Comparative perspectives on cybercrime legislation in Nigeria and the UK - a case for revisiting the "hacking" offences under the Nigerian Cybercrime Act 2015

Adekemi Omotubora [1]

Cite as Omotubora A., "Comparative perspectives on cybercrime legislation in Nigeria and the UK - a case for revisiting the "hacking" offences under the Nigerian Cybercrime Act 2015", in European Journal of Law and Technology, Vol 7, No 3, 2016.

ABSTRACT

Nigeria recently passed a cybercrime law which criminalises certain activities. This paper analyses the provisions of the law on unauthorised access into computer systems. It addresses two significant shortcomings of the law. First, it argues that the omission or failure to criminalise bare unauthorised access or 'basic hacking' into computer systems is inimical to the overall effectiveness of the provisions of the law dealing with unauthorised access. Second, it contends that it is unnecessary and counter-productive for the law to include a finite list of further offences that a hacker may intend to commit. In identifying the possible interpretation, implementation and enforcement challenges of the law, the paper examines the UK Computer Misuse Act (CMA) 1990 and the rationale of the Law Commission in proposing the 'basic hacking' offence. The paper concludes that although perceptions of cybercrime and cybercriminals are relative to social contexts and differ across jurisdictions, criminalisation and punishment for 'basic hacking' demonstrates recognition for the threats posed by hacker and is an increasingly significant way to deter hackers and improve cybersecurity at national and international levels.

INTRODUCTION

Nigeria has been rated one of the top three countries where cybercrime is most pervasive. [2] This rating underlined the scale of cybercrime in Nigeria and the need for criminal legislation to combat the problem. However, attempts to pass a cybercrime law was unsuccessful until the Nigeria National Assembly passed the Cybercrime Act May 2015. At both national and international levels, it was acknowledged that the law was overdue and therefore is a welcome development.

In terms of the scope, the law covers a wide range of cyber-threats and creates extensive criminal offences. However, the law also has significant shortcomings and lacunae. This paper focuses on section 6 which creates the offence of computer hacking. It argues that by criminalising unauthorised access subject to the hacker having criminal intent, the law fails to create a basic hacking offence. The paper also argues that because the law creates an infinite list of further offences, the section invariably limits both the interpretation and application of law. Drawing on provisions of the UK Computer Misuse Act and the Nigerian Criminal Code,

the paper highlights the technical aspects of computer hacking, the threats posed by basic hacking and the rationale for criminalising unauthorised access regardless of the intent of the hacker or the commission or non-commission of further offences.

After analysing the reasons why the law may have overlooked criminalising basic hacking including the social perceptions of cybercrime and the misunderstanding of the threats posed by hackers, the paper concludes with proposals for amendment of the law. It recommends framing a basic hacking offence without reference to the intention of the hacker or to further offences which may or may not be committed by the hacker. It however concludes that to legitimise the offence, punishment must be reflective of and fit the crime.

CRIMINALISING 'BASIC HACKING' - DOES MOTIVE/INTENT MATTER?

Section 6(1) of the Cybercrime Act provides as follows:

> Any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment.

The correct elements of the above offence are *intentionally accessing a computer system without authorisation, for fraudulent purposes, and obtain data of vital national security*. However, to underline the problematic aspects of this section, it is important to consider the provision of section 6(2) of the Act. Section 6(2) provides:

> Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information, the punishment shall be imprisonment for a term of not more than 7 years or a fine of not more than N7, 000,000.00 or to both such fine and imprisonment.

It is notable that similar to section 6(1), section 6(2) requires that the hacker's unauthorised access be accompanied by fraudulent intent. Also, while section 6(2) broadens the scope of further offences that the hacker may intend to commit to include intent to obtain computer data, secure access to any program and so on, it raises the same, if not more difficult questions. To illustrate, when juxtaposed with section 6(1), section 6(2) would read as follows:

> Any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information,….

There are two main problems with sections 6(1) and (2). Firstly, they limit the scope of hacking offences by failing to criminalise unauthorised access to computer systems without ulterior intent. The Law commission of England and Wales (hereafter the Law Commission) refers to this as the 'basic hacking' offence. To commit a basic hacking offence, a person only needs to access a computer system intentionally and without authorisation. It is immaterial whether his purpose or intent is fraudulent, malicious or even innocent. Secondly, because they enumerate categories of further offences that a hacker may intend to commit in accessing

computer systems without authority, the provisions severely limit the interpretation and application of the law. In other words, why must the hacker only be capable of forming the intent to access data that are vital to national security or computer data or program or commercially sensitive or classified data or any type of data for that matter? Stated simply therefore, the questions are, why is the definition of fraudulent purpose within the legislation inimical to the operation of the law and how and to what extent (if at all) should the law specify the categories of further offences?

