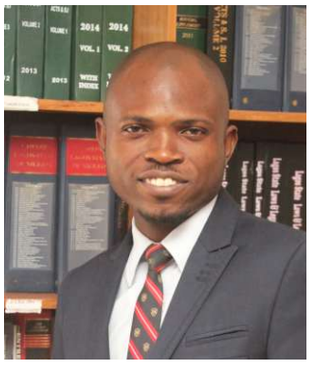
Crossing the Fine Line:

Legal Issues of Data Misuse in Nigeria

Thought Leadership | **By Chuks Okoriekwe** (Originally published in *BD Legal Business, 10. 05. 2018, p.25*)



c.okoriekwe@lelawlegal.com

Introduction

At the heart of the US election probe following recent developments from US Congress' hearing is the claim that Facebook's users' data were misused by Cambridge Analytica to manipulate voters' choice. This was also the case in Nigeria where President Buhari's medical records were said to have been hacked by Cambridge Analytica during the build up to the 2015 general elections.

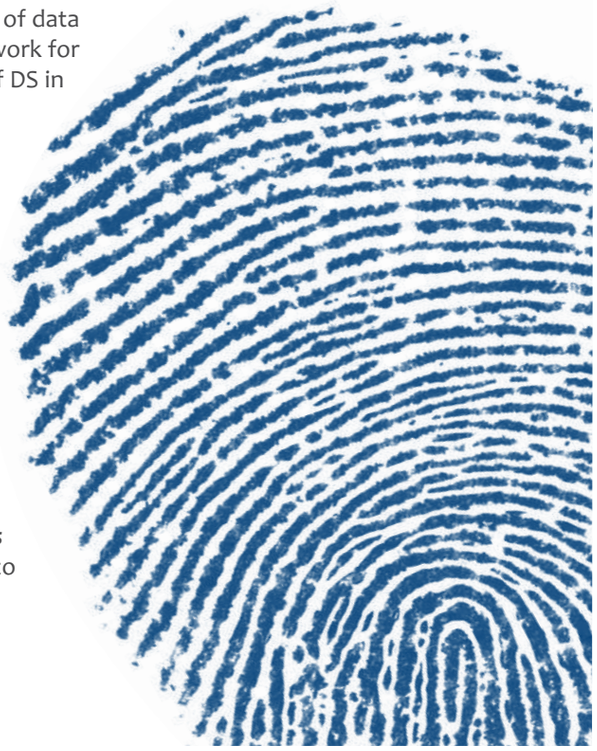
These issues have revealed one of the downsides of data storage and sharing of personal preferences on social media, particularly with third party applications using the interface/application of a 'trusted' platform. This is often the case where websites as part of their Terms of Services (ToS) indicate that they would share user information/data with third parties. It is therefore pertinent to ask whether data holders (DH) could be held liable for breach of contract and criminal breach of trust in instances where data subject (DS)'s data are used for purposes other than agreed by the DS?

For instance, Mr. A is required by Company B to take a survey wherein he inputs his personal information. Thereafter, he receives a message from Company C (an unrelated company) about the survey he filled, asking for more information from Mr. A or directly marketing a product to him based on the information filled in the survey. The question that arises is whether Mr. A's data has been used for the purpose for which it was meant? Simply put, has Mr. A expressly consented to his data being shared with another party? This article seeks to examine the legal issues of data misuse in Nigeria whilst examining the legal framework for the protection of data as well as possible redress of DS in cases of misuse.

Data Misuse in Nigeria – How Construed?

Data misuse can simply mean a situation where data is inappropriately used as defined when the data was initially collected from DSs. The legal basis for protecting personal data from any form of misuse is the duty to protect the confidence and privacy of personal information. This right to privacy is guaranteed by ***section 37 Constitution of the Federal Republic of Nigeria 1999 (1999 Constitution) (as amended)*** *"The privacy of citizen, their homes,* ***correspondence, telephone conversation and telegraphic communication is hereby guaranteed.****"* The sanctity of the right to privacy was reiterated by the Supreme Court in ***MDPDT v. Okonkwo [2001] FWLR (Pt. 44), 542*** when his Lordship ***Ayoola JSC,*** stated that *"The right to privacy implies a right to protect one's thought; and one's body from unauthorized invasion."* Although, the right to privacy is not absolute, any derogation must be within lawful justification (***section 45 1999 Constitution***).

