Rethinking Data Protection Model for Investor/User Confidence in Nigeria

Thought Leadership | By Chuks Okoriekwe (Originally published in *BD LegalBusiness (BusinessDay), 18th January, 2018, p. 19)*

c.okoriekwe@lelawlegal.com

Introduction

The Economist[1] reported that big data companies (BDC): Alphabet (Google's ParentCo.), Amazon, Microsoft, Apple, Facebook and Amazon raked in more than US$25 billion revenues in Q1 2017, a trend that typifies the industry as 'the new oil'. Steady investment in acquisition of Information Technology (IT) companies was recently exemplified in Microsoft's US$26.2 billion deal for LinkedIn which industry experts argue was essentially to have access to LinkedIn's users' data.[2] More so, IT has stimulated growth of the knowledge economy and new industry expertise, *viz*: data analytics, Artificial Intelligence (AI), Search Engine Optimization (SEO), amongst others.

Central to the revenue of these companies is the mining of users' data (using data analytics to understand consumer trend and behaviour) which is subsequently sold to advertisers by offering free, and to some extent, premium services, to their users. This therefore calls to question issues of users' data security in cases of data breach by unauthorised persons and liability for such breach.

In September 2017, Equifax (an American credit reporting firm), disclosed that it suffered a data breach potentially affecting 143 million US consumers (involving customers' names, social security numbers, birth dates, addresses and, in some instances, driver's license numbers). This resulted in a significant drop in the value of its shares (losing more than 18% of its share price within four days of the announcement of the breach and has continued to take a hit).[3] These incidents of real or potential data breaches could erode the gains made so far in the IT industry by increasing legal risk and exposure to class-action suits by users. This article seeks to look at ways to boost investors' and users' confidence to ensure continuous growth in the industry, given the opportunities in sub-Saharan Africa and Nigeria in particular.

Cyberattacks: Threat to New Oil?

With over 3.8 billion people connected to the internet (June, 2017),[4] cyber-attacks have become a usual occurrence. Cyberattacks sometimes take the form of: indiscriminate and destructive attacks; cyberwarfare; government and corporate espionage; stolen email and login credentials; stolen credit card and financial data; and stolen medical related data which have prompted governments all over the world to put in place regulations to curb these incidents. Indeed, Nigeria enacted its ***Cybercrime (Prevention, Prohibition, etc.) Act No. 17 2015*** (which provides legal, regulatory and institutional framework for the prohibition, detection, prosecution and punishment of cybercrimes in Nigeria. It also provides for the retention and protection of data by financial institutions, criminalizes the interception of electronic communications amongst others) in reaction to these attacks.

In May, 2017 the world was hit with *WannaCry ransomware* which reportedly affected more than 230,000 computers in over 150 countries; notable victims included UK's National Health Service (NHS), Spain's Telefonica, FedEx and Deutsche Bahn, amongst others. In response, many global IT agencies issued precautionary advices. Nigeria's National Information Technology Development Agency (NITDA) established pursuant to the ***NITDA Act, Cap. N156 LFN 2004*** similarly issued precautionary advice to IT companies and users in Nigeria.[5]

Issues Arising

The question that further arises is *do IT companies have a duty to make full public disclosure when their systems have been compromised or become vulnerable to attacks?* It has been observed that companies are reluctant to make full disclosure of incidents of data breach due to its resultant reputational damage which could erode share value of the companies.