Relevant provisions of the UK Computer Misuse Act (CMA) help to understand the potential pitfalls sought to be highlighted above. Sections 1 and 2 of the CMA provide as follows:

> (1) A person is guilty of an offence if-
>
> (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
>
> (b) the access he intends to secure is unauthorised; and
>
> (c) he knows at the time when he causes the computer to perform the function that that is the case. (2) The intent a person has to have to commit an offence under this section need not be directed at- (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer

Under section 1(a) cited above, an offence is committed simply by "logging into or attempting to log into a computer system regardless of whether access is motivated by fraudulent intent or otherwise. Hence the Law Commission referred to the crime as 'basic hacking'. [3] To illustrate the point, the Law Commission gave an example that is instructive. There are three stages involved in logging into a computer system for access purposes. The first stage occurs when the computer user enters his identity code, his name, initials or password. In the second stage, the computer verifies the identity of the user and if it recognises the user, grants access to the third stage where the user is allowed to use the facilities of the system. [4] According to the Law Commission, at stage three, the user unquestionably secures access to data or program held on the system and is therefore guilty of an offence. At stage two, he is guilty of an offence when he is verified by the computer because he intended thereby to obtain access to data or programs. The Commission also considers that the user is guilty of an offence at stage one because he already obtained information about data or program stored in the computer by finding out whether or not identification combination he presents is recognised as valid by a program held on the computer. In effect, securing access to a program includes running the program. [5] Following this reasoning, section 1 of the CMA defines unauthorised access in terms of causing the computer to perform *any function with intent to secure access to any program or data*. [6] As the hacker need not have fraudulent or other malicious intent, intentionally accessing information systems without or in excess of authority is an independent and choate offence under the CMA.

The Law Commission's overriding consideration here is the recognition of a 'hierarchical' level of offending, [7] and a need to create a 'preparatory offence' which could cover a broad scope of 'further offences' or 'ulterior intent' offences. [8] As the Commission suggested, for the purpose of liability, a further or substantive offence need not be committed or even attempted; all that is required is that the offender accesses the computer system without or in excess of authority. [9] This is consistent with the main justification often provided for criminalising hacking, i.e., the need to protect the confidentiality, integrity and availability of computer and

information systems. Indeed, the underlying rationale for most basic hacking offences is the protection of the integrity of information systems and the fact that they serve as a deterrent and prevent secondary offending. Therefore, as the Commission aptly argues, 'Basic hacking is proposed to be 'a simple means of deterring all hackers, whether fraudulent or malicious or not…' [10]

Furthermore, the Law Commission reasoned that a basic hacking offence is justified because unauthorised access is often perpetrated by outsiders and therefore difficult to discover and investigate. In this regard, the Commission noted that while insiders are people with legitimate access to a system who nevertheless exceed that (legitimate) access or use it for a wrongful purpose, outsiders are what is typically thought of when talking of 'hackers'. [11] The suggestion is that it is easier to discover employees or other insiders who exceed their access, whereas, because the outsider takes additional precautions to avoid discovery, their activity might not be discovered. The danger here is not so much the possibility of inadvertent damage to the system, but the uncertainty and cost caused by the hacker's attempts to infiltrate the system. For system administrators and owners of proprietary systems, this translates to additional cost of security including the cost of monitoring and investigating unauthorised access to their systems. [12] For example, while all systems are potentially vulnerable to misuse by insiders that could ordinarily be anticipated and discovered, [13] complete lack of authority on the part of outsiders raises further challenges to security mechanisms because they can be unpredictable and unexpected. [14] Although the distinction drawn by the Law Commission between insider and outsider access could become academic and tenuous, [15] and has indeed been criticised for creating 'confusion and lack of clarity in the application of the crucial concept of authority', [16] the criminalisation of basic hacking nevertheless underlines the very mischief and the nature of threat that the law is intending to prevent - i.e., the disregard for the integrity of information systems underlined by complete lack of authority on the part of the 'outsider hacker'. [17]

Contrary to the above position, simply accessing a computer without authority is not an offence under the Nigerian Cybercrime Act. An offence is only committed when unauthorised access is accompanied by an ulterior (fraudulent) purpose and an intent to access any program or certain data or content. As the debate on the law (then a bill before the National Assembly) demonstrates, lawmakers clearly misunderstood the legal and technical issues involved in hacking and were not convinced by the underlying rationale for criminalising basic hacking. One lawmaker argued for example:

> "… the moment somebody has access to your computer, as long as it is not for something illegal or criminal and he is not taking your computer away permanently, you cannot say the person has committed an offence. If …I pick your computer system and I try to crosscheck a file, I do not think it is an offence." [18]

Consequent upon observations such as the above, lawmakers made proposals to amend the basic hacking offence which had been part of the bill. One of the proposed amendments stated that, 'Any person who uses a computer to hack, obtain information or extract data or otherwise, create harm to the computer network has committed an offence.' [19] Another provides that, 'Any person who without authorisation intentionally accesses in whole or in part a computer system or network for fraudulent purposes commits an offence'. [20] These amendments demonstrate that lawmakers miss the very mischief at which the law is aimed. That is, that a person should not hack or access a computer system simply because he wants to or because he can. Therefore, proposals that the hacker should have fraudulent or other

intent to damage or otherwise make the computer unavailable would be irrelevant to the context of the crime. As the explanations of the Law Commission above correctly suggest, it is immaterial for the purpose of the basic hacking offence whether the hacker accessed computer systems for fraudulent or other malicious purpose(s) or merely as a prank.