One of the first attempts by the government to provide a shield for data use is vide ***section 10(1) (b) (i) Wireless Telegraphy Act***[1] which provides that: *"No person shall – otherwise than under the authority of the Commission, or in the course of his duty as a servant of the State, either – use any wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addresses of any message (whether sent by means of wireless or not) which is neither the person using the apparatus nor any person on whose behalf it is acting is authorised by the Commission to receive."* Accordingly, any attempt to intercept a message sent by telegraphic or any other (electronic) means without the authorization of the Nigerian Communications Commission (NCC) or the National Broadcasting Commission (NBC) is prohibited and punishable.



[1] ***Cap. W5 LFN, 2014***

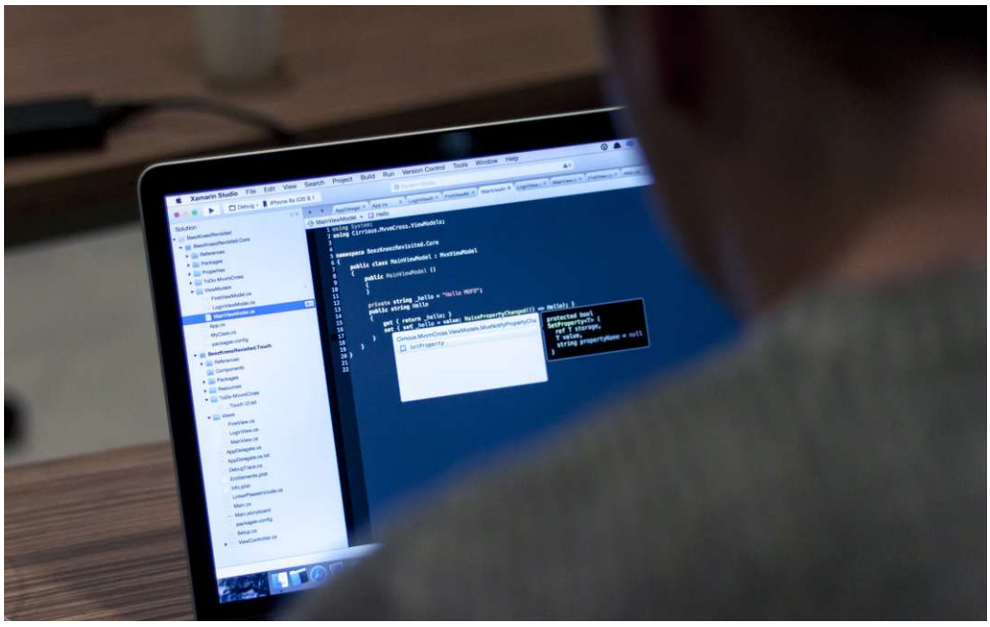
This is the precursor to the ***Cybercrimes (Prohibition, Prevention, etc.) Act***[2] which criminalises unlawful access to computer, system interference, unlawful interception, etc. with fines and terms of imprisonment. However, with Nigeria's increasing internet penetration rate (which has reportedly reached 100.9 million people by NCC, Feb 2018), there is need to strictly protect the confidence of users' data shared with online platforms.

In the medical space, the position of the law appears to be settled – a medical practitioner is prohibited from disclosing the data of patients except as permitted by the law. However, owing to technological advancement in health care service delivery (telemedicine), the thin line may have become blurry. ***Section 26(1) National Health Act (NHA)***[3] provides that: *"all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential."* Thus, disclosure in this circumstance is prohibited.

