Revisiting the Cybercrimes (Prohibition, Prevention, etc.) Act 2015

Ugochukwu Obi, Omolade Afonja and Ubong Ene

Introduction.

Before the *Cybercrimes (Prohibition, Prevention, etc.) Act 2015 ("the Act")* was enacted, Nigerian law enforcement and prosecutors were hamstrung in prosecuting cybercrimes, due to inherent limitations in 'prior era' legislation like the *Economic and Financial Crime Commission (Establishment) Act 2004*. The EFCC Act could not cater for prevention of threats to communication system and digital crimes. In the wake of increasing digitalization, the need for responsive legislative initiatives to deter ingenious cybercrimes became painfully evident. Hence, the Act. This article reviews the Act, and highlights areas of improvements through legislative amendment.

The Act.

Since the Act became law almost a decade ago, technology's disruptive influence in everyday life and business has remained pervasive. Technologies like the Internet of Things (IoT), Cloud Computing, Blockchain, Machine Learning and Artificial Intelligence, have become fairly commonplace. These emerging technologies have not been without significant baggage, by way of complex and sophisticated cybercrimes.

The Act aims to provide a unified legal and regulatory framework for preventing, prosecuting, and punishing cybercrimes; protecting critical national information infrastructure; promoting cyber security; and protecting computer systems and networks, electronic communications, etc. Notwithstanding ingenious misapplications of technology, the Act with its wide definition of terms and longsightedness has done an impressive job of keeping pace with modern realities. The rise of deepfakes offers a vivid example.

Artificial Intelligence (AI) has enabled the uncanny impersonation of people's images and voices. In the era of deeply divisive politics and rampant personal insecurity due to the scourge of kidnappers, the scope for political and criminal misapplications of this technology are astounding. These crimes can easily be situated within the Act; this, despite the Act preceding the global proliferation of deepfake tech by several years. The Act criminalizes fraudulent impersonation of another person to gain advantage, obtain property, or cause disadvantage to the person being impersonated or another person.[1] Despite the Act's seeming prescience, there is much that can yet be improved.

Strengthening the Act Through Legislative Amendments.

1. **Devolving the Regime for Protecting and administering Critical National Information Infrastructure (CNII).**

   Perhaps a major weakness of the Act is its overt focus on other areas of cybercrimes to the inadvertent neglect of a core objective - protecting CNII.

   Section 7.5(ii) of the National Cybersecurity Policy (2014) identified 15 sectors as critical infrastructure sectors; including communications, government facilities, defence, and

[1] Section 22(3c) of the Act.

financial services.[2] The Act, however, only mentions that the President is to designate certain systems as CNII. So, by implication, CNII can be found in each of the preceding areas. Any attack on, interference with, or destruction of any of these would not only potentially cripple the industry, but also affect national and economic security, or public health and safety. Cases in point are the 2015 hackings of the Independent National Electoral Commission (INEC)[3] and Defence[4] websites.

Considering the multiple sectors that comprise critical infrastructure, it is necessary to devolve administering the legal frameworks for their protection, to sectoral regulators. For instance, regulators like the Nigerian Communications Commission (NCC) and Central Bank of Nigeria (CBN) -each in collaboration with the National Security Adviser (NSA) – are in better positions to formulate sector focused regulations and administer their provisions in the context of CNII. Since these regulators engage directly with stakeholders in their industries, such oversight would significantly bolster their ability to detect, prevent, and resolve cyberattacks or interference of any sort; and even physical attacks such as sabotage or vandalism within their respective sectors.

2. Clarifying the National Cybersecurity Fund Levy

The Act creates the Cyber Security Fund and applies a "0.005" levy to all electronic transactions of GSM and telecommunications service providers, banks and other financial institutions, internet service providers, insurance companies, and the Nigeria Stock Exchange.[5] However, this provision is vague as it is unclear what "0.005" means; whether it is a percentage of the transaction, profit, or income. The Act also offers no indication of what the Fund is to be used for; save for the fact that no more than 40% of it is to be allocated for programs relating to countering violent extremism. This opens wide the door for possible misappropriation of the Funds at worst, or a lack of transparency at best.

3. Structural efficiency in administration

The Act is a radical, but apparently structurally deficient piece of legislation. It is surprising that the Office of the National Security Adviser (NSA) responsible (together with the Office of Attorney-General of the Federation) for coordinating the enforcement of the Act's provisions through an Advisory Council, is not itself a member of that Advisory Council.

---

[2] These sectors are Communications, Government Facilities, Manufacturing, Dams, Defence, Chemical (Oil & Gas), Power & Energy, Commercial Facilities, Financial Services, Food & Agriculture, Emergency Services, Transportation Systems, Public Health & Healthcare, Water & Wastewater Systems, and Information Technology.

[3] https://dailypost.ng/2015/03/28/breaking-nigeria-decides-inecs-website-hacked/. Accessed last on August 15, 2023 at 8:14 a.m.

[4] https://www.thecable.ng/hackers-deface-website-nigerian-military. Accessed last on August 15, 2023 at 8:16 a.m.

[5] Combined reading of Section 44(2a) and Second Schedule of the Act.

4. **More Extensive Definition of Certain Terms**

The Act adopts a wide approach to defining terms, thereby enabling modern technological changes to be accommodated. In certain other instances however, certain definitions are too specific and may give room for offenders to devise other means of committing crimes outside those prescriptive definitions. For instance, the Act penalizes the offence of committing a crime with an ATM or POS machine. While this speaks to payment devices that are currently prevalent within the financial industry, these provisions may become obsolete when the country expands beyond the use of these two platforms. It is therefore critically important for tech-focused legislation in particular, to anticipate technological advancements, and couch relevant provisions in terms that could apply to matters in the same or similar categories as those which currently exist.