The Commission further indicates that it is immaterial whether the hacker has the intention of subsequently committing an offence or whether it was indeed impossible to commit any further offence(s). This observation leads to a consideration of the second problem. That is, why must the hacker only be capable of forming the intent to access *data that are vital to national security or computer data or program or commercially sensitive or classified data or any type of data for that matter?* In other words, what is the effect of enumerating specific heads of further offences under sections 6 (1) and (2)?

Section 1(2) of the CMA again provides some direction. As noted above, the section provides that where a person secures access to a program under section 1 of the law, he is nevertheless guilty of an offence although he does not intend to access any particular program or data or a program or data of any particular kind. It is significant to note that the three stages of access identified by the Law Commission above support the inference that by logging onto a computer at all, a person already accesses any or some programs or data. By logical inference, it is unnecessary to further specify that he access any particular program or data. Arguably therefore, while the CMA itself contains reference to access to *any program*, the provision is at best repetitious since we can assume that access to programs can occur as a matter of course. Nevertheless, the Law Commission again offered insights into the rationale for this approach. According to the Commission, the CMA omitted the designation or enumeration of further offences in order to enable the creation of a 'preparatory offence' which also covers a broad scope of 'further offences' or 'ulterior intent' offences. To illustrate, the Law Commission cited the example of a hacker who breaks into the computer system of a banking organisation and succeeds in transferring funds. Whilst as noted by the Commission, he could be charged with theft immediately when the fund transfer succeeds, it is unclear whether the hacker could be charged with attempted theft if he fails on account of being inhibited by the bank's computer security system. The Law Commission rationalised that the difficulty in such cases lay in the speed with which it is possible to transfer funds in computerised systems which makes it difficult to distinguish preparation from attempt for the purpose of allocating criminal liability. It was argued that when he defeats security checks such as gaining access by trying a large number of alternative passwords, the hacker was merely at the preparatory stage for the substantive crime of theft. But thereafter, transfer can be instantaneous; and it becomes difficult to locate the point during the criminal transaction at which he could be charged with attempted theft. The Commission opined that while attempt is not clearly discernible in cases such as this, the law should be such that 'a person, if he were detected trying to find the password, would at that stage have committed the offence of obtaining unauthorised access to a computer with intent to steal.' [21]

The basis of the preparatory offences was therefore to pre-empt secondary offending by exposing the hacker to prosecution at an early stage. However, because it is difficult to anticipate all categories of wrongdoing which a person may achieve by hacking into a system, the Commission proposes that the law cover all types of secondary offending and not merely specific ones. As the Commission noted:

> We did not consider that it would be prudent or indeed possible to draw up a list of offences that might constitute such a 'further' offence, because it is not possible to draw up a finite list of the nefarious ends that a person might try to achieve by first

> securing unauthorised access to a computer. An indictment for the ulterior intent offence would contain particulars of the further offence allegedly intended. [22]

Correspondingly, drawing up a limited number of acts which may follow a hacking incident such as intent to obtain data vital to national security and so on, as done under sections 6(1) and (2) of the Nigerian Cybercrime Act is limiting and undesirable. This is more so because intent is a notoriously difficult element to prove. It is trite that a person is taken to intend the *actus reus* or forbidden act of a crime either in the ordinary, core sense of "intention", or in the sense that he recognised that the *actus reus* was a virtually certain consequence of his action. [23] In spite of this clear direction, intention is a subjective concept and a particular *actus reus* could support multiple intentions. In essence, if a person hacks into a system, it may be difficult to establish what he intended to further achieve. In *R v Delamare*, [24] the intent of the defendant was to commit fraud on an account. In *DPP v Lennon*, [25] the defendant intended to, and did overwhelm the target website to cause a denial of service attack. In other words, while obtaining certain content may seem a natural or direct or foreseeable or virtually certain reason for hacking into a system, the overt act of hacking can also support a number of intent. This may include potentially more serious offences such as hacking into a hospital computer which contains details of blood groups and rearranging the data with the intention that a patient should be seriously injured by being given the wrong blood. [26] It can also include offences which would be committed at a later date or offences unrelated to computers. [27]