Notwithstanding, it is pertinent to consider whether the standard of confidentiality reposed on a health establishment is applicable to online health care providers given recent developments in the sector. ***Section 64 NHA*** in interpreting *"health establishment"* posits that *"…the whole or part of a public or private institution, facility, building, or place, whether for profit or not, that is operated or designed to provide inpatient or outpatient treatment, diagnostic or therapeutic interventions, nursing, rehabilitative, palliative, convalescent, preventive or other health service…"*, it could therefore be presumed that this confidentiality requirement is binding on online medical platforms. Arguably, this position is apposite given that operators of such platforms are regulated by the Medical and Dental Council (MDC) – the regulator of medical practitioners in Nigeria.[4]

This is more so that ***Para. 9(f) Code of Medical Ethics in Nigeria*** reiterates confidentiality of patient's data by stating that *"All communications between the patient and the practitioner made in the course of treatment shall be treated in strict confidence by the practitioner and shall not be divulged unless **compelled by law or overriding common good or with the consent of the patient**."* By clicking to sign up with an online medical service provider, the user has invariably consented to having his medical records shared with third parties. However, this should not be misconstrued as a blanket consent. Users' data can only be shared in accordance with the online medical service provider's ToS and privacy policy.

Owing to deluge of unsolicited calls and text messages from telecommunications service providers (TSP), the NCC issued its "Do Not Disturb" directive in 2016 to TSPs mandating them to provide options for users to opt out of their messaging service through a short code. Similarly, the NCC through its ***Draft Consumer Code of Practice (Draft Code), 2018*** (an improvement on its 2007 Code) seeks to strictly regulate the use of consumer data by TSPs. Accordingly, **section 43(1)** ***Draft Code*** provides a minimum threshold for data collected from consumers particularly: shall be processed for limited and identifiable purposes; kept not longer than necessary; not transferred to any party except as permitted by any terms and conditions agreed with the consumer, etc. Also, a licensee (TSP) is required to meet accepted fair information principles including, the choices consumers have with regard to the collection, use, and disclosure of the information (***section 43(2) (b) Draft Code***). Although these provisions are only applicable to TSPs, it is nonetheless comforting that more than 148 million telephone subscribers in Nigeria would have recourse in ensuring that their data is not used for any other unintended purpose.



In a bid to strictly regulate the use of credit information released to Credit Bureaus by DSs under the ***Credit Reporting Act (CRA),***[5] ***CRA's section 7(1)*** provides that: *"a Credit Information User may only seek credit information from a Credit Bureau for a permissible purpose."* It thereafter listed "permissible purpose" under the ***CRA***. The implication of this provision is that where the Credit Information User seeks credit information from a Credit Bureau, the purpose of such information must be stated in the request form. Consequently, where such information is used for any other purpose, the Credit Information User will be liable under the ***CRA***. It is however in doubt whether DS could institute a civil claim against Credit Information Users for breach of privacy.

The ***Electronic Transaction Bill (ETB), 2017*** is illustrative of future legislative direction – having been passed by the National Assembly in May 2017 but lacking Presidential Assent and is therefore spent. ***Section 19(2), (3) and (5) ETB*** is to the effect that personal data ***shall only be obtained for specified and lawful purposes and are not to be processed in any manner incompatible with those purposes***. Also, it shall also be ***adequate, relevant and not excessive for the purpose for which they are processed***. In the same vein, regardless of the purpose of obtaining personal data, they are not to be kept for longer than required for the fulfilment of the purpose for which they were obtained. These provisions are instructive as they seek to strictly regulate the use of data collected from DS.