The first attempt at compelling companies and government to disclose incidents of data breach in the United States was initiated by California in 2002 *vide* its ***Data Security Breach Notification Law*** (effective on July 1, 2003) captured under **1798.29 (a)** and **1798.82** (a), ***California Civil Code*** which was subsequently amended in 2015. In respect of government's disclosure obligation, it provides, *"any agency that owns or licenses computerized data that includes personal information* ***shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data*** *to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent*

---

[1] The Economist, 'The World's Most Valuable Resource Is No Longer Oil, But Data' May 06 2017, <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (accessed 13.11.2017)

[2] Jay Greene, 'Microsoft to Acquire LinkedIn for $26.2 billion', Wall Street Journal, June 14 2016, <https://www.wsj.com/articles/microsoft-to-acquire-linkedin-in-deal-valued-at-26-2-billion-1465821523> (accessed 20.11.2017)

[3] The breach was made public on September 7, 2017 and its share price was down by 18% on September 11, 2017. It has continued to witness a significant decline from $143/share to $109.97/share as at 20/10/2017 demonstrating the impact of public disclosure of data breach on companies.

[4] See http://www.internetworldstats.com/stats.htm (accessed 16.11.2017)

[5] See Nkechi Isaac, 'NITDA Cautions Nigerians Over Ransomware Cyber Attack' Leadership Newspaper, 29/06/2017 <http://leadership.ng/2017/06/29/nitda-cautions-nigerians-ransomware-cyber-attack/> (accessed 16.11.2017)

with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." [Emphasis supplied]

Whist for businesses operating in the State, it provides, *"a person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."*

The ***US Securities and Exchange Commission*** (SEC) in its ***CF Disclosure Guidance*** issued in 2011 similarly states, *"…although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."*[6] This recognises the obligation of companies to disclose incidents of data breach.

The fact that there is no equivalent Nigerian provision is a serious cause for concern. To draw an allusion, whilst Nigerian public companies under ***para 34.5(g), SEC's Code of Corporate Governance, 2011*** are under an obligation to disclose risk management policies (which may include steps taken to ensure that its systems are not vulnerable to cyberattacks) to guide investors in their investment decision, private companies do not have similar disclosure obligations. The closest attempt to impose such obligation was witnessed in the Financial Reporting Council of Nigeria's *Code of Corporate Governance, 2016* which is currently suspended. This thus makes risk exposure (including cyberattack) disclosure discretionary for private companies.

As at date, there is no particular requirement for data holders (DHs) to disclose any incidents of data breach to data owners (DOs) despite the revelation by the Senate that more than US$450 million had been lost through cyberattacks by Nigerian firms in over 3,500 attacks.[7] It could however be argued that DHs owe a fiduciary duty to disclose such to DOs to enable them ascertain their level of exposure to cyber criminals. Given NITDA's regulatory mandate, it may be prescient to issue guidelines on disclosure of data breach by DHs to DOs or users following the State of California's model. However, the recently passed ***Electronic Transaction Bill, 2017 (ETB)*** (passed in May, 2017)[8] reposes more responsibilities on DHs. Accordingly, ***section 23, ETB*** provides *"a data holder must implement appropriate technical and organizational measures and exercise reasonable care to protect personal data against accidental loss and against unauthorised alteration, processing, disclosure or access, in particular where processing involves the transmission of data over a network, and against all other unlawful forms of processing."*

The ETB further strengthens DOs' rights in determining how and for what purpose their data could be processed. It further states in ***section 20(4)*** that: *"an individual shall be entitled to apply for the suspension, withdrawal or order the blocking removal or destruction of personal data, on proof that it is incomplete, outdated, false, compromised, unlawfully obtained, used for unauthorised purpose or no longer necessary for the purpose for which it was collected."* It is arguable whether a mere application to the DH would suffice in deleting owners' data from its database.

There are also instances where these data have been replicated and stored (lawfully shared) with multiple channels most of whom may not be known to, or have a relationship with, the DO. Could the liability of the DH under ***section 22, ETB*** (which makes a DH liable to compensate DO for damage), extends to any person acting under the instruction of the DH or could DHs be liable for third party 'unlawful' processing of owners' data after a request to delete same has been sent to the DH?

