IJESC

Research Article Volume 8 Issue No.12

Encryption Technology and Privacy Protection: A Critique

Enyia, Jacob Otu[1], MiebakaNabiebu[2]
B.Sc., MBA, LL.B, B.L, Ph.D., Senior Lecturer[1],
Department of Commercial and Industrial Law Faculty of Law, University of Calabar, Nigeria[1]
A Doctoral candidate, Faculty of Law[2],
University of Calabar-Nigeria and a corporate/legal consultant Port Harcourt, River State, Nigeria[2]

Abstract
The internet and information technology generally is changing the way of life of mankind. The act of exchange of word messages involves exchange of other forms of data-pictures, videos, commands for financial transactions and recently, storage of data on and access software and computing services through cloud computing. When we go online, we are doing much more than a passive absorption of information, reading articles and blogs. We are also sending out very sensitive data. Furthermore, on transaction online whether, buying goods/services or signing up for an online account, we send out a lot of personal and sensitive information like names, physical address, email address, passwords, PINs, credit card information, private correspondence, sensitive company information and Bank-account information is send out. Most of the contents that are store on the hardware and software as well as on the virtual cloud include sensitive and personal data that individuals are unwilling to let others access to. This makes security a major concern on the internet. Before now, one could ensure this by securing access to networks, software and hardware through a complicated system of controls. Passwords and other technology security architecture of password control and authorised access was breached and continues to be breached by the actions of hackers, technology experts specialising in either by passing the controls or figuring probabilities so that which we thought was secure, is not more. This paper examines the arguments for and against encryption especially in the context of privacy protection of individuals, analyses the Nigerian context and compares the argument in other more responsive jurisdictions. It further makes recommendations for strategic global actions as well as strategic third world and African action to maximise the gains and reduces vulnerabilities.

Keywords: Encryptions, Technology, Protection, Privacy, Cloud, Computing, Internet, Passwords, Software, Hardware.

Introduction

Encryption, also referred to as cryptography is the process of converting data to an unrecognizable or "encrypted" form, (encoding) a message so that it can be read only by the sender and the intended recipient'[1] or 'to scramble data in such a way that only someone with the secret code/key can read it'.[2] It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.[3]

It serves the purpose of storing data and passing a secret message from one place to another without anyone but authorized personnel being able to read it.In today's world with all of the access to the internet, encryption has emerged as one of the ways, perhaps the surest way of guaranteeing security and privacy on the net, much like drawing virtual blinds or turning virtual locks and keeping everyone out of our virtual homes that we do not want or restricting their access to certain rooms in our houses.[4]Encryption is extremely important for e-commerce as it allows confidential information such as credit card details to be sent safely to the online shop one is visiting and protects access to that information from third parties.

Privacy is the right to be let alone, in the absence of some "reasonable" public interest in a person's activities, like those of celebrities or participants in newsworthy events or suspected and/or convicted criminals.[5] Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating the right.

Section 37 of the *Constitution of the Federal Republic of Nigeria* ***1999 as amended, provides that*** the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'.This stops the police and other government agents from searching persons or property without "probable cause" to believe that we have committed a crime and protect our freedom to make certain decisions about our private lives without interference from the

[1] Encryption available at http://dictionary.reference.com/browes/encryption, Accessed 14th January, 2015

[2] Encryption works by scrambling the original message with a very large digital number (key). This is done using advanced mathematics. The computer receiving the message knows the digital key and so is able to work out the original message.

[3] Available at http://www.teach-ict.com/technology_explained/encryption/encryption.html, Accessed 14th January, 2015.

