress, 2nd Session, 1976, Joint Committee
Print (Y4.G74/6:L52/3).

[36] Jean Slemmons Stratford & Juri Stratford 'Data Protection and Privacy in the United States and Europe' available at http://www.iassistdata.org/downloads/iqvol223stratford.pdf accessed on 22nd May 2013

[37] See generally, Schwartz, P. M. and Reidenberg, J. R., (1996) *Data Privacy Law: A Study of United States Data Protection*, Michie Law Publishers, p. 5; Anderson, D. A. (1999) *The Failure of American Privacy Law*, in Markesisnis, B. S. (ed) Protecting Privacy, Oxford University Press, p. 139-167

[38] Schwartz, Paul M., "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* Vol 52 p 1609. Available online at http://www.paulschwartz.net/pdf/VAND-SCHWARTZ.pdf

FTC was established under the Federal Trade Commission Act of 1914. It is an independent agency of the United States government whose principal mission is the promotion of consumer protection and the elimination of anti-competitive business practices[39]. The mission of the FTC as stated on the official website is "to prevent business practices that are anti-competitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity."[40]

By the European standard, this body does not qualify for a data protection agency, though the Federal Trade Commission has made some important contributions to monitoring developments in the use of information in cyberspace.[41] In some case, where permitted, the agency has also taken some enforcement actions and further developed the existing law but the Federal Trade Commission has a specific mandate in hindering 'unfair and deceptive trade practices.'

Broadly, the Federal Trade Commission has three distinct bureaus[42] in its administrative operations. They are:

1. The Bureau of Competition – This is the FTC's antitrust arm, and it seeks to prevent anticompetitive mergers and other anti-competitive business practices in the marketplace. By protecting competition, the Bureau promotes consumers' freedom to choose goods and services in an open marketplace at a price and quality that fit their needs - and fosters opportunity for businesses by ensuring a level playing field among competitors.
2. The Bureau of Economics – This bureau helps the FTC evaluate the economic impact of its actions. To do so, the Bureau provides economic analysis and support to antitrust and consumer protection investigations and rulemakings. It also analyzes the impact of government regulation on competition and consumers and provides Congress, the Executive Branch and the public with economic analysis of market processes as they relate to antitrust, consumer protection, and regulation.
3. The Bureau of Consumer Protection – This bureau's mandate is to protect consumers against unfair, deceptive or fraudulent

[39] About the Federal trade Commission - http://ftc.gov/ftc/about.shtm accessed on 24th May 2013
[40] http://ftc.gov/ftc/about.shtm accessed on 24th May 2013
[41] The Federal Trade Commission took action against Geocities alleged deceptive practices on the ground of Geocities misrepresentation of a limited use of the data it collected. Despite its promise, Geocities engaged in unrestricted utilization of personal data without an individual's knowledge or consent, and then it also allowed third parties on its website to maintain and utilize personal data collected from children despite its promises otherwise. See Geocities, File No9823015 (Federal Trade Commission, 1998) agreement containing consent order.
[42] Official website http://ftc.gov/ftc/about.shtm accessed on 24th May 2013

practices. The Bureau enforces a variety of consumer protection laws enacted by Congress, as well as trade regulation rules issued by the Commission. Its actions include individual company and industry-wide investigations, administrative and federal court litigation, rulemaking proceedings, consumer and business education. In addition, the Bureau contributes to the Commission's on-going efforts to inform Congress and other government entities of the impact that proposed actions could have on consumers.

Of the three bureaus, it is the Bureau of Consumer Protection that as the name implies, has been involved in offering some measure of protection to data subjects.

CANADA

Canadian data protection laws are enacted by both the central government and the provinces. Thus each data protection regime has its own enforcement and compliance officer. The Privacy Commissioner[43] of Canada is the chief compliance and enforcement officer over data protection issues in Canada. He is an independent officer of parliament who reports directly to the Senate and the House of Commons and also has jurisdiction with respect to public sector privacy regulation. By design, the Commissioner is an ombudsman who has some powers as will be examined shortly. The office of the Privacy Commissioner is divided into eight operational branches[44] namely:

i. *The Privacy Act Investigations branch* which receives and investigates complaints from individuals who claim a breach of the *Privacy Act* (PA) or complaints that are initiated by the Commissioner. The Branch also receives notifications of breaches from federal government organizations, receives and reviews public interest disclosures made by them;

