

THE WHITE COLLAR

IDOWU OLOFINMOYIN

idowu.olofinmoyin@norfolk-partners.com



The Cost of Cold Calling

4:45pm on a Friday, a tense business conversation between Kene Rimii an investor and an auctioneer at the Bank of Industry assures the Kene that he has been short listed to participate in a private auction where his company and two others can gain exclusive access to five start-up companies and their lucrative technologies. The auctioneer informs Kene that the bids are closed and they must be by text message to a specified number within a five minute period, after which if there is no reply text each company must rebid. All is well with Kene's bid, he does get a reply text, but then he opens it and reads "Congratulations! You have won 5 Days FREE Trial of inspirational tips & messages send 'INSPIRE ME' to 001100". As he reads this another message comes in from the auctioneer informing him his company narrowly lost out to another bidder's second bid.

Value of Text Alert Business

It goes without saying that anyone with a mobile phone in Nigeria can relate on some level to Kene's frustration. Millions of mobile network subscribers everyday are bombarded with unsolicited messages and telephone calls from vendors or all kind that have acquired access to the varied and lucrative market of mobile phone users. In fact in some countries these markets are so lucrative that with proper analysis mobile phone users' data can be cross-referenced with other information to identify buying patterns and even political ideology, and so the power inherent in that information cannot be underestimated. In fact today it is not strange for mobile phone users to receive phone calls from perfectly legitimate numbers which then turn out to be conduits for mechanical-automated services selling the next best miracle product.

While of course some of these messages and "cold calls" are received because the mobile phone user somewhere consented to some direct marketing correspondence program, most are never aware nor are they informed of the manner in which their personal information will be used or sold to and by third parties trading in bulk customer data. The difference with our relatively nascent telecommunications industry is that while this might be a legitimate means of contacting willing and consenting users, there are very few ways of restricting the abuse and misuse of personal data that is obtained often by data theft, data 'phishing' i.e. the acquisition of sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy source, or simply by misapplication.

CAMPBELL v GOMEZ

An interesting case of this nature decided recently at the Supreme Court of the United States in **CAMPBELL-EWALD COMPANY**

v JOSE GOMEZ 2016 (cited as 577 U. S. No. 14-857 (2016)) gives an interesting perspective on unsolicited messaging and cold calling. A United States Navy Contractor Campbell-Ewald Company was engaged for the purpose of developing a multi-media campaign for young adults that had "opted-in" to receive such direct marketing information on topics that concerned U.S. Navy service. Campbell's subcontractor then generated a list of mobile telephone numbers and transmitted the U.S. Navy's message to over 100,000 recipients including Mr. Jose Gomez who claimed he did not "opt-in" to receive the information and being 40 years old was not part of the U.S. Navy's catchment age group. Mr. Gomez then started a class action against Campbell claiming that the company breached section 227(b)(1)(A) (iii) of a U.S. Statute, the **Telephone Consumer Protection Act** (TCPA), 47 U. S. C., which prohibits "using any automatic dialing system" to send a text message to a mobile telephone. Now while the statute breached in the above matter is a U.S. statute and inapplicable within our Nigerian shores, we do have similar laws passed to protect the same intent here at home, the most significant being the **Consumer Code of Practice Regulations** (CCP Regulations) 2007 formed pursuant to section 106 of the Nigerian Communications Act (NCA) 2003.

The Consumer Code of Practice

For the most part the NCA 2003 sets the framework for the regulation of the Telecommunications industry in general, but the Consumer Code of Practice sets the regulations regarding the protection of Consumers and acceptable standards of consumer related practices. Section 35 of Part II of these regulations deals with the Protection of Consumers Information. It stipulates:

"(1) A Licensee [mobile network provider] may collect and maintain information on individual Consumers reasonably required for its business purposes. However, the collection and maintenance of information on individual Consumers shall be—

(a) fairly and lawfully collected and processed; (b) processed for limited and identified purposes; (c) relevant and not excessive; (d) accurate; (e) not kept longer than necessary; (f) processed in accordance with the Consumer's other rights; (g) protected against improper or accidental disclosure; and (h) **not transferred to any party except as permitted by any terms and conditions agreed with the Consumer, as permitted by any permission or approval of the Commission, or as otherwise permitted or required by other applicable laws or regulations.**"

Subsection 2 continues to identify the principles of fair information collection to which mobile network operators should adhere and section 36 goes further to make compulsory the formation and application of a policy regarding the

proper collection, use and protection of Consumer information collected.

Therefore, following on from the spirit of the U.S' TCPA as seen in **CAMPBELL v GOMEZ** above our **CCP Regulations** seem to impose a similar duty to treat Consumer information with care. This is of course separate from the implied and express contractual obligation owed by mobile network operators to their Customers to use Customer data for the purpose it is given.

Business Purposes

Nonetheless some clear differences exist between the protection the U.S' TCPA provides and the intent in the CCP Regulations. For instance a cursory examination of the wording of the TCPA's duty will show that it creates a peremptory strict liability duty actionable immediately upon breach. Section 227 states:

"It shall be unlawful for any person ...-

(A) to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice—"

(iii) to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call, unless such call is made solely to collect a debt owed to or guaranteed by the United States;"

Whereas our CCP Regulations create an *intent*, by identifying principles upon which mobile network operators should operate when dealing with Customer information the TCPA stipulates exactly what is prohibited, it creates a negative obligation "not to do" something which is easier to enforce than an obligation to "act in accordance with certain principles".

Also the CCP Regulations permits the use of customer information *reasonably required for its business purposes* a very welcome exception to every shrewd mobile network operator because there is no limitation inherent in that, against the use of Customer information for new businesses i.e. Customer information may be used in new promotions even where they have not requested to be included in such. Customer information may then be viewed as a secondary "work product" or asset developed in the primary operation of providing mobile network service, and if viewed that way the information now belongs to mobile network operators rather than individual customers.

