



Editor's Note

Welcome to the maiden edition of the Trenchard Partners Newsletter. For readers who are hearing about our firm for the very first time, Trenchard Partners is a Lagos-based full service commercial law firm, with its strengths lying in corporate and commercial law, commercial litigation and alternative dispute resolution. We have put this publication together for the enlightenment and entertainment of our readers. We hope you find the information here useful and look forward to receiving your feedback on the format and contents of our newsletter.

THE GROWING NEED FOR A DATA PROTECTION LAW

The Nigerian Communications Commission (NCC) at the end of 2009 issued a directive mandating mobile operators to register SIM cards prior to activation. The telecoms operators have cited many reasons not to proceed with the scheme, including the high cost of any such exercise and the likely aversion of subscribers to SIM registration. However, the NCC has stated that the measure will be useful in the prevention and the prosecution of crime, and the compilation of a national database. This article articulates other reasons which suggest that further thought needed to have been given to the matter before a directive was issued.

The question that immediately came to mind was that of data protection and what measures, if any had been taken to protect subscribers' privacy. Anyone who has ever filled a form in, for example, the UK requiring the entry of personal information will confirm that such forms, regardless of the

nature of the business of the data collector, contain a statement of the data protection policy of the company and informs the person providing the information of the limits within which the personal data can be used.

Unlike the UK, Nigeria does not have a Data Protection and Privacy Act. However, embedded in the Schedule to the Consumer Code of Practice Regulations 2007, are provisions relating to data protection. The relevant sections of the NCC regulations (ss. 34-38 of the Schedule) adopt the basic principles of data protection, as follows: "...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."

Currently, SIM registration requires the subscriber's photograph and fingerprints to be taken in addition to the name and address of said subscriber. If data collected is meant to be relevant and not excessive, one must surely question the relevance of biometric information (particularly, fingerprints) to a subscriber directory. Given the garb of crime prevention with which the exercise has been cloaked, is it the intention of the NCC for such details to be handed over to the law enforcement agencies? I suspect that the response of the average reader would be that if the writer is not a law-breaker, then he should have nothing to fear. However, section 37 of the 1999 Constitution of Nigeria guarantees the right to privacy of Nigerian citizens. Furthermore, there are no obligations on any non-telecoms operator (e.g. the Nigerian Police or the State Security Service) to deal with personal data according to the same

standards as the telecoms companies. Again, as the NCC initially proposed a uniform gatherer of this information, who is the custodian of the personal information taken from subscribers? The NCC or the telecoms companies?

The relevance of biometric data to SIM card registration must also be questioned. Surely, a subscriber's name and address should be sufficient information for registration. Is the requirement that subscribers have their photographs and thumb-prints taken not excessive?

Sub-paragraph (h) of the regulations should also give subscribers cause for concern. It provides to the effect that a subscriber's personal data may only be transferred to other parties in accordance with the terms and conditions agreed with the customer or otherwise permitted by law. The registration form that subscribers are required to complete for the SIM registration exercise (I have been to two of such centres) do not contain any terms and conditions upon which personal data is being processed. Neither of the terms and conditions displayed on the websites of either of these two companies have any terms pertinent to the collection and maintenance of subscriber data. This is notwithstanding the fact that section 37(1) of the Commission's guidelines requires each operator's policy on the protection of consumer information to be made available in an accessible and easy to read manner. The question is also relevant whether authorities, who are permitted by their enabling laws to enter into premises and seize documents, can lawfully seize the devices on which subscriber records are stored. Normally, these agencies would require warrants to search and seize. Under what circumstances

would they be able to obtain biometric data of suspects? Only when the suspects' telephone records are relevant? Or at any time at all?

One must also examine other companies and organisations that collect and process data. This sub-set would include banks, stockbrokers, utilities companies (e.g. PHCN, Water Boards), the Immigrations Service, the Federal Road Safety Corps and even, one might argue, embassies. Every one of these companies now has an 'e-resolution' to their companies' products and services. The question is not how likely it is for these entities to share our personal information with third parties but rather, whether such a possibility exists, and what the ramifications would be if they did. Apart from sharing our personal data, if it is proved that personal data has been misplaced or dealt with negligently by a custodian to whom we as consumers have provided this information, what should the consequences be? There have been adverts in newspapers by some cable television companies advertising direct debit as a means of payment. Direct debit would require the subscriber to entrust his bank details to the broadcaster. Should there not be a minimum legal standard for the handling of such information?

Recently, social networking website Facebook came under fire from many of its users because its privacy settings stopped working as they were designed to. Ordinarily, particulars of and updates to a user's profile should only be visible to other users designated as 'friends'. However, due to a glitch, these restrictions temporarily failed to work, removing the restrictions to users' personal information and communications. The incident left many users weighing the usefulness of the network

against the security of their privacy and many users considered this such a grievous breach that they stopped using the website altogether. The rationale for this was quite clear – a website can no longer be trusted if communications and information that were meant and believed to be private and confidential turned out to be the opposite. Likewise, there was a huge public outcry when British civil servants misplaced flash drives where details of millions of British residents were stored, as well as when the British Government lost a truckload of brand new passport booklets. We live in an era when access to personal data provides ample opportunity for identity theft and if this concerns residents in countries where law enforcement has the technological wherewithal to combat electronic theft, it should most certainly concern residents of such a country as ours.