ii. *The PIPEDA Investigations branch* which investigates complaints under the Personal Information Protection and Electronic Documents Act (PIPEDA). It is divided between Ottawa and Toronto. In Ottawa, the Branch receives and investigates all complaints of national scope filed by individuals or initiated by the Commissioner, from anywhere in Canada except from the Greater Toronto Area (GTA). In Toronto, the Branch investigates complaints from the Greater Toronto Area and coordinates public education and stakeholder outreach activities in the area;

iii. *The Audit and Review branch*: This branch audits organizations to assess their compliance with the requirements set out in the two federal privacy laws[45]. The Branch also analyses and

[43] He is appointed under the provisions of Section 53 of the Privacy Act, 1980

[44] Office of the Privacy Commissioner of Canada – Organizational Structure available at http://www.priv.gc.ca/au-ans/au_org_e.asp accessed on 23rd May 2013

[45] The Privacy Act and the Personal Information Protection and Electronic Documents Act

provides recommendations on privacy impact assessment reports (PIAs) submitted to the Office of the Privacy Commissioner of Canada (OPC) pursuant to the Treasury Board Secretariat Policy on PIAs;

iv. *The Communications branch*: This branch focuses on providing strategic advice and support for communications and public education activities for the Office of the Privacy Commissioner. In addition, the branch plans and implements a variety of public education and communications activities through media monitoring and analysis, public opinion polling, media relations, publications, special events, outreach activities and the OPC web sites. The branch is also responsible for the OPC's Information Centre, which responds to requests for information from the public and organizations regarding privacy rights and responsibilities

v. *The Legal Service, Policy and Research branch* provides strategic legal and policy advice and conducts research on emerging privacy issues in Canada and internationally. More specifically, the branch provides strategic legal advice to the commissioners and various branch heads on the interpretation and application of the *Privacy Act* and PIPEDA in investigations and audits, as well as general legal counsel on a broad range of corporate and communication matters. The branch represents the OPC in litigation matters before the courts and in negotiations with other parties both nationally and internationally.

vi. *The Technology Analysis branch* identifies and analyzes technological trends and developments in electronic platforms and digital media. The Branch conducts research to assess the impact of technology on the protection of personal information in the digital world. It also provides strategic analysis and guidance on complex, varied and sensitive technological issues involving breaches in the security of government and commercial systems that store personal information. As a corporate centre of expertise, the Branch analyzes current and emerging issues and trends in national security and public safety. The technological expertise concentrated in the Branch also supports core functions of the OPC, including audits, investigations and Privacy Impact Assessment reviews;

vii. *The Human Resources Management branch* is responsible for the provision of strategic advice, management and delivery of comprehensive human resource management programs in areas such as staffing, classification, staff relations, human resource planning, learning and development, employment equity, official languages and compensation; and

viii. *The Corporate Services branch* which provides advice and integrated administrative services such as corporate planning, resource management, financial management, information

management/technology and general administration to managers and staff.

POWERS OF THE PRIVACY COMMISSIONER

Unlike the United Kingdom, there is no provision in either the Privacy Act, 1980 or the Personal Information Protection and Electronic Documents Act requiring any organization involved in data processing to notify the Privacy Commissioner or register in any form. But the Act provides[46] that every organization shall comply with the obligations set out in schedule 1 of the Act which deal with the principles set out in the National Standard of Canada covering data protection principles.

Where a party is aggrieved that an organization has contravened a provision of Division 1 of the Act or for not following a recommendation set out in Schedule 1 (governing protection of personal information or the data protection principles), such a person may file a written complaint against the concerned organization with the Commissioner.[47] Where the Commissioner is satisfied that there are reasonable grounds to investigate a matter, he may initiate a complaint in respect of the matter.[48]

The powers of the Commissioner under the Canadian enactment are much similar to the stipulations of the European Union Data Protection Directive mandating European nations to cloth the office of the supervisory agencies with sufficient power to execute their offices. In the conduct of an investigation of a complaint, the first power of the Commissioner is the power to summon and enforce the appearance of persons before him and compel them to give oral or written evidence on oath and to produce any records or things that the Commissioner consider necessary to investigate the complaint in the same manner and to the same extent as if he were a superior court of record.[49]

