The Reach and Impacts of the Cybercrime Act, 2015 on **Providers of ICT Services**

The Cybercrime (Prohibition, Prevention, etc.) Act, 2015 (the "Act") was enacted to provide a unified legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation, and prosecution of cybercrimes in Nigeria. The Act is a legislative response to the increasing rate of fraudulent activities in the cyberspace for which there had never been any specific statutory or regulatory regime in the country. The Act also reflects a positive legislative effort to ensure the protection of information which is vital to national security, by providing for the designation of computer systems or networks containing such information, as constituting Critical National Information Infrastructure. The Act also aims at protecting intellectual property and privacy rights in addition to the foregoing objectives.

The Act is a well-articulated effort to discourage some behavioural activities within the cyberspace by an outright legislative proscription. For example, behavioural patterns such as cyberstalking, cybersquatting, computer-related fraud and forgery, cyber terrorism and the likes, are prohibited and violations attract a wide range of sanctions, including monetary fines and terms of imprisonment under the Act.

Under the Act, the Cybercrime Advisory Council (the "Council") is established with the mandate to co-ordinate and work with existing law enforcement, security and intelligence agencies in the administration and enforcement of its provisions. The Act also imposes certain duties on persons and organisations in the Information Communication and Technology ("ICT") industry including online service providers[1] and financial institutions.

This newsletter considers the potential impact of the Act on the activities of ICT-related service providers.

Obligations and Potential Criminal Liabilities of Service Providers under the Act

The Act imposes certain obligations on service providers, the breach of which is punishable by various terms of imprisonment and/or fines. The foremost of these obligations is the duty to preserve information pertaining to traffic data[2] and subscriber information for a period of 2 years, and to disclose any such information as may be requested by any law enforcement agency.[3] A breach of this duty is punishable by a term of imprisonment of not more than 3 years, or a fine of not more than ₦7 Million, or both the fine and imprisonment.[4]

Another obligation imposed on service providers is the duty to assist law enforcement agencies in identifying, apprehending and prosecuting offenders; as well as, tracking and tracing proceeds of any offence or any property, equipment or device used in the commission of any offence.[5] Similarly, service providers are also obligated to support the relevant law enforcers in the performance of their duties of freezing, removal, erasure or cancellation of any services of an offender that enable the offender to commit the offence, hide or preserve the proceeds of any offence or any items used in the commission of the offence. It follows therefore, that if an offender subscribes to a particular product or service, say an email account or mobile phone network or a blog, uses such product or service to commit fraud or conceal proceeds of fraud, the product or service provider has a duty to assist the law enforcement agency in charge of investigating the crime.

[1] By section 50 of the Act, service provider means "any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and any other entity that processes or stores computer data on behalf of such communication service or users of such service."
[2] Traffic Data means any computer data relating to a communication by means of a computer system or network, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, data, size, duration, or type of underlying service.
[3] Section 38(1) and (2) of the Act.
[4] Section 38(6) of the Act.
[5] Section 40(2) of the Act.

Where a service provider is found to have failed to live up to these obligations, it faces penal sanctions in the nature of a fine of ₦10 Million, and if the service provider is a corporation, an additional punishment of a 3-year term of imprisonment or fine of ₦7 Million or both fine and imprisonment for any director, manager or officer of the service provider who is found complicit in the corporation's violation(s) of the law.

Furthermore, the Act imposes on service providers a compulsory reporting obligation regarding cyber threats to the effect that they shall inform the National Computer Emergency Response Team Coordination Centre ("NCERTCC") of any attacks, intrusions and any other disruptions that could affect or hinder the proper functioning of any computer system(s) or networks.[6] The NCERTCC is the body charged with protecting and securing the Nigerian cyberspace against threats, attacks, etc., and responding to requests for support against threats and attacks, etc., against information systems in the Nigerian cyberspace.[7] The obligation of service providers to report cyber threats is designed to aid the NCERTCC in the performance of its duties effectively. Where a service provider defaults on this obligation by failing to report any cyber threat or breach to the NCERTCC within 7 days of its occurrence, it faces the sanction of prohibition of access to, and use of, internet services, as well as a fine of ₦2 Million.

By the same token, section 39 of the Act which governs interception of electronic communication expressly provides that for a service provider to intercept electronic communication reasonably required for the purpose of a criminal investigation or proceeding, a court warrant must first be sought and obtained upon information on oath, supplied by the law enforcement agency concerned.