It is our suggestion that the SIM registration directive is premature, because the telecoms operators do not exist in a vacuum. They interact and transact business with various companies and it is not inconceivable that some of these companies may come into contact with the data gathered by the telecoms companies. As long as there is no statutory obligation on these third parties to treat subscriber's personal data with the same standard required of telecoms companies, the system is inherently compromised. The National Assembly needs to enact a law regulating the protection of data gathered by service providers. Failure to do this, instead of helping to stop crime, could lead to the next generation of cybercrime and identity theft. For the system to work properly, all gathering and potential sharing of personal data must be regulated.

Our government and its agencies must also adopt a broader approach as they seek to modernise and keep up with current trends. Privatisation and deregulation are laudable, but everywhere else in the world,

they are accompanied by competition/antitrust laws. The NCC does have competition regulations, but competition/antitrust issues are certainly not the exclusive preserve of telecoms companies.

Likewise, telecoms companies are not the only bodies required to register customers, and the attendant privacy and data protection issues must be addressed.

COMPETITION LAW IN NIGERIA

The scope of competition regulation in Nigeria is currently limited to the context of sector-specific mergers or acquisitions. For example, the Central Bank of Nigeria (CBN) is empowered to refuse to permit the merger of two or more banks if it is of the opinion that competition in the sector will be adversely affected. The same goes for companies under the regulatory review of the Securities and Exchange Commission (SEC) and the Nigerian Communications Commission (NCC). While this is a useful and arguably necessary power for regulators to have, the reality is that competition issues extend far beyond business combinations and the economy will benefit from numerous advantages that competition law imbues until a full-fledged competition commission is established.

This issue will increase in its importance as the government continues its privatisation and deregulation programmes. In fact, one of the key concerns of government as it privatises its industries should be that state-owned monopolies are not simply being converted to privately owned ones. In *Salink/B&I Holyhead: Interim Measures* [1992] 5 C.M.L.R. 255, the European Court of Justice prevented a port concessionaire from altering the docking time-table solely to suit its fleet (to the detriment of other port users). The court ruled that the attempt by the concessionaire amounted to uncompetitive behaviour because 'a company which has a dominant position in the provision of facilities which are essential for the supply of goods and services on another market abuses its dominant position if, without objective justification, it refuses access to these facilities.' At present there is no similar framework in Nigeria to protect users of privatised government infrastructure from such discriminatory practices.

In the face of deregulation, the public also has to be protected against cartelisation. As things currently stand, with regard to the proposed deregulation of the petroleum industry, nothing prevents marketers

from forming a 'club' and agreeing on the prices that they will jointly levy. Nothing prevents them from agreeing to grant each other exclusive operating rights in the different regions of the Nigerian market. In almost all jurisdictions with a competition law, these practices are respectively known as cartelisation, price-fixing and market division, each one punishable by a very large fine. For example, in 2007, Virgin Atlantic and British Airways were fined £270 million after admitting collusion in fixing the prices of fuel surcharges.

It must be pointed out that cartelisation should not only be punishable when committed by large companies. Small-scale providers of goods and services like barbers and bakers should be able to price their goods as competitively as they wish. In practice, they have no choice but to belong to umbrella associations who set prices and sanction any seller or service provider who sells below the set price.

Again, as the law currently stands, nothing prevents, for example, a dominant producer or importer of grain or sugar from selling his goods below cost price in a bid to squeeze out a new participant in the market. Most competition laws would prohibit this as uncompetitive behaviour because, apart from closing the market to new entrants, the dominant producer would simply recoup his losses by raising the price of his commodity after the squeeze-out is achieved.

Competition regulation is sometimes criticised for punishing innovation. However this criticism is frequently misconceived. A market should not be the exclusive preserve of any party simply because they 'got there first'. If market participants are guaranteed a fair market, free of uncompetitive behaviour, and the market forces of demand and supply are allowed to operate without manipulation, the consumer will be the ultimate beneficiary. This will happen because goods and services will be priced reasonably and providers will improve the quality of their goods and

services, to achieve distinction in the market and increase their market share.

In order for a competition regulator to function effectively, however, certain factors must exist to complement it. For one, the regulator will need to have reliable statistics and market data for its analysis. Information gathering and ready disclosure of information are not qualities for which Nigeria is best known.

Additionally, there must also be the political will to allow the regulator the required independence it needs. While any competition regulator would ostensibly report to the Ministry of Commerce, the Chairman of the Commission must be given the freedom to operate independently of the Minister. This again is an issue that the Nigerian Federal

Executive continues to grapple with, as was evident in the recent cases of the Ministry of Mines and Steel Development and the Mining Cadastral Office, and the Ministry of Information and the Nigerian Communications Commission.

The turnaround time for responding to petitions and complaints must also be kept to the barest minimum. If the company complaining of uncompetitive behaviour has already been successfully forced out of the market, any response from the regulator would be merely academic.

It is imperative that a competition regulator be established to address these issues to protect consumers and safeguard the growth of the economy.

Newsflash

Minister of Commerce and Industry approves upward review of fees payable in respect of intellectual property prosecution and enforcement, with effect from 1st September 2010. Official fees in many categories have been increased by up to 100%.



The Trenchard Partners Newsletter is a periodic publication of Trenchard Partners, a full-service commercial law firm based in Victoria Island, Lagos. To contact the firm, please send correspondence by post to *Trenchard Partners, 1607 Omega Bank Avenue, Victoria Island, Lagos* or rfawole@trenchardpartners.com.

DISCLAIMER: Please note that the information contained in this Newsletter is of a general nature, may not apply to any specific situation and should not be considered as legal advice. It is best to seek legal advice concerning your particular set of facts before taking any steps to address your situation.