Bring Your Own Device to Work: Balancing Workplace Confidentiality and Employees' Privacy

By

Brooks & Knights Legal Consultants[1]

1. Introduction

In the wake of the COVID-19 pandemic (the **pandemic**) and the attendant global economic slowdown, most businesses are now considering pragmatic measures to reduce overhead costs. Part of the measures being embraced include the BYOD scheme which also helps the employer save the funds earmarked for procuring hardware for employees. In addition, employees - owing to the current restriction of movement in major cities in Nigeria, for instance – now work from home. Businesses that utilise desktop computers and other immovable work devices prior to the lockdown are likely to find it difficult to operate remotely from home. Those businesses may have no choice but to resort to the BYOD scheme by allowing their employees to use their private laptops and phones to remotely execute work-related assignments, pending the time normal work schedule can resume. Also, employers that provide movable work devices like laptops and phones for their employees may be unable to remotely track employees' usage of their personal devices for work. Accordingly, the emergence of the pandemic has contributed to the perceived inevitability of the BYOD scheme in the world of work, and forward-thinking cum survival-seeking businesses are beginning to embrace the scheme.

However, the dark side of the BYOD scheme is that if not properly implemented and regulated, it could result in many issues including data breaches which may threaten the employer's IT security and possibly result in the infringement of the employee's privacy. This article considers the legality of such BYOD guidelines in Nigeria and their efficiency in curbing the inadequacies associated with the use of personal devices for work. The first section of the article explains the concept of BYOD, the second section explains workplace security issues that may result from the use of personal devices for work. The second section discusses how the implementation of the BYOD scheme may violate an employee's privacy. The third section considers the position of the Nigerian courts on the waiver of constitutional rights with a view to determining whether an employee's right to privacy can be waived when implementing the BYOD scheme.

2. The Concept of BYOD

Bring Your Own Device to Work (**BYOD**) is a growing concept in the world of

[1] **Brooks & Knights Legal Consultants (BKLC)** is a law firm established in Lagos, Nigeria to provide bespoke legal advisory and policy consulting services to individuals, corporates, government agencies and NGOs. BKLC consultants are qualified attorneys in their chosen fields of expertise.

work. With rapid improvements in technological trends, businesses experience difficulty expanding their recurrent expenditure in keeping up with yearly technological innovations. This struggle has culminated in the consumerisation of information technology (**IT**) as most employees prefer to execute work-related assignments on their personal devices, which are usually in tune with the most recent technology. Interestingly, millennials constitute the largest percentage of the global workforce. Millennials consider personal devices extensions of their lives and being able to achieve work-life integration through the use of personal devices increases job satisfaction and productivity. Thus, it is becoming almost impossible for employers to prevent their employees from using their personal devices for work, even in circumstances where employers provide work devices. Consequently, BYOD guidelines are usually implemented in the workplace in protecting the employer's confidential information and the employee's privacy.

3. BYOD, Workplace Confidentiality/ Security and Data Protection

Notwithstanding the fact that most employers do not constantly keep up with the use of the latest technological devices for work, they also do not implement state-of-the-art IT security measures in ensuring that work-issued devices are properly encrypted to prevent data leakages in the event those devices are lost or stolen. Conversely, personal devices which are most times state-of the-art usually lack adequate data encryption and as such, are more susceptible to data breaches. Where such unencrypted personal devices are allowed to access the employer's corporate network, this could result in the possibility of a data breach which could cost the employer financially. Consider a situation where an employee's unencrypted personal device contains corporate information and such device is stolen, this would definitely give the culprit unhindered access to the employer's confidential information and may constitute a breach of data protection regulations.

In 2012, an employee of Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc (**Massachusetts Hospital** or the **Hospital**), without the prior approval of the Hospital, loaded his unencrypted personal laptop with sensitive health information of some patients of the Hospital. The laptop was subsequently stolen and the culprit gained access to the confidential health information of the patients of the Hospital. As a result, the Hospital paid the U.S. Department of Health and Human Services $1.5 million to prevent charges under the Health Insurance Portability and Accountability Act.

The above incident would have certainly constituted a breach of the Nigerian Data Protection Regulation, 2019 (the **Regulation**). One of the objectives of the Regulation is to safeguard the privacy of natural persons to data privacy. Health information of a data subject qualifies as "sensitive personal data" under the Regulation. The health

information of data subjects under the Regulation are only meant for lawful processing and cannot be given out to third parties without the consent of the data subjects. The Regulation mandates data controllers like Massachusetts Hospital to secure the patients' data against all "foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind". Since Massachusetts Hospital is vicariously liable for the acts of its employees, it would be in breach of the Regulation owing to the thief's unlawful access to the health information of its patients.

In addition to the data breaches that may occur through lost or stolen personal devices containing employer's confidential information, employees generally use their personal devices for social purposes like accessing unsecure websites, uploading pictures and other contents. They may in the process unintentionally get their devices infected with viruses or malware. Where such devices are connected to the employer's network, the viruses or malware may be introduced into the employer's network thereby creating a backdoor for data leakage. Hence, data leakage is a major issue associated with the BYOD scheme as far as the employer is concerned.