[4] Haynes, A. B. Virtual Blinds: Finding Online Privacy in Offline Precedents VANDERBILT J. OF ENT. AND TECH. LAW [Vol. 14:3:603 2012] Electronic copy available at: http://ssrn.com/abstract=1984733, visited 14th January, 2015

[5]right of privacy: an overview available at http://www.law.cornell.edn/wex/privacy, visited 14th January, 2015

government.[6]

The conflict between this privacy right and the interest of the State particularly in law enforcement, public safety and national defence is almost as old as the right itself.However, developments following the Snowden and Sony incidents, Apple and Google plans to introduce encryption as default settings as well as terror activities have introduced new dimensions to the debate.[7]

Maintaining privacy in our personal communications is something everyone desires. Encryption is a means to achieve that privacy. It was invented for that very purpose. That makes encryption a good idea. But encryption, like most things, can be used for good or evil. Hence, the debate over how to harness this powerful tool rages on as people on both sides see that there are no easy answers.How much sanctity should be accorded the right to privacy?What level of threat to the public/State justifies derogation from this right?In the context of information technology, how much of a breach to this right can be tolerated before the State machinery becomes an unbearable tyranny?

The Paradigm of Encryption

Encryption can provide a means of securing information. As more and more information is stored on computers or communicated via computers, the need to ensure that this information is invulnerable to snooping and/or tampering becomes more relevant. Any thoughts with respect to personal information (i.e. medical records, tax records, credit history, employment history, etc.) many bring to mind an area in which individual need or expect privacy.

Encryption is seen by many people as a necessary step for commerce on the internet to succeed. Without confidence that net transactions are secure, people are unwilling to trust a site enough to transact any sort of business using it. Encryption may give consumers the confidence they need to do internet business.[8]

Encryption can also provide a means of "message authentication". The PGP User's Guide explains,

> The sender's own secret key can be used to encrypt a message thereby *signing* it. This creates a digital signature of a message...This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature.[9]

This prevents forgery of that signed message, and prevents the sender from denying the signature.[10]

E-mail is certainly not secure. While the general belief is that the use of a password makes your business private, we should be aware that sending information without encryption has been likened to sending postcards through the mail. The message is totally open to interception by anyone along the way. Personal e-mail may not contain content that must be kept secret. But there are many common situations, where users have a legitimate need for security both to protect that information and to ensure that information is not tampered with: Consumers placing orders with credit cards via the Internet, journalists protecting their sources, therapists protecting client files, businesses communicating trade secrets to foreign branches, ATM transactions, political dissenters, or whistle-blowers - all are examples of why encryption may be needed for e-mail or data files, and why it might be necessary to create a secure environment through its use.

---

[6] Froomkin, A. M., Anonymity and the Law in the United States

[7] Matthew A, NSA Revelations 'Changing How Businesses Store Sensitive Data', THE GUARDIAN, http://www.theguardian.com/technology/2014/mar/31/data-storage-nsa- revelations-businesses-snowden(Jan 14, 2015); Nicole Perlroth, A Call for a Highly Encrypted Future, N.Y. TIMES BITS BLOG http://bits.blogs.nytimes.com/2014/03/12/a-call-for-a-highly-encrypted-future(Jan 14, 2015); Jon FingaJ, FreedomPop's New Smartphone Keeps Your Calls and Data Private for $189, ENGADGET, http://www.engadget.com/2014/03/05/freedompop- privacy-phone(Jan 14, 2015); LoekEssers, KPN Strikes Deal with Silent Circle to Offer Encrypted Phone Calls, PCWORLD http://www.pcworld.com/article/2099160/kpn- strikes-deal-with- silent-circle-to-offer-encrypted-phone-calls.html(Jan 14, 2015); David Meyer, Meet Blackphone, A Privacy-Centric Handset from Some Serious Security Veterans, GIGAOM , http://gigaom.eom/2014/01/15/meet-blackphone-a-security-centric-handset-from-some-serious- encryption-veterans(Jan 14, 2015); Nicole Perlroth&VinduGoel, Twitter Toughening Its Security to Thwart Government Snoops, N.Y. TIMES B ITS BLOG http://bits.blogs.nytimes.com/2013/11/22/twitter-toughening-its-security-to-thwart-government-snoops/?_php=true&_type=blogs&_r=0(Jan 14, 2015); Sean Gallagher, Googlers say "You" to NSA,