To cite a hypothetical scenario, suppose a person is caught accessing the computer system of a bank without authority. The system presumably contains personal (financial) information of the bank customers and we therefore assume that the hacker will be charged under section 6(2) of the Cybercrime Act. The hacker admits that he accessed the bank's systems without authority but denies that he acted with fraudulent intent. He argues that he is prankster or ethical hacker testing the strength of the bank's computer systems, in which case there is no crime because the law does not criminalise intentional access without authority *per se,* but intentional access without authority for a fraudulent purpose. The prosecution then has to prove that the hacker's intention was to access any of the data specified in section 6(2). How can the prosecution discharge the burden of proof? The Cybercrime Act did not define confidential or classified data, so the prosecution is left with a charge of intent to access content data or any program on the computer. The Act did define content data to include every information required by the computer to be able to operate, run and store programs, [28] and it was argued above that logging onto a system automatically translates to access but this does not help much. For example, if the prosecution argues that fraudulent purpose can be inferred from access to content data or programs, the defense could counter the argument by pointing out that as some content data or computer programs are accessible as a matter of course, it is immaterial whether a person logs on with a fraudulent or innocent intent.

It is important to state that the objective here is not to suggest that the UK CMA comprehensively deals with all possible difficulties which may arise with respect to hacking. For example, it is often technically difficult to detect hacking itself, much less any accompanying further offences. Indeed, as Nelson argues, 'it is far more common for the computer hacker to access a network without resulting in damage and to exit without ever been detected'. [29] More fundamentally, even if further offences could be established, proving the same may be a legal impossibility considering the slow responses of law to the peculiarities of cybercrime. Identity theft is a good example which highlights this argument under both Nigerian and UK laws.

Under section 383(1) of the (Nigerian) Criminal Code Act, 'A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing'. Section 383(2), provides additionally that a person who takes or converts anything capable of being stolen is deemed to do so fraudulently if he does so with intent, inter-alia, [30] to permanently deprive the owner or any person who has any special property in the thing of the property. [31] Generally, a thing capable of being stolen is every inanimate thing whatever which is the property of any person, and which is movable or capable of being made movable. [32] For the purpose of the offence, it is immaterial that the thing is made movable in order to steal it, [33] but a person shall not be deemed to take a thing unless he moves the thing or causes it to move. [34]

The elements of a theft offence are therefore ownership, fraudulent conversion, movability and indeed moving the property, as well as intent to permanently deprive the owner of the property or the thing in the property stolen.[35] In addition, the law requires that inanimate things capable of being stolen must also be movable or made movable by the thief. Conversely, in data terms, 'theft' may involve the mere copying of the information rather than *taking or moving*. By processes of replication and duplication, data can be 'stolen' even while literally, it remains unmoved. However, even if moving could creatively be extended to include copying, (as in cases where information is copied from hard drive to flash drive), the fact that the 'thief' has not permanently deprived the owner of the information is arguably fatal to a charge of theft. This is even more compelling when one considers that the information may be backed up. The Nigerian Court of Appeal affirmed this position when it held that for the purpose of the theft offence, there must be an intention to deprive the owner permanently of the property or 'animus furundi.' [36] In England, the court in *Oxford v Moss* [37] had applied the same reasoning when it held that since copying of an examination paper did not permanently deprive the owner of the intangible property, a material element of the offence of theft was not satisfied. [38] Moreover, there is still no separate or specific offence of identity theft under the UK law [39] and the bare theft of identity information cannot ground criminal liability. [40] As Walden argues, criminalising identity theft is problematic because the term 'identity theft' is a misnomer since information itself is not generally capable of being stolen. [41]

The core of the argument here is that the lacunae created by the provisions of sections 6 (1) and (2) of the Cybercrime Act are likely to be exploited by criminals and defense lawyers. As the hypothetical case and the example on identity theft demonstrates, in spite of the law providing a broad or infinite scope of further offences, it is possible that all the prosecution can prove is the fact that a system has been hacked at all.

In view of the above, a proposal may be made to expand the scope of the hacking offences under the Cybercrime Act. Although the position of the Nigerian law is that preparatory acts cannot attract criminal liability, [42] the provision of the Criminal Code would clearly accommodate the notion of basic hacking. The Code provides for instance that:

> It is immaterial, except so far as regards punishment, whether the offender does all that is necessary on his part for completing the Commission of the offence, or whether the complete fulfilment of his intention is prevented by circumstances independent of his will, or whether he desists of his own motion from the further Prosecution of his intention. It is immaterial that by reason of circumstances not known to the offender it is impossible in fact to commit the offence. [43]