In keeping with the above statutory obligations, the service providers are simultaneously required to respect the constitutional rights of their subscribers or users of their products or services to privacy by not disclosing their private information unnecessarily. The same penal sanctions that follow a breach of the duty to preserve and/or disclose information will similarly apply to a service provider who violates an individual subscriber's right to privacy.[8]

The practical question that arises from the above is what should a service provider do in a situation where it is faced with this balancing requirement of the Act, i.e. the duty to disclose information of a subscriber who is being investigated on an allegation of a crime by a law enforcement authority and the duty to observe the privacy rights of such a subscriber under the Act? In other words, should a service provider comply once it receives a request from a law enforcement authority to disclose information relating to a subscriber who is under investigation? Or should the service provider decline on the basis that such disclosure would be inconsistent with the service provider's duty to preserve the subscriber's privacy rights? Or should the service provider insist that the request be

[6] Section 21(1) of the Act.
[7] See at: https://www2.cert.gov.ng/proactive-services.
[8] Section 38(6) of the Act

supported with a warrant[9] or an order of court?

It is pertinent to note that the Act does not provide any clear-cut guidance on the options available to the service provider regarding the issue. However, from a community reading of sections 38(4), 39 and 45 of the Act, it would seem fair to say realistically that where a service provider discloses a subscriber's information based on a warrant or an order of a court, the service provider may be excused from any potential liability for an allegation of violation of the subscriber's privacy rights that could arise[10]. Thus, any derogation from a subscriber's privacy rights may not be allowed or excused except as may be permitted by law. This view is consistent with one of the key objectives of the Act, which is the promotion of privacy rights of citizens under section 1 (b) of the Act.

Other Provisions of the Act that Service Providers must be Wary of

Quite apart from the duties of service providers identified above, the Act also criminalises a number of conducts commonly associated with service providers in the ordinary course of their businesses. Service providers may become liable for these crimes either on the basis of the roles carried out directly from their routine business activities or from the conducts or activities of their employees and other agents.

Such other offences created by the Act include the following: (i) unlawful access to a computer system or network with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information; (ii) intentional use of any device to avoid detection or prevent identification or attribution with the act or omission while committing an offence; (iii) unlawful interference with the functioning of a computer system; (iv) frauds committed using computer systems or networks; (v) phishing[11], spamming, and spreading of computer virus; (vi) unlawfully accessing a computer or computer system or network, or granting another person access to a computer or computer system or network, for the purpose of terrorism (vii) cyberstalking;[12] (viii) cybersquatting,[13] etc.

---

9 See for example, section 39 of the Act which provides that a court warrant must be first obtained, upon information on oath supplied by the law enforcement agency, before a service provider may perform its duty to intercept electronic communication.

10 In any case, it is important to bear in mind that the right to privacy is not absolute. The Constitution of the Federal Republic of Nigeria, 1999 (as amended) under section 45 envisages scenarios where possible derogation from privacy right could be lawfully allowed. Such scenarios will include but not limited to, derogations or limitations made in the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedom of other persons. It thus follows that where a request made on a service provider without a corresponding warrant or order of court in any of the foregoing or related circumstances, may not be lawfully excused and a service provider who complied with such a request is likely to have a good defence to any potential issue of violation of privacy rights.

11 Phishing is described under the Act as: the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e-mails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his identity so that such information can later be used to defraud the user.

12 A course of conduct directed at a specific person that would cause a reasonable person to feel fear.

13 The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, particularly

The punishment for these offences include both fines (a minimum of ₦2 Million) and terms of imprisonment ranging from 2 years to life imprisonment.

Interface of Service Providers with the Administrators of the Act

As previously mentioned, the administration and enforcement of the Act is vested primarily in the Council. However, other regulatory and law enforcement agencies such as the Office of the Attorney-General of the Federation, the Court, the Nigerian Communications Commission, and the office of the National Security Adviser to the President have express obligations under the Act to liaise with the Council in the enforcement of the Act. Similarly, other law enforcement agencies such as the Nigerian Police Force, the Economic and Financial Crimes Commission, and the Independent Corrupt Practices and Other Related Offences Commission, etc. are required to be involved in the daily enforcement of the provisions of the Act under the laws creating the respective agencies.

The process of the administration and enforcement of the Act by these agencies and institutions would necessitate their interacting with service providers on a daily basis. This underscores the need for service providers to familiarise themselves with the provisions of the Act and the role of these agencies and institutions.