5. **Imposing the Duty to Secure**

The Act pays (and necessarily so) attention to unauthorized interference and access to computer systems. However, it must also impose on owners/controllers of critical infrastructure and others affecting the public, the active duty to protect or secure their networks. Although, this duty to protect is recognized in the *Nigerian Data Protection Act 2023 (DPA),*[6] the DPA is restricted to personal data. The DPA's reference to the duty to protect however lends credence to the need to include same in the Act in relation to general cybersecurity. Again, the level of duty is best imposed by sectoral regulators.

6. **Criminalizing Possession of Illegally Obtained Data/Information**

The Act creates the offence of intentionally hiding or detaining emails, messages, electronic payment, credit/debit card found by or delivered in error to a person who is an employee or under the authority of a government or private organization.[7] But beyond this, is the need to also criminalize the possession, by any person, of illegally obtained data or information. This means criminalizing the possession of data which could only have been obtained unlawfully even if there is no evidence of unlawful interference, or other active crime committed by the suspect.

7. **Enforcing the Act.**

Section 50(1)[8] of the Act provides for the jurisdiction of the Federal High Court if the crime is committed outside Nigeria under the following circumstances: (i) if the victim of the offence is a citizen or resident of Nigeria; or (ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution. However, this presents a lacuna that needs to be filled: the possibility that a crime may be committed by a non-Nigerian outside the country and without a victim. As such, it is advisable to extend the jurisdiction of the court where the target device is in Nigeria, irrespective of the existence of a victim.

Again, the Act creates a controversial provision which makes it possible for the court to make an order for the winding up of a body corporate (and its assets forfeited to the

[6] Sections 39 and 40 of the Data Protection Act 2023.
[7] Section 1(3) of the Act
[8] See section 50(1) for a full list of instances where the jurisdiction of the Federal High Court will be invoked.

Federal Government) found guilty of an offence under the Act.[9] This provision may discourage investment as it is made without any due regard to the rights of creditors and shareholders of such erring companies.

8. **Infringing Constitutional Rights to Freedom of Movement**.
Perhaps more serious is the provision of the Act's section 48(4) which provides that any individual who is convicted of an offence under the Act *"shall have his international passport cancelled"*. Now, it is understandable that the constitutional right of freedom of movement[10] is not absolute and can be forfeited under certain circumstances such as in the case of a criminal offence.[11] However, this provision poses certain risks in its application.

How long is this cancellation? It is doubtful that such cancellation is intended to be perpetual such that the convict can never subsequently be issued a passport. If cancellation is intended to be limited to the incarceration of the convict, this seems redundant since imprisonment works essentially to limit movement. Should it however be the intention of the draftsman to limit the application of this provision to cases in which the punishment is a fine, this would work to limit the freedom of movement of a convict for a crime where a fine would have sufficed. This provision also seems to contradict the Passport (Miscellaneous Provision) Act[12] which provides strictly for instances where passports can be cancelled.

9. **Revision of Punishment.**
This review would be incomplete complete without a review of punishments and fines prescribed under the Act. These are grossly inadequate to serve a deterrent function, by comparison to the gravity of the crimes created and potential losses suffered by the victims. Not only should the fines in criminal adjudication consider the foregoing but must also serve primarily as sufficient deterrent, commensurate with present economic realities.

For instance, a 1-year imprisonment or fine of ~~₦~~250,000 (or both) on a person convicted of intentionally hiding emails, messages, electronic payment, credit/debit card which is found by him or delivered to him in error, and which to his knowledge ought to be delivered to another person[13] seems grossly inadequate considering the nature and implication of the crime created. The same goes for the imposition of a fine of <u>not more than</u> ~~₦~~5 million or imprisonment of not more than 5 years (or both) on conviction of intentional accesses to a computer system or network for fraudulent purposes and containing data that are vital to national security.[14]

[9] Section 29(2a) of the Act
[10] See section 41(1) of the Nigerian Constitution of the Federal Republic of Nigeria (as amended). See also DSS V. Olisa Agbakoba (1999) 3 NWLR (Pt 595) 314
[11] Section 41(2a) of the Constitution of the Federal Republic of Nigeria (as Amended)
[12] Cap 343 LFN 1990 at section 5.
[13] Section 12(3) of the Act.
[14] Section 6.

Conclusion.
The Act extensively covers issues of cybersecurity even in relation to today's sophisticated cybercrimes. Nonetheless, there are several areas recommended for review, from administration to enforcement of the Act. Administratively, it is important to devolve the administration of the CNII, revisit the structure of the Cybercrime Advisory Council to include the NSA, and introduce clarity in the imposition and the administration of the Fund.

In addition, certain lacunae in the Act should be filled. These include extending the jurisdiction of the court on crimes committed outside Nigeria but targeted at devices within Nigeria, and criminalizing the possession of illegally obtained data. The Act should also provide more context and details to some potentially constitutionally infringing provisions that seek to cancel a convict's passport. Finally, the punishment for crimes must be revisited to ensure deterrence, commensurability with unlawful gains, and current economic realities.

A publication of the ICT team of Perchstone & Graeys LP.

Lagos: 1, Perchstone & Graeys Close, off Remi Olowude, Lekki Epe Expressway, Lagos; Tel: +234- 1-3429131, 7611051

Abuja: D3, Jima Plaza, 1627 Ahmadu Bello Way, Area 11, Garki Abuja; Tel: +234 92919191, 07045984792

Benin City: 40, Adesogbe Road, Benin City, Edo State; Tel: +234 70685186 50, 07045984776

Email: editor@perchstoneandgraeys.com; counsel@perchstoneandgraeys.com

Website: www.perchstoneandgraeys.com