Given this provision of the Code, even if the intention of the draftsman was to avoid the pitfall of so called 'preparatory offences', the sections 6(1) and (2) offences can still be more broadly defined. Rather than defining the offence restrictively in terms of intent to obtain computer data, program or commercial or industrial secrets, the offence could be defined in terms of unauthorised access with intent to commit a felony, a misdemeanor, or to commit any offence defined by the cybercrime law or the general criminal law. As further examples, under the Code, breaking and entering is an offence if committed with intent to commit a felony. A felony in turn encompasses a wide scope of other offences and is punishable with a minimum of three years' imprisonment. This is a more dynamic approach since the Criminal Code also accommodates the notion of general rather than specific intent. Section 24 provides that 'Unless the intention to cause a particular result is expressly declared to be an element of the offence constituted, in whole or part, by an act or omission, the result intended to be caused by an act or omission is immaterial.' [44] Therefore if D breaks into the computer systems of P bank, whether or not he intends to obtain personal data or other content he could be charged with the basic hacking offence and sundry offences. These may include intent to commit fraud, theft, blackmail or other computer-related or real world offences rather than the prosecution restricting itself to specific content offences.

LEGITIMISING THE BASIC HACKING OFFENCE - PUNISHMENT MATTERS

Having concluded the analysis of the substantive provisions of the law, it is important to also examine how a basic hacking offence should be punished. Section 4(2) of the Criminal Code cited above underlined the significance of punishment for crimes such as basic hacking. For clarity, the key part of the provision are the words '*It is immaterial, except so far as regards punishment …*'

This provision suggests that as far as the law is concerned, the measure of punishment is a legitimate basis for distinguishing between attempts and substantive offences. As examples, under the Criminal Code, an attempt to commit felony or misdemeanor is itself only a misdemeanor and attempts to commit misdemeanors carries one-half of the greatest punishment for the substantive offence. Also, attempts to commit a felony punishable with death is punishable with imprisonment for seven years unless other punishment is prescribed by law. If a person desists on his own motion from further prosecution of his intention, the law provides that punishment is one-half of the punishment to which he would otherwise be liable. [45] Therefore, the inference to be drawn from the provisions of the Code is that punishment must reflect the seriousness and severity of the offence and the courts must apply punishment which fits the crime.

Apart from the emphasis the law lays on the measure and degree of punishment, the analysis of punishment for basic hacking is necessary for two additional reasons. One, is that it is generally possible to question the moral and jurisprudential basis of criminalising basic hacking and the culpability of hackers. Two, there are societal perceptions of cybercrimes and cybercriminals in Nigeria and indeed in other jurisdictions, that may impact on the ability of the judicial system to impose punishment when further offences cannot be detected or attributed to the hacker. It has been argued for example that criminalisation (of hacking) is manifestly undesirable because it encroaches on certain fundamental freedoms. According to Nelson:

> We might propose that the unauthorised access of a computer database is immoral because it violates the dignity of those who have labored and produced something of value over which they expect to exercise a certain amount of control. We might also argue that computer hacking is a moral affront to the right to privacy when a database contains personal information…However…According to the "alternative ethic," computer hacking is an expression of a fundamental human impulse. [46]

This "alternative ethic" also holds that criminalisation inhibits the hacker instinct essential for innovation. It further associates the hacker with the ideals of intellectualism and fanatism. [47] In fact, as Chandler suggests, the personal computer would never have existed without hackers. [48] Although, it is largely inaccurate, this controversial notion of the hacker persists in contemporary discourse and even the courts have tacitly endorsed it. In *R v Bedworth*, [49] the jury accepted the defence of computer addiction in acquitting the defendant. In *R v Cuthbert*, [50] although the defendant was nonetheless convicted, the court considered him as deserving sympathy because of lack of malicious intent. The public support for 'Pentagon hacker' Gary McKinnon in the UK and the eventual quashing of the order to extradite him to the US further suggests that the society differentiates between "ethical" and criminal hackers. [51]

Similar to the position above, the ethical and moral values at stake in computer hacking in Nigeria are contestable. For example, there is a tendency to undermine the hacker threats and see hackers as little more than activists (or hacktivists) who attack government owned websites in pursuit of radical social or political agendas. In fact, music which extols the exploits of cybercriminals has been promoted by popular media in Nigeria. [52] In their research into the social organisations of internet fraudsters in Nigeria, Tade and Aliyu [53] found that mass youth unemployment and the corruption and impunity of public and political office holders were the explanations offered for the emergence of the yahoo-boys (internet fraudsters) sub-culture in Nigeria. The authors argue that the sustenance of the sub-culture itself is aided by society's propensity towards celebrating wealthy individuals irrespective of the source of wealth. Accordingly, since the system also fails to punish large scale fraud and corruption perpetrated by public officials, the society and cybercriminals justify their crimes on grounds of necessity and survival and societal tolerance towards economic crimes generally. [54] As shown by earlier arguments in this paper, inferences drawn from records of legislative debates suggest that even lawmakers struggle to understand the basic hacking offence and the rationale behind its criminalisation. [55] Therefore, to fully address the moral and legal questions that basic hacking raises, it is important to understand the rationale for and limits of punishment. The utilitarian and retributive theories of punishment provide some answers in this respect.