How the International Outlook on the Enforcement of the Act may Impact Service Providers

The offences created by the Act extend to acts and omissions occurring outside of Nigeria provided that there is a Nigerian connection, no matter how slight. Hence, the Nigerian Court would have jurisdiction to try offenders where the offence was committed outside of Nigeria by a Nigerian citizen or resident of Nigeria outside of Nigeria if the person's conduct would also constitute an offence under the law of the country where the conduct occurred. By the same token, where the victim of the conduct occurring outside of Nigeria is a citizen or resident of Nigeria, or where the alleged offender is in Nigeria and has not been extradited to any country for prosecution for the offence, the offender may be tried in Nigeria under the Act.[14] It is worth noting that the Act appears to be the only criminal statute in Nigeria which expressly provides for the extraterritorial application of its provisions.

International Mutual Assistance & Collaboration

The Act further creates a framework for international mutual legal assistance.[15] It provides that the Attorney-General of the Federation may request or receive assistance from or conduct a joint investigation with any agency or authority of a foreign country for the purpose of detection, prevention or prosecution of offences under the Act. This mutual

where the domain name is similar or identical to an existing trademark or anyway similar with the name of a person other than the registrant.

[14] Section 50(1) of the Act.
[15] Section 52 of the Act.

assistance may be undertaken with a foreign country regardless of whether there is a subsisting bilateral or multilateral agreement between Nigeria and that country.

To further bolster this mutual international assistance, the Act renders admissible for proof of the commission of an offence under the Act, authenticated evidence obtained from an investigation conducted abroad or in a proceeding before a foreign court.[16] Such evidence obtained abroad can be requested from the foreign country by a Nigerian law enforcement agency.[17]

What the foregoing implies is that foreign service providers who have business presence in Nigeria or whose conducts affect any one of the over 190 Million Nigerian citizens or residents could trigger the criminal jurisdiction of the appropriate Nigerian court and be tried under the country's municipal judicial system. Similarly, the Nigerian State as the prosecutor, could source evidentiary proof in support of a criminal charge under the Act through international cooperation which could be acceptable proof of an offence against a foreign service provider in Nigeria.

Conclusion

In our view, the Act is a welcome instance of legislative response to the dynamic and progressive nature of the human society and the ubiquity of modern day technology. It is a well thought out reaction to the rising tide of cybercrimes in Nigeria as well as some conducts occurring outside of Nigeria in-so-far as such conducts have some level of connection, no matter how slight, with Nigeria.

Although there is as yet a dearth of reported cases of successful enforcements or completed prosecutions for offences under the Act, it is hoped that the enforcement of the Act would make the cyberspace more secure and at the same time limit potential cyber-related impediments to the ease of doing business in Nigeria.

As has been shown from this expose, the enactment of the Act has increased compliance risks on the part of ICT service providers, hence the need for ICT service providers to not only get familiar with their obligations and potential exposures under the Act to ensure they are in compliance at all times, but also for raising the stakes for businesses within the crosshairs of the law by setting up policies and processes to address such risks.

[16] Section 53(1) of the Act.

[17] Section 54 the Act.

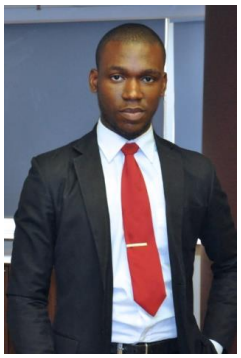
Contacts:

Sadiq Ilegieuno
Partner

sadiku.ilegieuno@templars-law.com
+234 (1) 4611890

Jacob Obi
Associate

jacob.obi@templars-law.com
+234 (1) 4611290



Collins Ogbu
Associate

collins.ogbu@templars-law.com
+234 (1) 4611290

OFFICE LOCATIONS

Lagos

5th Floor, The Octagon
13A, AJ Marinho Drive
Victoria Island
Lagos Nigeria

Tel: +234 1 461 1294, +234 1 270 3982
+234 1 279 9396, +234 1 461 1889-90

Fax: +234 1 271 2810
Email: info@templars-law.com

Abuja

3rd Floor, Metro Plaza
Plot 991/2, Zakaria Maimalari Street
Central Business District
Abuja Nigeria

Tel: +234 9 273 1898, +234 9 273 1877

TEMPLARS
www.templars-law.com

templars
@templars_law