Company Encrypts Internal Network, ARS TECHNICA http://arstechnica.com/ information-technology/2013/ll/googlers-say-f-you-to-nsa-company-encrypts-internal-network(Jan 14, 2015); Claire Cain Miller, Angry Over U.S. Surveillance, Tech Giants Bolster Defences, N.Y. TIMES, Nov. 1, 2013, at Al, available at http://www.nytimes.com/2013/ll/01/technology/angry-over-us-surveillance-tech- giants-bolster-defences.html(Jan - 14, 2015); Kurt Opsahl, 6 Steps Silicon Valley Can Take to Protect Users from NSA Spying, CNET http://news.cnet.com/8301-13578_3-57610139-38/6-steps-silicon-valley-can-take-to-protect-users-from-nsa- spying(Jan 14, 2015); Adrianne Jeffries, Escape from PRISM: How Twitter Defies Government Data-Sharing, THE VERGE http://www.theverge.com/2013/6/13/4426420/twitter-prism-alex-macgillivray-NSA-government(Jan 14, 2015).

[s]Dijk, M. and Juels, A, On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing

[9] Zimmermann, Philip "PGP User's Guide, Volume I: How it works"

[10] Graham Greenleaf & Roger Clarke - Privacy Implications of Digital Signatures, 10 March 1997 Invited Address, IBC Conference on Digital Signatures, Sydney, 12 March 1997

To ensure security of data, there are even data breach notification laws. An organisation that has suffered data breach, such as a 'hacking' incident, which potentially exposes personal information, must notify those persons whose information may have been acquired. This provides consumers with an opportunity to protect themselves against identity theft and provides a regulatory tool that highlights poor organisational information security practices.[11]

The power of encryption to keep secrets could be misused. It might be employed to conceal criminal activity or for harassment. Stalkers or predators could "hide" using encryption, their identities would be untraceable. It could be used for acts of terrorism, the likes of which are pretty frightening when you consider all of the systems that are computerized today.[12]

In many applications, encryption, could be seen as a threat to existing methods of law enforcement.[13] Should a level of encryption that law enforcement is unable to decipher become easily available, law enforcement would be unable to use current surveillance/wiretapping techniques.[14]

With malevolent use of encryption the information infrastructure may be at risk. Free, unrestrained encryption could cause loss of governmental control on the tax revenues generated in businesses on the web.[15] If the business is "secret", how can taxes be assessed? There would be no means for the government to track revenues in order to collect! With the loss of tax revenues, government as we know it could simply cease to exist. Timothy May describes (foretells?) of or fotold of a hypothetical underground black market for swapping proprietary information could be set up on the internet (BlackNet) that would allow for the sale of all types of destructive and/or sensitive information. The legal authorities would be powerless to stop it.[16]

Children are increasingly having greater access to the net and content therein. The implication of encrypted data made available to these ones that cannot be accessed by their adult supervisors boggle the mind, a pedophile for instance may be able to communicate with the child and lure them out and efforts to track the child yield no results because all of the communication between child and pedophile was encrypted.[17]

The latest technologies make it easier for criminals to contact children in ways that were not previously possible. Children are particularly vulnerable to the exploitation of online predators because they rely heavily on networking websites for social interaction. Offenders use false identities in chat rooms to lure victims into physical meetings, thus connecting the worlds of cyber and physical crime. When this happens, virtual crime often leads to traditional forms of child abuse and exploitation such as trafficking and sex tourism.[18]

Understandably, there are concerns to making powerful encryption available to all. The question is, which set of concerns should weigh more heavily, those of individuals or those of government security forces?