From the perspectives of the retribution theory of punishment, it is possible to understand the jurisprudential basis of contesting a basic hacking offence. The theory proceeds on the principle that it is morally right to hate criminals and society extracts retaliation (for the crime) through the suffering of the offender based on a principle of equality or like for like. [56] Accordingly, punishment is justified only in response to a violation of the moral order. This implies that justice is inherent to the act of punishment and that punishment is consistent with and equal to the severity of the offence. [57] In context, to be fit for punishment, the hacker must cause some harm for which society seeks to extract retribution. However, unless hacking is followed by some form of secondary offending, the hacker may cause no actual harm or damage. Consequently, the basis upon which society seeks to vilify him may be unclear.

Conversely, when viewed from the utilitarian perspective of punishment, the hacking offence appears more defensible and pragmatic. The Utilitarian conceives punishment as having a goal beyond merely extracting retribution for a wrongful act. Utilitarians argue that punishment is itself evil and may only be administered if it promises to exclude some greater evil. [58] Therefore, punishment is justified only if it maximises utility in the sense that when balanced against the pains and cost, society finds punishment efficacious and profitable in preventing the mischief in question. According to Bilz and Darley, utilitarians assess what will happen as a result of different punishments, and weigh these outcomes against one another, and society may impose punishment only if the net result is that society will be better off. [59] To this end, punishment must be seen as having an instrumental value or socially beneficial consequences which utilitarians conceive as deterrence, restriction and reformation of the offender.

Applied to hacking, the utilitarian approach shows that criminalisation is not necessarily aimed at extracting retributive justice for an inherent wrongfulness. It aims rather to achieve ends beneficial to society, which include protecting computers and networks and developing electronic transactions and commerce for the broader economic well-being of the society. However, while the utilitarian theory is useful in explaining and justifying an offence of basic hacking, its approach to punishment may give rise to concerns. While the retribution theory proposes that the seriousness of an offence be measured by the actual harm inflicted and that on grounds of reasonableness, principle and pragmatism, punishment must reflect the seriousness of the offence, [60] the utilitarian considers it immaterial that punishment fit the crime and may often propose punishment which appear excessive relative to the crime. Accordingly, as Bilz and Darley correctly posit, 'if we ask, how much should we punish? He (the utilitarian) might answer "Exactly as much as is necessary to offset the bad effects of the crime." [61]

Therefore, on the one hand, if we follow the strict retribution theory - the approach taken by the Nigerian Cybercrime Act - we cannot punish the hacker unless his activities create further suffering or losses. As basic hacking may not result in such suffering, it does not distort the moral order and should not attract punishment. On the other hand, if we adopt the utilitarian approach, we may impose excessive punishment and inadvertently attract moral arguments about the severity or otherwise of the punishment. For example, Gary McKinnon faced 60 years in a US jail for hacking into the Pentagon computers whereas he could be jailed for as little as 6 months if he was convicted of the same offence in the UK. While this could not be ascertained, the potentially long jail term probably account for the public support that McKinnon attracted and why the UK government did not eventually extradite him.

In the Nigerian context, the provisions of the Criminal Code and peculiar socio-cultural and legal problems force the consideration of a balanced approach to punishment even more. For example, because hackers are often characterised as well-educated, young, technology-savvy individuals, [62] questions may arise on the desirability of exposing such individuals to the full impact and severity of the penal system with its attendant stigmatisation and implications for recidivism. Furthermore, precedents suggest that Nigerian courts tend to punish economic criminals comparatively less severely and they may impose small fines in lieu of imprisonment. [63] Hence, a criminal who loots the state treasury would receive a comparatively less serious punishment than a bank robber. While the argument here is not that hackers should not be punished, it is important that further considerations be given to the issue of punishment particularly considering the nature and severity of the crime and the characteristics of likely offenders. In other words, to legitimise basic hacking, it is important to ensure that the punishment fits the crime. If punishment is perceived as too severe, tensions

may arise within the criminal justice system both as to the nature and severity of punishment as well as its desirability and utility. The Scottish Law Commission put the inherent difficulties here in perspective when it noted that 'The disadvantage (of a basic hacking offence) is that, on conviction of an offence …, a court might find it impossible to pass a more severe sentence…without reference to the actual or intended consequences.' [64]