For instance, Paylater,[9] an innovative financial service company and major player in Nigeria's FinTech space, which provides access to credit to Nigerians within 30 minutes requires potential customers' Bank Verification Number (BVN) including access to social media account(s) during the loan application process. Whether or not such application is approved, data entered on its database is retained. Extracts from its privacy policy, '*Disclosure of Your Information*' provides: *"we may share your personal information with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries. We may share your information with selected third parties including: a) Business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or you. b) Advertisers and advertising networks that require the data to select and serve relevant adverts to you and others."* Consequently, data collected from users may be shared with third parties with whom the data subject may not have a relationship.

Paylater's data policy however, stipulates its adherence to ***Section 5, Parts 1 and 2, NITDA's National Information Systems and Network Security Standards and Guidelines, 2013*** which obligates organizations doing business in Nigeria to protect the confidentiality of Object Identifiable Information (OII) defined to mean *"information which can be used to distinguish or trace an individual's identity, such as name, national ID number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."*

Despite ETB's silence on issues of DHs' vicarious liability, there could be compelling argument (depending on the terms of contract between the DH and DO) to suggest that such DH may become liable upon written notice to delete owner's data and failure to notify others (DHs or processors) with whom it has shared such data which results in damage to the DO.

Notwithstanding, the Nigerian Communications Commission (NCC)'s ***Consumer Code of Practice Regulations (CCPR), 2007*** provides that licensees must take reasonable steps to protect customer information against improper or accidental disclosure whilst under ***Registration of Telephone Subscribers Regulations (RTSR), 2011*** subscriber's information in Central Database shall be held in strict confidence and no person or entity shall be allowed to have access except as may be provided under the RTSR failing which there are penal sanctions against licensees. These regulation are however only applicable to telephone operators.

Recourse of Data Owners Against Data Holders For Breach

Considering the emergence of business models built on data analytics, especially in the financial services industry, the need for optimum data security cannot be over emphasized. It is no longer news that IT companies globally suffer reputational and financial loss as a result data breach. A good example is the infamous *Ashley Madison* data breach in 2015. Ashley Madison, a Canadian online dating site promotes extra marital affairs among married people (using its famous tagline: "*Life is short. Have an Affair*"). It reportedly made millions of dollars from members by offering premium *'Full Delete Feature'* service with an assurance to delete members' data upon the payment of a

---

[6] See, Securities Act Rule 408, Exchange Act Rule 12b-20 and Exchange Act Rule 14a-9. See also: Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976).

[7] Azimazi Momoh Jimoh, Oludare Richards and Segun Olaniyi: 'Senate Alert NSA, Others to Cyber Attacks on Nigerian Firms', The Guardian, 24 May, 2017 <https://guardian.ng/technology/senate-alerts-nsa-others-to-cyber-attacks-on-nigerian-firms/> (accessed 02.11.2017).

[8] Given that the President is yet to assent the bill and the 30 day window to do so had lapsed – section 58(4), 1999 Constitution (as amended) – the bill will have to undergo fresh legislative process at the National Assembly (National Assembly v. President & Ors. [2003] 9 NWLR (Pt. 824) 104.

[9] Paylater is a product of and operated by One Finance & Investment Limited (One FI). <https://www.paylater.ng/privacy> (accessed 18.12.2017)

$19 fee, which it never did. The hack on its database potentially exposed more than 37 million users' data, resulting in the payment of over $11.2 million as compensation (without proof of damage) to users.

Under ***section 21(3) ETB, 2017,*** for a data owner (defined as an individual who is the subject of personal data) to successfully claim against DHs, he must show that he has suffered ***'damage'*** by reason of contravention of the provisions of the Bill. Merely failing to secure owner's data thereby resulting in unauthorized access is insufficient to claim compensation. This is however not restricted to data owners as the Bill rightly employed the word, 'individual' thereby opening up the category of persons that could institute an action against DHs, once such a person could show that damage resulted from the contravention of the Bill by DHs.