The 'crypto wars' of the 1990's were in the main, a conflict between this technical need for strong communication security and the opposing concern of law enforcement and national security agencies that strong encryption would block access to data, a situation, technically referred to as 'going dark'[19]

The right of privacy has evolved to protect the ability of individuals to determine what sort of information about themselves is collected, and how that information is used. Most commercial websites utilize "cookies," as well as forms, to collect information from visitors such as name, address, email, demographic information, social security number, Internet Protocol address, and financial information. In many cases, this information is then provided to third parties for marketing purposes. Other entities, such as the federal government and financial institutions, also collect personal information. The threats of fraud and identity theft

[11] Burdon, M, Low, R and Reid, J, 'If its Encrypted its Secure! The Viability of US State-based Encryption Exemptions' (Paper presented at the IEEE International Symposium on Technology and Society, University of Wollongong, 7-9 June 2010)

[12] Diaz, C., Tene, O. and GURSES, S., Hero or Villain: The Data Controller in Privacy Law and Technologies

[13] Swire, P. From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud Working Paper Series No. 175 April 12, 2012, co-sponsored by the Center for Interdisciplinary Law and Policy Studies at the Moritz College of Law

[14] Shah, R. and Sandvig, C. , Software Defaults as De Facto Regulation: The Case of Wireless Aps, Presented to - The 33rd Research Conference on Communication, Information and Internet Policy, Arlington, Virginia, USA. September 23, 2005, SEE ALSO Arizona Legal Studies Discussion Paper No. 13-06 ; Bambauer, D., Privacy Versus Security , The University of Arizona James E. Rogers College of Law January 2013

[1] Presently, the taxation system lets offline businesses go without taxing and online businesses are not even reckoned with. Imagine the implications of encrypting all of that information in Nigeria.

[16] May Timothy "Introduction to BlackNet"

[17] **Petty, K.** *A., Protecting Children from Cyber Crime: The Twentieth Session of the UN Commission on Crime Prevention and Criminal Justice inASIL* **Insights, Issue 24, Volume ISSeptember 01, 2011**

[18] Economic and Social Council [ECOSOC], Commission on Crime Prevention and Criminal Justice, 20th Sess., Discussion Guide for the Thematic Discussion on Protecting Children in a Digital age: The Misuse of Technology in the Abuse and Exploitation of Children, Note by the Secretariat, A14, U.N. Doc. E/CN.15/2011/1 (Jan. 31, 2011) [hereinafter Discussion Guide], All documents relating to the 20th Session are available at http://www. unodc.org/unodc/en/commissions/CCPCJ/session/20.html.(Jan 14, 2015)

[19] Electronic Frontier Foundation, "DES Challenge III Broken in Record 22 Hours", Jan 19, 1999

created by this flow of personal information have been an impetus for right of privacy legislation.

As a constitutional right, privacy is as inviolate as any of the other rights- right to life etc.[20]and the only derogations therein allowed are as provided for in the Constitution itself which in essence legitimizes any law reasonably justifiable in a democratic society in the interest of defence, public safety, public morality, inter alia and also allows derogations from rights for the purpose of protecting the rights and freedoms of others.[21]

The import of this is that, anything that threatens society in the context of the issues mentioned therein provides impetus for derogations from this right.

Legal Framework for Encryption in the Nigerian

There is no specific data protection law in force in Nigeria and also no law that is set out to regulate encryption. The laws that have been made that are relevant in this context apart from the 1999 constitution, E-banking guidelines, Freedom of Information Act, 2011 and consumer codes of practice regulationinclude*inter alia*, the Advanced Fee Fraud Act[22] which provides in Section 12 as follows:

1. any person or entity providing an electronic communication service or a remote computing serviceby email or any other form shall be required to obtain from the customer or subscriber
a. full names
b. residential address add in the case of an individual
c. corporate address in the case of corporate bodiesfailure to furnish or provide info above or falsifying is a 100, 000 naira offence[23]

The Nigeria Communication Act[24]provides that the *commission may direct operators to produce electronic data on whatever matter'*[25]

Moreover, *on the occurrence of any emergency or in the interest of public safety, the Commission may order communication intercepted and disclosed in a manner authorized'*[26]

Surprisingly, and in the light of money laundering and terrorism crimes and Nigeria's vulnerabilities in that regard as well as the central role information technology plays today in such activities as well as in the fight against them, the Acts on these issues contain no reference to the necessity or the procedure for obtaining information from electronic data. Such laws as the National Security Agencies Act and the Money Laundering Act make no mention of access to online profiles and activities of potential and suspected criminals and accomplices. Therefore, the contribution of the Nigerian regime to IT Law and to the debate between privacy and encryption is marginal.