To address the dilemma, the law must impose punishment which reflects the threats posed by hackers while at the same time recognizing that further offences could be potentially more serious than the hacking itself. One approach is to amend the Cybercrime Act by inserting a provision which simply makes it an offence to access computers intentionally and without authority. If the law takes this approach, the basic hacking offence would then be punished less severely than those cases where intent to steal data, or commit fraud or disrupt a computer system is established. Ideally imprisonment could range from one year to a year and 6 months. Alternatively, the law may create an offence of attempt to access data or content. The fact of such attempt would be inferred from circumstances such as accessing computers intentionally and without authorization or exceeding lawful authorization. Punishment would normally follow the precedent under the Criminal Code and would be one-half of that prescribed for the substantive offence of actually accessing the data or content. Additional or more severe punishment may be imposed for attempting to or accessing specific data such as data vital to national security or commercially sensitive data if this is desirable. Finally, the courts must be allowed discretion on punishment including the power to impose fines in lieu of imprisonment. Section 382 (1) of the Nigerian Criminal Procedure Code encapsulate the rule in this respect. It provides:

> Subject to the other provisions of [the] section, where a court has authority under any written law to impose imprisonment for any offence and has not specific authority to impose a fine for that offence, the court may, in its discretion, impose a fine in lieu of imprisonment.

The proposal above would ensure fairness and even facilitate the rehabilitation or reformation of so-called "ethical hackers". More importantly, it would promote the legitimacy of punishment and help to avoid any speculation of legislative overkill. As Nelson rightly observed, 'Where the law has lost the appearance of legitimacy, those who are called upon to behave or to refrain from behaving in a particular way are less likely to comply.' [65]

CONCLUSION

This paper has analysed the provisions of Nigerian Cybercrime Act 2015 relating to intentional unauthorised access into computer systems. The analysis suggests that merely accessing a computer or other information systems intentionally and without authority does not constitute an offence under the new law. Consequentially, in spite of the threats posed by hacking, hackers are likely to go unpunished unless the prosecution can show that they have fraudulent purpose for hacking into the computer. The paper highlights the distinct advantages of criminalising basic hacking. This includes the fact that hacking is a preparatory offence and often a precursor to further offences such as identity theft and fraud. It also includes the recognition of the fact that hacking, whether malicious or not, undermines the integrity of information systems and increases the cost of securing proprietary information systems. Therefore, criminalising and punishing hacking as a primary and independent offence can pre-empt and prevent secondary offending and expose the hacker to punishment at an earlier stage of the criminal transaction. The paper also highlights the fact that because it is often difficult to establish the intent and motive of hacker as well as to establish further

offences, the fact that a computer was hacked at all may be all that the prosecution can prove. However, it was conceded that there are legitimate moral, social and legal bases for contesting a basic hacking offence as a result of which it is vital to ensure that punishment for hacking fits the seriousness of the crime. The analysis in the paper was concluded with the consideration of how the theories of punishment address the social and judicial dilemmas on the morality and legality of punishing hackers to whom further offences could not be attributed. The paper proposed that if the punishment prescribed by law is made to fit the crime, the law would be more practical and pragmatic in its approach to the technical and legal difficulties of detecting further offences and discerning the hacker intent.

---

[1] Lecturer, Faculty of Law, University of Lagos, Nigeria.

[2] See eg Federal Bureau of Intelligence Internet Crime Complaint Centre, '2013 Internet Crime Report' <https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf> accessed 25/12/2016.

[3] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186, 1989) para 2.1.

[4] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186, 1989) paras 3.16-3.18.

[5] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186, 1989) paras 3.16-3.18.

[6] Computer Misuse Act 1990, s 1.

[7] See Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186, 1989) para 3.11.

[8] See further notes on preparatory offences below..

[9] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 2.1.

[10] The Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186, 1989) para 3.9.

[11] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186, 1989) para1.20.

[12] Law Commission *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 1.29.

[13] See, for e,g,,*DPP v Bignell* [1998] 1 Cr App R 1.

[14] Law Commission *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 1.22.

[15] see *DPP v Bignell* [1998] 1 Cr App R 1; see also *R v Bow Street Metropolitan Stipendiary Magistrate and another, ex parte Government of the United States of America* [1999] 4 All ER 1.

[16] Neil MacEwan, 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future' (2008) Criminal Law Review 1, 3.

[17] See generally Law Commission *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) paras 1.19-1.36.

[18] Senate Hansard, vol 1 No 27, Thursday 23rd October 2014, 9.

[19] Senate Hansard, vol 1 No 27, Thursday 23rd October 2014, 9.

[20] Senate Hansard, vol 1 No 27, Thursday 23rd October 2014, 9.

[21] Law Commission, *Criminal Law- Computer Misuse* (LAW COM No 186 cm 819, 1989) para 3.52.

[22] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 3.54.

[23] AP Simester and others, *Simester and Sullivan's Criminal Law: Theory and Doctrine* (4th edn, Hart Publishing,2010) 127.

[24] [2003] EWCA Crim 424.

[25] [2006] EWHC 1201.

[26] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 3.55.

[27] Law Commission, *Criminal Law-Computer Misuse* (LAW COM No 186 cm 819, 1989) para 3.57.

[28] See section 58 Cybercrime (Prohibition, Prevention, Etc.) Act 2015.