4. BYOD and Privacy Issues

Where an employee who uses his personal device for work is under investigation and the employer needs to retrieve some corporate information from the employee's device, the employer may need to conduct a forensic analysis of the device. It would be extremely difficult if not impossible to distinguish between the employee's personal information and the employer's corporate information on the employee's personal device as both information would have commingled. The employer may therefore in the process of the forensic analysis access the employee's sensitive personal information thereby infringing the employee's right to privacy.

To circumvent this infringement, an arrangement that is gaining favour with employers is the implementation of BYOD guidelines. This usually entails the use of a Mobile Device Management (**MDM**) system which is a way of separating the employee's personal information and the employer's corporate information on the employee's personal device using a virtual partition. Once the MDM software is installed on the employee's personal device, the employer's administrator will be able to remotely access the employer's corporate information on the employee's personal device. Nevertheless, this could also result in the infringement of the employee's privacy as the employee may be unable to know what or how much information the employer's IT administrator collects from his or her personal device. Once the MDM software is installed on the employee's device, the employer's administrator could, despite the partition, remotely read the employee's text messages, check browsing history, wipe the employee's device and determine the employee's location in real-time.

5. Legal Issues/ Waiver of Employee's Right to Privacy

As indicated above, the installation of an MDM software on an employee's personal device may give an employer access to the employee's personal information even though its essence is simply to give the employer access to its corporate information on its employee's personal device. For effective utilisation of the BYOD scheme, the employee must as a condition waive his right to privacy. This waiver of right to privacy expresses the voluntariness of the scheme and precludes an employee from maintaining an action against the employer for breach of right to privacy in circumstances where the employer intentionally or accidentally accesses the employee's personal information on his personal device.

The legality of the waiver of an employee's right to privacy may be in issue in view of the position of Nigeria's appellate courts on whether the right of privacy - a constitutional right – can be waived. In the case of ***Ariori v Elemo (1983) LPELR-552(SC)***, the Supreme Court held that where a right is conferred by the Constitution, a waiver of such right is dependent on whether same is conferred solely for the benefit of an individual or where same involves public interest. Where public interest is involved, it becomes a right that cannot be waived. Since the right to privacy appears to be a right solely conferred for the benefit of an individual, it could be argued that it is a right that can be waived. This makes the implementation of the BYOD scheme legal.

However, Justice Ogunwumiji, JCA (as she then was) in the case of ***Okafor v Ntoka (2017) LPELR-42794(CA)*** held that the right to privacy guaranteed by Section 37 of the Constitution is a fundamental right that cannot be waived except for the derogations in Section 45 of the Constitution. This position of the Court of Appeal on the inalienability of the right of privacy puts the legality of the BYOD scheme in issue since a successful implementation of the scheme is contingent on the waiver of an employee's right of privacy. By the doctrine of *stare decisis*, the Court of Appeal is bound by the decision of the Supreme Court. In ***Okafor's case***, no reference was made to ***Ariori's case***. It may thus be argued that the decision of the Court of Appeal on this point was arrived at *per incuriam*. However, in the case of ***NNPC v Nwodo (2018) LPELR-45872(CA)***, the Court of Appeal relied on the decision in ***Ariori v Elemo*** in arriving at the finding that a person can waive a right conferred upon him by a statute where the right is for his sole benefit and the state has no interest. Where the state has an interest in the matter in the sense that public policy is involved, such a right cannot be waived. The implication of this decision, which reflects the Supreme Court's position, is that the right to privacy, being a right that confers a sole benefit, can be waived. Thus, it can be fairly concluded that the implementation of BYOD guidelines (premised on waiver of employee's right to privacy) in Nigeria is legal.

6. **Conclusion**

While an employer may achieve a reasonable level of control over its corporate information on an employee's personal device by implementing BYOD guidelines, the employee's privacy is not adequately protected by the scheme. In fact, the scheme requires an employee to waive his right to privacy. This puts the workability of the scheme in Nigeria in issue as it may be difficult for employees to allow employers install MDM software on their personal devices. We propose that employers should continue to provide tools of work for their employees especially portable devices like laptop and mobile phones that serve the exigencies of today's world of work and protects the data of the employer and/or the client. This creates flexibility and may also improve the productivity of employees so they may work from anywhere and at any time. Upon the cessation of the employment contract, the employee is obligated under the Section 31 of the Cybercrime (Prohibition Prevention ETC) Act, 2015 to relinquish all codes and access rights to work-issued devices and the employer's corporate network.

To achieve strict compliance with the use of only work-issued devices, the employer can (a) impose stringent penalties for the use of personal devices to work, (b) allow only registered devices to access the corporate network, (c) maintain a central server where all corporate information are stored, (d) create a BYOD policy mandating employees to submit their personal devices for investigation where it is established that such devices were used for work.

Employees, on the other hand, must bear in mind that once they make the decision to use their personal devices for work, they must be ready to allow their employers access such devices. While employers should continue to provide tools of work for their employees as the primary mode of work, BYOD guidelines should also be implemented to compel the use of work-issued devices as employees are not ready to face the undesired consequences associated with the implementation of the BYOD scheme.