Comparative Jurisdictions

The Korea-Sony incident reveals the threats that is faced online if information is allowed to lie around without any safeguards.

In the USA, the whistle-blower incidents[27] reveal how responsive a government can be to threats to its citizens and its territory arising from the use of the internet for telecommunications services and interactions.Currently in the US and UK Government and law enforcement agencies are agitating for greater access to data on the net.

In July 2014, Britain's parliament voted in favour of emergency legislation to allow police and security services to continue accessing internet and mobile phone data, despite a ruling in 2007 by the European Court of Justice that existing data-retention laws across Europe breached citizens' rights to privacy.[28]

David Cameron during his campaign for the office of the U.K. Prime Minister, promised that should he win the general elections, his government would push through new legislation allowing law enforcement access to the content of private, encrypted Internet communications in reaction to the terror attacks in Paris, where 17 people were killed by Islamic extremists. Stressing that the interception of Internet-based mobile communications could only occur in extreme circumstances with a personally signed warrant from the home secretary Mr. Cameron said that the government should not be in a situation where it could not gain access to the content of messages because they are encrypted or because the companies that host the conversations themselves don't have access to them.[29]

According to him:

> *the attacks in Paris once again demonstrated the scale of the terrorist threat that we face and the need to have robust powers through our intelligence agencies and security agencies and policing in order to keep our people safe...And the powers that I believe we need, whether on communications data or on the content of communications, I'm very comfortable that those are absolutely right for a modern, liberal democracy. I will make sure that it is a comprehensive piece of legislation that makes sure we do not allow terrorists safe space to communicate with each other. That is the key principle. Do we allow safe spaces for them to talk to each other? I say no, we don't, and we should legislate accordingly".*

[20]See Chapter 4 of the 1999 Constitution

[21]S 45

[22]Cap. A6, Volume 1, L.F.N., 2010

[23]S12(2)

[24]Cap. N97, Volume 10, L.F.N., 2010

[25] 64(2)(b)

[26] sl48(1)(c)

[27] Snowden, chelsea manning, assange@wikileaks

[28] Copland v. United Kingdom, 62617/00 [2007] ECHR 253 (3 April 2007)

[9] UK PM looking to outlaw encrypted online communication available at http://www.zdnet.com/article/uk-pm- looking-to-outlaw-encrypted-online-communication (Jan 14, 2015)

Following the Charlie Hebdo attack, the head of MI5, Andrew Parker,reiterated the importance of communications interception in the fight against terrorism, and cautioned that changing technology is making it harder for agencies to keep tabs on such communications.

He stated that:

> *Interception of communications, which includes listening to the calls made on a telephone, or opening and reading the contents of emails, form a critical part in the Security and Intelligence Agencies' tool kit...Changes in the technology that people are using to communicate are making it harder for the agencies to maintain the capability to intercept. The communications of terrorists...Wherever we lose visibility of what they are saying to each other, so our ability to understand and mitigate the threat that they pose is reduced."*

In the US, Attorney General Eric Holder expressed hope that technology companies would be willing to work with his office"to ensure that law enforcement retains the ability, with court-authorization, to lawfully obtain information in the course of an investigation, such as catching kidnappers and sexual predators. It is fully possible to permit law enforcement to do its job while still adequately protecting personal privacy."*According to him,* "when a child is in danger, law enforcement needs to be able to take every legally available step to quickly find and protect the child and to stop those that abuse children. It is worrisome to see companies thwarting our ability to do so.*"*[30]

On Apple's plan to install encryption by default on its smartphones, Washington Metropolitan Police Chief Cathy Lanier told Bloomberg that *"Smartphone communication is going to be the preferred method of the pedophile and the criminal. We are going to lose a lot of investigative opportunities*."When arguing why law enforcement should continue to have easy access to phones, James Soiles, US DEA Deputy Chief of Operations, said, *"as long as we are doing it with court orders, there shouldn't be any reason to keep us from it. We want to attack command-and-control structures of drug organizations, and to do that we have to be able to exploit their communication devices."*