[29] Brennan Nelson, 'Straining the Capacity of the Law: The Idea of Computer Crime in the Age of Computer Worm' (1991) 11 Computer LJ 299, 319.

[30] s 383(2)(c)-(f) Criminal Code Act.

[31] 383(2)(a)-(b) Criminal Code Act.

[32] s 382 Criminal Code Act.

[33] s 382 Criminal Code Act.

[34] s 383(6) Criminal Code Act.

[35] See eg *FRN v Yaro* (2012) 3 SCNJ 236-237.

[36] *FRN v Yaro* (2012) 3 SCNJ 236-237.

[37] (1979) 68 Cr App R 183.

[38] *Oxford v Moss* (1979) 68 Cr App R 183, 185.

[39] This is in contrast for example to the Identity Theft and Assumption Deterrence Act 18 USC 1028 which makes identity theft a separate and distinct offence in the US.

[40] Emily Finch, 'The Problem of Stolen Identity and the Internet' in Yvonne Jewkes (ed) *Crime Online* (Willan 2007) 29.

[41] Ian Walden, *Computer Crimes and Digital Investigations* (OUP 2007) 116.

[42] See *Dibia v State* (2012) l PERL 8564 (CA); see also *Yakubu Sanni v State* (1993) 4 NWLR (pt 285) 99, 199.

[43] s 4(2) Criminal Code Act.

[44] s 24 Criminal Code Act.

[45] ss 508-512 Criminal Code Act.

[46] Brennan Nelson, 'Straining the Capacity of the Law: The Idea of Computer Crime in the Age of Computer Worm' (1991) 11 Computer LJ 299, 309.

[47] See Helen Nissenbaum, 'Hackers and the Ontology of Cyberspace' (2004) 6(2) New Media & Society 195,199-200.

[48] Amanda Chandler, 'The Changing Definition and Image of Hackers in Popular Discourse' (1996) 24 International Journal of the Sociology of Law 229.

[49] (unreported) 1991 in Yaman Akdeniz, 'Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Viruses' in Stefan Fafinski, *Computer Misuse* (Willan Publishing 2009) 54.

[50] (unreported) cited in S Fafinski, *Computer Misuse* (Willan Publishing 2009) 60.

[51] See eg Graham Cluley, '71% Say Extradition of UFO Hacker Gary McKinnon Is Wrong' (*Dark Reading*, 31/07/2009) <http://www.darkreading.com/71--say-extradition-of-ufo-hacker-gary-mckinnon-is-wrong/d/d-id/1131645?> accessed 02/08/2014.

[52] See eg "I Go Chop Your Dollar" by Nkem Owoh and "Yahozee" by Olu Maintain, <http://news.bbc.co.uk/1/hi/entertainment/7670788.stm> accessed 15/03/2015.

[53] Oludayo Tade and Ibrahim Aliyu, 'Social Organisation of Internet Fraud among University Undergraduates in Nigeria' (2011) 5(2) IJCC 860.

[54] Oludayo Tade and Ibrahim Aliyu, 'Social Organisation of Internet Fraud among University Undergraduates in Nigeria' (2011) 5(2) IJCC 860.

[55] See notes above at p 4.

[56] Immanuel Kant 'Justice and Punishment' in Gertrude Ezorsky, *Philosophical Perspectives on Punishment* (Albany State University of New York Press 1972) 102-106.

[57] Immanuel Kant 'Justice and Punishment' in Gertrude Ezorsky, *Philosophical Perspectives on Punishment* (Albany State University of New York Press 1972) 102-106

[58] See generally Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation 1781* (*White Dog Publishing* 2010).

[59] Ken Worthley Bilz and John M Darley, 'What's Wrong with Harmless Theories of Punishment' (2004) 79 Chi-Kent L.Rev. 1215,1222.

[60] See eg HLA Hart, *Postscript: Responsibility and Retribution' in Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford Clarendon 1968) 210, 235-36.

[61] Ken Worthley Bilz and John M Darley, 'What's Wrong with Harmless Theories of Punishment' (2004) 79 Chi-Kent L.Rev. 1215, 1223.

[62] See e.g. UNODC Comprehensive Study on Cybercrime 2013, 39-42 <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>accessed 12/03/2016.

[63] See eg Ihuoma Chiedozie, 'Nigerian Wonder: N27 Billion Pension Thief Gets N750,000 fine' *The Punch Newspaper* (Abuja, January 29 2013) <http://www.punchng.com/news/nigerian-wonder-n27bn-pension-thief-gets-n750000-fine/> accessed 04/08/2014.

[64] Scottish Law Commission, *Report on Computer Crime* (Scot Law Com No 106 1987) paras 4.5-4.8.

[65] Brennan Nelson, 'Straining the Capacity of the Law: The Idea of Computer Crime in the Age of Computer Worm' (1991) 11 Computer LJ 299, 321.