Secondly, the Commissioner can, at any reasonable time enter into any premises (apart from a dwelling house) occupied by an organization on satisfying security requirements of the organization relating to the premises and converse in private[50] with any person in those premises and otherwise carry out in the premises any inquiries that the Commissioner sees fit. The Commissioner can also examine or obtain copies of or extracts from records found in those premises that contain any matter relevant to the investigation.[51]

[46] Section 5 (1)
[47] Section 11 (1)
[48] Section 11 (2)
[49] Section 12.1 (1) (a)
[50] Section 12.1 (1) (e)
[51] Section 12.1 (1) (f)

Thirdly, the Commissioner has power to discontinue[52] the investigation of a complaint if he is of the opinion that there is insufficient evidence to pursue the investigation,[53] or the complaint is trivial, frivolous, vexatious or made in bad faith,[54] or that the organization has provided a fair and reasonable response to the complaint,[55] or the matter is the subject of an investigation[56] or part of a report, or the matter has been otherwise addressed.[57]

Fourthly, the Commissioner has power to audit the personal information management practices of an organization if he has reasonable grounds to believe that the organization is contravening a provision of Division 1 of the Act or is not following a recommendation set out in Schedule 1. In doing this he may exercise any of the powers discussed above. And an ancillary power to this is the that the Commissioner has power to publicly report on the personal information handling practices of public and private sector organizations.

The Privacy Commissioner of Canada unlike her European counterparts does not have power to issue notices or impose fines and other stiff penalties on erring organizations that violate the provisions of the Act. All manners of penalties can only be imposed by the courts. The immediate past Privacy Commissioner for Canada, Jennifer Stoddart, pushed for more powers for the office while she was there. In May 2012, she appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics to call for greater enforcement powers for the agency.[58] It seems evident that other countries are moving towards more robust enforcement regimes. She suggested that if there were stricter penalties for companies that would affect their bottom lines; they would be more inclined to adhere to the privacy laws. In her words, "This is the age of big data where personal information is the currency that Canadians and others around the world freely give away. I have become very concerned about the apparent disregard that some of these social media companies have shown for Canadian privacy laws... I believe companies take notice when they are subject to major fines or some kind of enforcement action. We have very limited power in that regard, and I believe more respect would be shown to Canada's laws if we did have that power."[59] In her

[52] Section 12.2 (1). This is similar to the constitutional power of an attorney-general to discontinue criminal proceedings)
[53] Section 12.2 (1) (a)
[54] Section 12.2 (1) (b)
[55] Section 12.2 (1) (c)
[56] Section 12.2 (1) (d)
[57] Section 12.2 (1) (g)
[58] Privacy Commissioner looks for stronger enforcement powers, ability to levy fines – available at http://blog.privacylawyer.ca/2012/05/privacy-commissioner-looks-for-stronger.html
[59] Social media websites ignoring privacy laws, watchdog says – CBC News available at http://www.cbc.ca/news/politics/story/2012/05/29/pol-social-media-privacy.html accessed on 23rd May, 2013

view, the Personal Information Protection and Electronics Document Act is too weak to bring desired effects compared to the laws of other nations.

In the light of the federal nature of the Canadian lawmaking system and the fact that the various provinces equally have laws protecting personal information, Section 23 (1) of the Act authorises the Commissioner where it is considered appropriate, in order to ensure that personal information is protected in a manner as possible, to consult with any person who under provincial legislation, has functions and duties similar to those of the Commissioner with respect to the protection of such information. Agreements or arrangements may be entered into with such person to coordinate the activities of their offices and provide mechanisms for the handling of any complaint in which they are mutually interested, or to jointly undertake and publish research or develop guidelines related to the protection of personal information. The foregoing is to ensure much harmonisation in the operations of the privacy commissioners of the provinces as well as the federal privacy commissioner.

Similar to the above mandate, the Act further authorises the Privacy Commissioner to share information that are relevant with any person or body from a foreign state whose functions and duties are similar to those of the Commissioner with respect to personal information[60]. This provision seems to conform to the requirement of the European Union Data Protection Directive[61] wherein data protection agencies of member states were required to cooperate with each other in their duty of protection personal data.