According to FBI Director, James Comey,We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions. The second challenge concerns court- ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Arguing that the notion that law enforcement can obtain any information by tapping a switch is true only in TV and movies and that the post Snowden pendulum has swung too far in favour of privacy rights. He says that '[i*]n the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. ... law enforcement needs to be able to access communications and information to bring people to justice'.*

Lamenting that even with lawful authority, law enforcement may not be able to access the evidence and the information for crime prevention and detection,

> Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost? ... There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

For him, the fundamental questions are:

> *Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away...willing to leave victims in search of justice?*[30]

The pro-privacy groups however argue that 'national government access to encryption keys would undermine and hold back both the development of e-commerce and the political use of the Internet in pursuit of free expression rights'.[31]They argue thatencryption technology is a fundamental element for the development of a global electronic commercial system. For financial transactions to be securely transmitted and conducted, there must be confidence that the mode of communication delivers both secrecy and verification. ... the same encryption technology can be used for securing true private communications concerning public affairs.[32]

It has enabled the use of the Internet as a mode of information gathering and dissemination concerning, for example, human rights abuses,[33] a mode of communication that allows them to

---

[30]Interview by Alex Hern in The Guardian(US) of 17/10/2014 available at;

[31] See, e.g., Fred H. Cate, James X. Dempsey, & Ira S. Rubinstein, Systematic Government Access to Private-Sector Data, 2 INT'L DATA PRIVACY L. 195, 198-99 (2012), available at

[32]*Akdeniz, Y. and Walker , C.*, Whisper Who Dares: Encryption, Privacy Rights, and the New World Disorder, *University of Leeds, United Kingdom available*at[http://www.isoc.org/inet99/proceedings/3g/3g_3.htm (January](http://www.isoc.org/inet99/proceedings/3g/3g_3.htm) 14, 2015)

[33]Brown, I.&Korff, D.Global Network Initiative, Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online (2012), available

operate even against repressive regimes that have closed other avenues of communication for dissent.[34]

The responsive and sensitive governments have policy changes, ranging from totally outlawing encryption.[36] Previously, the US governments would not allow encryption but privacy right activists brought all their arguments and the US government acceded to a 64 bit encryption.[35] A 128 bit encryption is still outlawed because even with brute force, it would still take security experts a long time to unravel and decipher messages therein. This time could mean the difference between apprehending a criminal before he commits the crime, a terrorist before the plans are implemented and thebombs detonated and arresting an offender after the fact. This is the difference between arresting a terrorist before he detonates his bombs - with all the implications in terms of human life, resources, property value and State security and arresting him after he has detonated it. Imagine still if he is a suicide bomber, what has law enforcement gained?The difference in law enforcement between prevention and punishment. This basically answers proponents of the theory of unrestricted encryption who argue that security agencies have expert personnel, programs and technology for decrypting encrypted data.[36]

Conclusion

The right to privacy is still a fledgling area of Nigeria law. Nevertheless, the right is constitutionally guaranteed and protected by the Court. It is also set out in most international human rights conventions as enshrined in Article 8 of European Convention on Human Rights (ECHR) and Article 12 of the Universal Declaration of Human Rights.

The implications of this are direct: protection of privacy in some form is built into almost every legal system, whether explicitly in statute or via some kind of common law principles. Across the world, governments have acknowledged the importance of technological change in the daily lives of the people. Notwithstanding the effect on privacy, we still communicate over the net as it is still the most convenient form, we still need to supply sensitive and personal information data form and make financial transactions via the net; and we still need to secure this piece of information against data and identity theft and fraud through encryption. With all of the access to the internet in today's world; encryption has emerged as one of the ways, perhaps the surest way in guaranteeing security and privacy on the net. It has however not address totally the abuses on privacy.

There is therefore absolute need to radically address the problems associated with encryption to expand the horizon of privacy right and address the inherent inhibitions.