[2] ***Act No. 17, 2015***
[3] ***Act No. 8, 2014***
[4] See ***section 1 Medical and Dental Practitioners Act, Cap. M8, LFN 2004***
[5] ***Act No. 2 2017***

American Data Use Disclosure Approach

The United States (US) has evolved its data use disclosure requirements to ensure that online platforms disclose in their ToS the nature of data collected from users, the manner in which they are collected and intended use. The Federal Trade Commission (FTC) has been at the forefront of sanctioning erring platforms which fails to either properly disclose its privacy policy to its intended users or uses such data in an unintended manner. In a landmark case filed by the FTC against ***GeoCities Inc.***[6], it was established that GeoCities Inc. shared users' data with third parties against its privacy policy.[7] The settlement increased the debate for informed consent in data use especially with regards to children who cannot validly give consent. The US Congress thereafter passed the ***Children's Online Privacy Protection Act (COPPA)***[8] to protect children's privacy.

According to ***Julie Brill***, an FTC Commissioner *"…companies should disclose how they will protect consumers' data, and those disclosures must be truthful and not misleading."*[9] Also the FTC has gone ahead to strictly enforce privacy standard even against 'big' companies including Facebook[10] and Snapchat.[11] States in the US have begun to take measures to protect online privacy of residents. In 2003, California became the first to introduce its ***Online Privacy Protection Act*** which requires operators of commercial websites that collects personally identifiable information about California consumers to conspicuously post its privacy policy on its website.[12] This policy must identify the type of personally identifiable information that the operator collects and the type of third parties with whom the operator might share the information.[13]

The US position on application of privacy rules may have been relaxed following President Trump's signing of the ***Joint Congress Resolution (S.J.Res.34)*** which removed the Federal Communication Commission (FCC)'s restriction on Internet Service Providers (ISP) from selling customer data.[14] Some have argued that it would create a level playing field for ISPs and big data companies such as Google and Facebook which already have access to such data – which has been trailed by States (including Connecticut, Illinois, Kansas, Maryland, Massachusetts, Minnesota, Montana, New York, Washington, and Wisconsin) proposing their model law for regulating internet privacy of their residents.

Liability for Data Misuse in Nigeria – Culpability in Breach of Contract and Trust?

The relationship between DHs and DOs is strictly governed by contract, that is, the ToS to which the DO agreed to upon signup. These ToS usually contain privacy policy which stipulate the nature of data obtained from the DO and how such data is to be used. It is noteworthy that any deviation from the ToS would constitute a breach of contract actionable against the DH. According to ***section 21 ETB,*** *"…an individual shall be entitled to be* ***informed*** *by any such DH where personal data of which that individual is the DO are being processed by or on behalf of that DO….the purpose for which they are being or are to be processed…"* A key element recognised under the ETB on data use by DHs is disclosure to the DO and consent to use such data for specific purposes. More so, DOs can validly withhold consent and instruct the DH to stop further processing of his data, ***section 22 ETB***. Perhaps, the liability of DHs were amplified when ***section 22(3) ETB*** makes a DH liable to compensate the DO where he has suffered damage arising from DHs breach of the ETB.

[6] *Re GeoCities, Inc.*, No. C – 3849 <https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm> (accessed 17.04.2018)

[7] Amongst other reliefs granted to the FTC by the Court, it was required that: i) a clear and prominent privacy notice on each page of its internet site at which information is collected telling consumers what information is being collected, the purpose for which it is collected, to whom it will be disclosed and how consumers can access and remove the information; ii) an opportunity for the member to have his or her information deleted from GeoCities' site along with any third party databases; iii) visitor access to the information collected at the site; iv) secure data storage; v) parental consent before collecting personal identifying information from children ages 12 and under; and vi) an ability to enforce the requirements, including a link to the FTC Internet site.