THE NIGERIAN POSITION

There is no doubt that beyond the enactment of data protection legislation for Nigeria, the country will definitely need an appropriate institution to oversee personal information management in Nigeria with the sole aim of being the watch dog of the people's rights. Nigeria is not as developed as the American society where people can be expected to ensure that their personal information is not abused. This is one more reason why the NITDA Draft Guidelines may not be sufficient as a data protection instrument. As developed as the United States is, there have been arguments (as pointed out earlier) that the absence of a data protection authority similar to the European model is not good enough. A developing economy like Nigeria needs to invest in very strong institutions to ensure that the expectations of the law especially in new areas like this are met.

[60] Section 23.1 (1) This provision is appropriately titled "Disclosure of information to foreign state

[61] Article 28 (6) Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

In the present, the available institutions that seem to offer some protection for personal data are:

The National Identity Management Commission

Nigeria as a country has a long history of creating institutions[62] for managing virtually every aspects of governance. There is already a National Identity Management Commission which is responsible for the issuance of the national identity card and as such has a large volume of the personal data of Nigerians in its custody. But this body is not a data protection agency as the law[63] creating it does not vest it with such authority. Much as it is expected to preserve the integrity of the personal data in its custody, it does not have the power to regulate other institutions. The thrust of its mandate is to:

1. be the primary legal, regulatory and institutional mechanism for implementing Government's reform initiative (in the identity sector) as contained in the National Policy and National Identity Management Commission Act[64],
2. wind up and take over the assets and liabilities of the former DNCR which no longer exists, including the personnel in both the State and Local Government offices nationwide
3. establish, operate and manage the National Identity Management System (NIMS):
   a. carry out the enrolment of citizens and legal residents as provided for in the Act;
   b. create and operate a National Identity Database;
   c. issue Unique National Identification Numbers to qualified citizens and legal residents;
   d. issue a National Identity Smart Card to every registered person 16 years and above;
   e. provide a secure means to access the National Identity Database so that an individual can irrefutably assert his/her identity [Person Identification Verification Services (PIVS) Infrastructure];
   f. harmonize and integrate Identity Databases in Government Agencies to achieve resource optimization through shared services platform;
   g. collaborate with private sector and/or public sector institutions to deliver on the NIMS; and
   h. register births and deaths through specific collaboration with the National Population Commission.
4. foster the orderly development of an identity sector in Nigeria.

[62] We have the Nigeria Telecommunications Commission, Corporate Affairs Commission, Nigeria National Petroleum Commission, Police Affairs Commission, Judicial Service Commission, Civil Service Commission,

[63] The National Identity Management Commission Act, 2007

[64] Sections 1, 2, 5 & 6

None of the foregoing has to do solely with data protection in the sense of supervising other agencies and ensuring that they comply with the provisions of the law in the course of processing the personal data of Nigerians. It seems the NIMC was created largely to continue the work (howbeit in a modified sense) of the defunct Department of National Civic Registration. According to the Act, the Commission shall have the power to:

a) request for any information on data from any person on matters relating to its functions under this Act;
b) fix the terms and conditions of service including remuneration of the employees of the Commission;
c) establish and operate administrative and monitoring offices in the States, Local Government Areas and Area Councils;
d) monitor any matter that may affect the functions of the Commission; and
e) do such other things which this Act or any other enactment are required or permitted to be done by the Commission.

As stated above, none of these is data protection supervision. The Commission is only concerned with managing an identity database. Thus, in accordance with standard practice, a proper data protection authority for Nigeria, when established, should also have oversight of the data use practices of this Commission.

The Nigerian Communications Commission

The Nigerian Communications Commission is the independent National Regulatory Authority for the telecommunications industry in Nigeria. Unlike the National Identity management Commission, the NCC does not retain data of individuals as it does not deal directly with personal data. The Commission is responsible for creating an enabling environment for competition among operators in the industry as well as ensuring the provision of qualitative and efficient telecommunications services throughout the country.[65] The Commission was created under the Nigerian Communications Act, 2003[66] primarily to regulate the telecommunications sector. However, part of the functions of the Commission as provided under the Act is "the protection and promotion of the interests of consumers against unfair practices including but not limited to matters relating to tariffs and charges for and the availability and quality of communications services, equipment and facilities;"[67]

It seems part of the assignment of the Commission from the foregoing provision is to ensure that the consumers interests are protected against unfair practices generally and one may say this should extend to the