Could it be argued that making contravention actionable *per se* (without proof of damage) may expose DHs to frivolous claims? Whilst DHs have both legal and fiduciary obligations to secure owner's data using appropriate technologies, it may however stiffen growth of the industry if they are subjected to unsubstantiated claims by DOs. It is nonetheless prescient to strike a balance between DO and DH interests, whilst not compromising data security.

Cyber and Privacy Insurance Policy Options

It is becoming increasingly expedient that DHs put in place mechanisms to engender users' and investor confidence to promote growth. An option that has been widely adopted in advanced economies (US, Canada, South Africa, amongst others) in mitigating DH's monetary loss resulting from data breach is the *Cyber Liability Insurance Policy* (CLI). As its name implies, it is specifically designed to cover users of technology services and products as it relates to the collection and usage of data. This insurance policy option could be applicable to liability resulting from data breach affecting client or user's personal information. Depending on the arrangement between the insurance companies and DH, it could also cover notification costs, cost of defending data breach claims, fines, credit monitoring, etc.

One of the learning points from the Equifax data breach was the fact that Equifax had reportedly insured itself against such liability to the tune of more than $130 million,[10] although it has been argued that the amount is inadequate to off-set its entire liability (which is estimated to run into billions) owning to the magnitude of breach and the number of users involved.[11] Equifax witnessed more than 250 lawsuits filed against it by users within days of the data breach disclosure.

In Nigeria, there is no express provision for CLI. Notwithstanding, ***section 2(h) and (5), Insurance Act, Cap. I17 LFN, 2004***, allows insurance companies to carry on new category of miscellaneous insurance business if they shows evidence of adequate reinsurance arrangement in respect of that category of insurance business and requisite capital where necessary. Considering the level of cyberattacks and its potential to erode investor and user confidence in Nigeria's budding cyberspace, it may be prescient that CLI products be introduced by insurance companies (few insurance companies have introduced the product, it is yet to gain full traction) in collaboration with National Insurance Commission (NAICOM) and NITDA such that it would be compulsory for DHs to insure the data they hold against theft, loss, damage, liability or damage arising from unauthorized access.

The provision of CLI would ensure that DHs pass the risk of potential liability to insurance companies which would in turn settle any claim that may arise in respect of the insurance policy thus boosting investors' and users' market confidence. It may be argued that a CLI would increase compliance cost of DHs, thereby increasing their cost of doing business. However, the provision of CLI would secure a win-win position for DHs. This is premised on the fact that their risk exposure would be optimised in addition to the potential to on-board more DOs with the assurance of an insurance package in case of data breach whilst assuring them of state of the art data security offerings.

Conclusion

Looking at the value in big data in Nigeria, the Federal Government (FG) ought to put in place policies to strengthen and unlock its growth potential. The threat of cyber-attacks pose a grave danger to upping the potential of this emerging market. Investors must be assured of security of their investment in data companies whilst users must also have heightened confidence in the security of the system to protect personal information provided to DHs. In this regard, law enforcement agencies are constantly wading off cyberattacks through arrest and prosecution of offenders (which could take months and sometimes years) whilst the damage has been done leaving DOs distrust with the system.

The regulator, NITDA however need to put in place mechanisms to ensure that incidents of breach are disclosed to those affected and adequate compensation paid in the event the DO suffered damage as a result of the breach. Nonetheless to protect DHs, there should be collaboration with NAICOM to provide compulsory cyber liability insurance. This would ultimately increase liquidity in the insurance industry whilst ensuring incremental insurance penetration rate in Nigeria.

[10] Equifax Breach: Cyber Insurance to the rescue?! <https://www.riskbasedsecurity.com/2017/09/equifax-breach-cyber-insurance-to- the-rescue/> (accessed 02.11.2017)

[11] Sonali Basak and Jennifer Surane: Equifax Liability Insurance is Likely Inadequate for Breach. Bloomberg, 9 September, 2017 <https://www.bloomberg.com/news/articles/2017-09-09/equifax-s-insurance-said-likely-to-be-inadequate-against-breach> (accessed 02.11.2017)