[8] ***15 U.S.C. §§ 6501-06***

[9] Julie Brill, ***'Privacy and Data Security in the Age of Big Data and the Internet of Things'***, lecture delivered at Washington Governor Jay Inslee's Cyber Security and Privacy Summit, January 5, 2016 <https://www.ftc.gov/system/files/documents/public_statements/904973/160107wagovprivacysummit.pdf> (last accessed 17.04.2018)

[10] See, ***'Facebook Settles FTC Charges That It deceived Consumers by Failing to Keep Privacy Promises,'*** available at <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep> (accessed 17.04.2018)

[11] ***In re Snapchat Inc., No. C - 4501***

[12] ***Cal. Bus. & Prof. Code § 22575***(a); See also, ***Internet Law and Practice, West South Asian Edition (Vol. 2), 2013 §19:52***

[13] ***Cal. Bus. & Prof. Code §22575(b)***

[14] See, FCC December 20016 rule, ***'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.'*** The Rule : (i) applies the customer privacy requirements of the Communications Act of 1934 to broadband Internet access service and other telecommunications services; (ii) requires telecommunications carriers to inform customers about rights to opt in or opt out of the use or the sharing of their confidential information; (iii) adopts data security and breach notification requirements; (iv) prohibits broadband service offerings that are contingent on surrendering privacy rights; and (v) requires disclosures and affirmative consent when a broadband provider offers customers financial incentives in exchange for the provider's right to use a customer's confidential information.

Although civil liability for data misuse could be gleaned from contract and statute, could there be a criminal angle arising from such misuse, for instance, criminal breach of trust? To answer this question, ***section 311 Penal Code Act (PCA), Cap. 532, LFN 1990*** (applicable to only Northern parts of Nigeria) could be helpful. It states: *"whoever, being in any manner* ***entrusted with property*** *or with a dominion over property, dishonestly misappropriates or converts to his own use that property or* ***dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which that trust is to be discharged*** *or* ***of a legal contract express*** *or* ***implied,*** *which he has made touching the discharge of the trust, or* ***wilfully suffers any other person so to do,*** *commits criminal breach of trust." (Emphasis supplied)*

In establishing ingredients of the said offence, the Court of Appeal in ***Hon. Yakubu Ibrahim & Ors v. Commissioner of Police***[15] *per* ***Peter-Odili JCA*** (as she then was), held: *"The ingredients of the offence of criminal breach of trust contained in section 311 of the Penal Code and which must be proved before a charge, for same can be sustained are:- (a) that (t)he accused was entrusted with property or with dominion over it. (b) that he (i) misappropriated the property; (ii) converted such property to his own use; (iii) disposed it. (c) that he did so in violation of:- (i) any direction of law prescribing the mode in which such trust was to be discharged; or (ii) any legal contract of law expressed or implied which he had made concerning the trust; or (iii) he intentionally allowed some other persons to do or commit the above stated, (d) that he acted dishonestly as in (b) above."*

Could it therefore be argued that DHs ToS creates a trust relationship between the DHs and DOs? Although, trust is a creation of equity (which will not suffer a wrong to be without a remedy),[16] it has been rightly opined that the relationship between DHs and DOs could be classified as such. For instance, when compared with bailment, where goods are delivered to the bailee without transferring ownership, the bailee thereafter becomes a 'trustee' for the goods delivered to him. Same position could be applied to DHs/DSs relationship, the data is owned by the DS whilst the DH merely act to hold such data.

Consequently, data being an incorporeal property to which DOs have rights, can validly fall within the contemplation of ***section 311 PCA*** and the relationship between the DHs and DOs are governed by the ToS including its privacy policy. Any form of misuse by DHs would constitute criminal breach of trust thus, increasing their legal exposure in both contract and trust.

Conclusion

Whilst it is true that data drives the digital economy, it is important that in processing DS' data, DHs must ensure that the purpose for which such data is to be used is well stated in their privacy policy. This would invariably create a measure of disclosure and informed consent by the DS. Although, the ***ETB*** is yet to become applicable, its provisions are instructive and as such DHs should begin to take steps to ensure that their data disclosure and use standard are aligned with its provisions. By so doing, reputational risk exposure (in addition to potential fines, damages and possible criminal breach of trust), would be minimized.

[15] *(2010) LPELR – CA/A/6C/2007*
[16] *Omoyinmi v. Ogunsiji [2008] 3 NWLR (Pt. 1075) 471 at p. 490*