[65] www.ncc.gov.ng
[66] Section 3 (1) of the Act provides that "There is established a commission to be known as the Nigerian Communications Commission with responsibility for the regulation of the communications sector in Nigeria."
[67] Section 4 (1) of the Act

protection of the personal data of telecommunication services subscribers. Though the express language of the Act does not mention data protection or personal information protection, one is of the opinion that pending the enactment of proper data protection laws and the establishment of a data protection agency or authority, part of the functions of the Nigerian Communications Commission should be the oversight of how telecommunication companies use the personal data of Nigerian subscribers. Presently, no Nigerian has a right of access under any law to the personal data collected by telecommunication companies during the last SIM card registration exercise. Whether the data collected is accurate or not, whether they would be used for other purposes than the intended purpose or not is not for any subject to contest. This writer visited the website of a telecommunications company to check the record of his personal information only to discover that his name was wrongly spelt and there is no means of correcting such errors.

One feels the provision of Section 4 (1) of the Act should be sufficient legislative authority for the NCC to oversee the data-use practices of the telecommunication companies and ensure that Nigerian subscribers have such measure of protection from the abuse of their private information.

The National Information Technology Development Agency

The National Information Technology Development Agency was originally established as a government agency under the Federal Ministry of Science and Technology in 2001[68] to implement the National Information Technology Policy which was presented to Nigerians then. Subsequently, it became a creation of statute under the NITDA Act 2007.

The agency is committed to the drive to bring government and its services closer to the people through information technology. It is the agency entrusted with the implementation of the National Information Technology Policy, the pursuit of which is to make Nigeria an IT capable country in no distant future. Part of the assignment of the agency[69] is to create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria and all matters related thereto and for that purpose, and which without detracting from the generality of the foregoing shall include providing universal access to Information Technology and systems penetration including rural, urban and under-served areas. It is also to provide guidelines to facilitate the establishment and maintenance of appropriate information technology and systems application and

[68] http://www.nitda.gov.ng/aboutNitda/nitda-history.aspx
[69] Section 6 of the NITDA Act, 2007

development in Nigeria for public and private sectors, urban-rural development, the economy and the government.[70]

The agency is mandated by the 2007 Act to develop information technology in Nigeria through regulatory policies, guidelines, standards, and incentives. The agency claims[71] that part of the mandate is to ensure the safety and protection of the Nigerian citizen's personal identifiable information otherwise known as personal data, object identifiable information and a successful implementation of guidelines on data protection. In furtherance of the foregoing, the agency has published the draft guidelines which are yet to be adopted for implementation. However, there is no express statutory provision that empowers this agency to supervise private data processing practices. Other institutions that manage data like the National Identity Management Commission are not under any form of supervision by the NITDA.

Since it is the NITDA that is saddled with the responsibility of implementing the National Information Technology Policy and one of the basic strategies of the policy is the establishing of a Data Protection Act for safeguarding privacy of national computerized records and electronic documents, the Agency should push for the enactment of an appropriate data protection legislation even if it will take a little bit more enhanced version of the Draft Guidelines.

CONCLUSION

From the foregoing, it is clear that there is practically no institutional framework for data protection in Nigeria that is comparable to the institutions the United Kingdom and Canada. It is imperative that Nigeria not only legislate appropriately for data protection, the NITDA at the least should be given appropriate powers to oversee that data practices of companies that handle personal data until a proper government agency is established after the European model.

[70] *ibid*
[71] Preamble to the Draft Guidelines on Data Protection Version 3.1 available at http://www.nitda.gov.ng/downloads/Guidelines3.pdf

References

Books

Anderson, D. A. (1999) The Failure of American Privacy Law, in B. S. Markesisnis, (ed) *Protecting Privacy*, Oxford University Press.

Lloyd, Ian J. (2011) *Information Technology Law*, Oxford University Press, 6th Ed.

Schwartz, P. M. and Reidenberg, J. R., (1996) *Data Privacy Law: A Study of United States Data Protection*, Michie Law Publishers,

Periodicals

Reidenberg, J. R. Resolving Conflicting International Data Privacy Rules in Cyberspace 52, *Stanford Law Review* 1315

Schwartz, P. M., "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* Vol 52 p 1609.

Data-Protection Agencies Target Google *European Voice.com* 3rd April, 2013. Stratford, J. S. & Stratford, J. 'Data Protection and Privacy in the United States and Europe' available at http://www.iassistdata.org/downloads/iqvol223stratford.pdf.