The general perspective that becomes clear comparatively across both the Nigerian and American approach to the same breach is that the Americans take it more seriously and so they place greater requirements of accountability for Customer information. Our approach on the other

hand is to afford mobile network operators, rightly or wrongly ample leeway to create the mobile networks necessary for the Telecommunications revolution we have experienced since 2001 when the first licenses were issued. Still, we need to ask ourselves at what cost it has come.

Quantifying Frustration

So how much is your frustration worth? What is the value of these interferences into our daily lives? How many times do we rush to the phone hearing a message or a call come through hoping to see a "bank alert" or talk to a human being, only to find that we "have won" something we are really paying for? The TCPA says in section 227 (3) :

"A person or entity may... bring in an appropriate court of that State-

(b) an action to recover for actual monetary loss from such a violation, or to receive \$500 in damages for each such violation, whichever is greater, or

(C) both such actions."

That means ordinarily to every American customer every unsolicited marketing message, call or page, wherever they come from, is worth \$500 or more, and there aren't many more effective deterrents to abuse of Customer information than a punitive monetary fine. So if a punitive monetary fine is deterrent to the abuse of customer information what is the effect of its absence? And what does that say your customer information is worth?

Customer is King

We are a nation 150-170 million strong, mobile cellular usage penetration is 107% greater than economies in Europe and more than even the U.S. We are the delight of any business operator that can manage to learn to thrive in the understandably difficult business conditions we have come to know as our economy. We have a voice. But consistently we see the reinforcement in our laws, our businesses and thinking the ideology that the ordinary Nigerian consumer is insignificant. One out of 170million can be ignored especially when they have no connections or influence, while the same principles we claim to protect make other nations great as they ensure that they go beyond words to actually protect their citizens. The comparisons may seem clichéd, but the truth is in today's global economy best practices become apparent in spite of what we know and have become used to. So what should we do? How do we begin to protect ourselves and the privacy of our information? By beginning to ask for accountability and asking that those who have our information use it only in ways that we permit. If we do not then we can all just get used to the unwanted intrusions we every time we hear the phone ring or that phantom bank alert comes through.

Panama Papers and Tax Planning - Beyond the Hysteria

Tunde Esan

The headlines are mind numbing "# Panama Papers: How Tinubu operated 12 Shell Companies in Tax Havens"; "EFCC to probe Nigerians named in Panama Papers"; "Topmost Cleric, TB Joshua caught in Panama Papers Money Laundering Scandal". From Dangote to David Mark and to the perennial 'suspect', Bukola Saraki, the 'criminality' of individuals and corporate bodies for operating tax havens are 'exposed' daily.

While one may excuse the ignorance of a lot of contributors who may be truly ignorant on the usage of a tax haven as an instrument of tax planning, the deliberate blurring of the fine line between tax avoidance and tax evasion by informed commentators in order to fit a preconceived narrative of the thieving elite is inexcusable.

A Tax Haven is described as a State, country

or territory where on a national level certain taxes are levied at a very low rate or not at all. It also refers to countries which have a system of financial secrecy in place while the Organisation for Economic Cooperation and Development (OECD) identifies the absence of any form of taxation or only nominal taxation as the most vital ingredient in determining whether a jurisdiction is a tax haven (Wikipedia).

The question that arises is whether it is criminal for an individual or juristic person to plan his/its financial affairs in a manner not prohibited by law to pay the least possible tax on his/its income?

In 2009, Google reported a gross profit of €5.5billion and an operating profit of €45million claiming it had spent €5.46billion on administrative expenses at its Bermuda Headquarters as licence to operate. Amazon had a running battle with the Internal Revenue Service of the United States of America in 2011 over an alleged USD 1.5 billion in back taxes over its Permanent Establishment (PE) hosted in Luxembourg,

Barclays, Ikea, AIG, GlaxoSmithKline, HSBC, Microsoft, FedEx, Citigroup, Black & Decker, JP Morgan, Vodafone and other companies which pride themselves in best practices have utilised tax havens in tax planning.

A cursory look at the upstream sector of the oil and gas sector in Nigeria reveals that while Shell with its extensive interests in the Niger Delta Area has only 18 (eighteen) subsidiaries registered in Nigeria it is reported to have 455 (Four Hundred and Fifty Five) subsidiaries registered in tax havens. In the same sector, the registration of the drilling rigs employed in the sector with the exceptions of Akpo, Trinity Spirit, OES Integrity and a few others registered in Nigeria are in far flung places like Singapore, Saint Vincent and Grenadines, Marshall Islands, Panama, Liberia, Belize and other tax havens.

The implication of the two preceding paragraphs above should be a condemnation of the usage of tax havens which robs the country of tax but the reverse really is the case that as long

as the usage of tax havens is not criminalised it may raise ethical questions and not a lot more.

J. Matsen Esq, speaking on tax havens and the litigious propensity of the average American said "Imagine spending years of your life building your financial empire only to have all seized and lost in a legal battle...when created in a legal manner, an offshore bank account can be an effective part of your asset protection plan and protect you from future creditors. Offshore bank accounts aren't and don't have to be a grey area of law".

In the classification of countries in 2013 which would fit into the definition of a tax haven 82 countries were listed while a body calling itself the Federation of American Scientists launched a report on 15 January 2015 where it listed 49 countries as tax havens spanning British Virgin Islands, US Virgin Islands, Mauritius, Liberia, etc.

Tax matters are a function largely of sovereign

CONTINUED ON PAGE 15