Blowing the Whistle and the Unlawful Interception of Information

In a bid to unravel cases of fraud and financial misappropriation, the whistleblowing policy of the Nigerian government may have opened up a debate regarding the extent to which information obtained through unlawful interception can legally be tendered in evidence. The policy, which is aimed at enabling the government obtain useful information on the violation of financial regulations, mismanagement of public funds, financial malpractices and discovery of concealed funds, revolves around the submission of factual information by citizens to law enforcement agencies (LEA), who then utilize the information in their investigations and prosecutions. By its nature, an aspect of whistle blowing involves some level of unauthorized interception of information (for example, covert investigation of financial fraud in an institution). Furthermore, since the act requires no judicial or police warrants, it is typically undertaken by ordinary citizens who sometimes are motivated by the reward of their whistle blowing activities.

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 refers to unlawful interception as the intentional and unauthorized interception of private data or content from a computer system or network by a person¹ with the use of technical means. The

¹Since the Act appears to make a distinction between private person and corporations on the one hand and LEAs on the other hand, we take the view that the Act is primarily targeted at curbing the cracking activities of private persons and not LEAs, who often covered by exemptions regarding national security and protection of public peace and order.
offence is punishable by 2 years imprisonment or a maximum fine of N5 million or both². While no judicial interpretation of this section of the Act yet exists, it is possible to identify instances that will qualify as unlawful interception. For example, getting hold of an unread email or a WhatsApp message that is intended for another recipient will reasonably qualify as unlawful interception. An Internet service provider’s interception of data (e.g. peer-to-peer files) sent by an Internet user to another using deep packet inspection techniques is an obvious instance of unlawful interception. In the same vein, workplace surveillance or other forms of surveillance can amount to unlawful interception, since the nature of surveillance necessitates intrusion into the private space of individuals and monitoring at will (except where there is consent to the surveillance by the surveilled party).

In whistle blowing, the central question is the balance of interests at stake, which interests have an effect on the security, freedom and liberty of Nigeria. In one category, the security of information requires that information should only be obtained through lawful means, otherwise unlawful access could threaten the security of a nation. In a second category, the protection of the privacy of citizens allows citizens to conduct their affairs privately and away from the preening eyes of the public. By implication, an invasion of privacy (even through the act of whistle blowing) must necessarily be authorized by law, otherwise this fundamental right is threatened. In a third category, the need for criminal prosecution and dispensation of justice requires that concrete evidence is presented that can avail a finding of guilt. Without this assemblage of credible evidence, the administration of criminal justice in a society falls apart.

The foregoing rights do not however exist in a vacuum, and the determination of the balance of interests is more fluid, as in a spectrum, than static. The Evidence Act, 2011 specifically provides that improperly obtained evidence through contravention of a law is admissible except where the court is of the opinion that the desirability of admitting the evidence is outweighed by the undesirability of admitting such evidence³. In Onyuike⁴, the Court of Appeal upheld the principle of admissibility of improperly obtained evidence, stating that the test to be applied in determining the admissibility of evidence is relevancy to the matters in issue. It opined that the illegality (if any) may only attach to the person who obtained evidence illegally or improperly⁵; and that no general rule exists wherein relevant evidence is excluded merely by the way in which it has been obtained. The judge is however at liberty to exclude evidence, where the interest of justice demands it, and upon considering the circumstances of its discovery and production⁶. In Sunday John⁷, the court highlighted the gravity of the contravention as a guiding factor in the exercise of the court’s discretion to exclude illegally obtained evidence.

We posit that beyond this factor, the courts should also consider the nature of the privacy violation, particularly in joint criminal-liability cases arising by way of misappropriation and negligence. For example, criminal information obtained through

²Section 12(1) of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
³Section 14 of the Evidence Act, 2011.
⁴Onyuike v. The People of Lagos State & Ors (2013) LPELR-24809(CA).
⁵(although not within the scope of the present discussion, the implication is that the individual will be criminally liable under the Cybercrimes Act, notwithstanding his whistleblowing activity).
⁶Onyuike v The People of Lagos State; See also, Sadau & Anor v. The State (1968) ANLR 125; Ukachukwu v. UBA (2006) All FWLR (Pt. 300) 1736 @ 1755 – 56.
unlawful interception of communication over a network between a client, his banker, a financial beneficiary, an escrow agent and a lawyer should not be deemed admissible, notwithstanding that it incriminates one or more of the parties. In this scenario, the protection of the privacy of the individuals should be of more importance to public policy considerations than the criminal prosecution based on evidence obtained illegally. This is because a violation of privacy in the manner indicated herein may lead to continual erosion of the boundaries of private sphere as well as unwarranted intrusion by the state (either through LEAs or private citizens). This will in turn create a surveillance state where no actual privacy exists.

The whistleblowing policy is undoubtedly geared towards the public good, and should be commended for the level of transparency and accountability that it has engendered in the country. However, it requires clear parameters concerning obtaining evidence through unlawful interception. Without these parameters, there is the likelihood that the policy will be subjected to abuse and could potentially undermine the cybersecurity infrastructure in Nigeria. In the era of digital and electronic banking, access to confidential and private information is made easier due to the viral nature of the Internet and associated technologies. The more reason why the balance of interest should sometimes be in favour of security of information and protection of privacy, particularly in the online environment, and notwithstanding the default provisions of section 14 of the Evidence Act.
The Corporate & Commercial Group (CCG) is one of the 6 practice groups of Aina Blankson LP. Renowned for its bespoke commercial work and ability to lead and manage complex transactional processes, the cutting edge results that have been achieved in the two decades of our existence, attests to the leadership position of the Firm in the corporate world.

Rated as one of the top commercial practices in Nigeria, the CCG provides services which range from corporate structuring, capital markets and capital raise to private equity, mergers and acquisitions. To us at CCG, transaction success requires not only legal skills, but also commercial sophistication, customized solution and efficient project management.

This Newsletter was written by Banji Adenusi and Daphne Ekpe and engaged in the Corporate & Commercial Group, Aina Blankson, LP.

Corporate & Commercial Group
Aina Blankson LP
5/7 Ademola Street
South-West Ikoyi
Lagos
Tel: +234 1 8980882-3
Fax: +234 1 2710566
E-mail: publications@ainablankson.com
www.ainablankson.com

Disclaimer: This document serves merely as a note and is not intended to provide legal advice to any person or group of persons whether natural or corporate regarding the issues discussed herein. All persons desirous of legal advice should therefore contact a lawyer. Aina Blankson LP shall not be liable for any breach or loss resulting from reliance on any part of this Bulletin.