Recommendations

In the light of the issues and challenges highlighted above, arguments can be advanced for 2 sets of strategic actions to maximize Information Technology gains and reduce our vulnerabilities in that context – one is a global call to action which includes proposals to all countries on structures to be put in place to maximize for State benefits and world peace, the encryption and privacy instruments and technology; and the other consisting of suggestions to African countries on mechanisms for maximizing the gains of IT and minimizing their vulnerabilities thereunder in the context of their peculiar circumstances. This third leg may be applied, with some slight modifications, to third world countries.

Argument for Strategic Global Action

1. **Cooperation in the Realization of our truly Interdependent World**

   States should create dialogues and form agreements to help clarify the contours of privacy and encryption technologies, focusing on mutual interests, interdependence, and coexistence rather than perceiving the net as a zero-sum resource. States must cooperate in the realization of a truly interdependent world. Without States cooperation at the international level, national legislation may remain incapable of enforcement. Internet accidents are an illustration of how issues of IT governance defy territorial, jurisdictional and geographical boundaries. When there is an incident on the net, the impact is likely to be manifold: It will affect the countries whose nationals originated the transaction and the countries in whose jurisdictions the facilities hosting the different segments of the transaction are located as well as the country whose nationals are victims of the transaction.

   We need such international cooperation to ensure the safety and security not only of the net, but also of the whole world as no single State has the resources-manpower or material- to deal effectively with the threats to and arising from the net alone. Enhanced cooperation among States on net governance efforts can only benefit everybody.[37]

   As early as 1994, the Bangemann Report to the European Commission dealt with the use of encryption tools and stated that a solution at a national (member State) level will inevitably prove to be insufficient because communications reach beyond national frontiers and

athttp://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law_0.pdf(Janl4, 2015)

[33] Land, M. B. Google, China, and Search, ASIL Insights Issue: 25, Volume: 14, August 05, 2010

[35] The more the bit, the harder it is to decipher an encryption code without the key

[36]Couillard, D. Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing Electronic copy available at: http://ssrn.com/abstract=1832982(Jan.4, 2015) Accessed 14th January, 2015

[37]Swire, P. and Ahmad, K., Encryption and Globalization in The Columbia Science & Technology Law ReviewVol. XIII, Spring 2012; van Hoboken, J. and Rubinstein, I.Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era in Maine Law Review [Vol. 66:2 2014]

because the principles of the internal market prohibit measures such as import bans on decoding equipment. Therefore, according to Bangemann a solution at the European level was needed "*which provides a global answer to the problem of protection of encrypted signals and security. Based on the principles of the internal market it would create parity of conditions for the protection of encrypted services as well as the legal framework for the development of these new services"*[38]

Strengthening International Institutional ArrangementsandDeveloping International Rules and Standards

The world needs a framework or an "umbrella" Convention whose provisions will set out general principles, which will be effectively implemented following the adoption and implementation of other instruments. States will be required to cooperate at the global, and as appropriate, on a regional basis, directly or through competent international organizations, in formulating and elaborating international rules, standards and recommended practices and procedures, while providing the principles on which action should be based.

This would include enhanced information and manpower sharing among member states to tackle the most of the challenges arising from net governance, provision for information exchange, cooperative enforcement action, capacity building and other cooperative arrangements and supplementing the framework by providing a mechanism to enhance the protection and safety of the world's net spaces. A key pillar of this would be an Information Sharing Centre for reporting, studies of incidents; issuance of alerts and information sharing among member States. It would facilitate communications and information sharing among national focal points of member countries, as well as improve the quality of statistics and reports on global IT governance challenges.

Existing institutions that might benefit from support and in turn, be of greater global use if strengthened include the ***International Telecommunication Union(ITU).***

This also requires States to establish international rules and standards throughthese international organization(s) or general diplomatic conferenceand to re-examine these rules and standards from time to time as necessary. To maximize the gains of the net therefore, there is a need for international rules to be developed by competent institutions regulating these details in line with the general spirit of IT Governance particularly in the context of privacy laws and encryption technology.

2. National Legislation Development

Once, international rules and standards have been adopted, they must be implemented in national legislation for the realisation of the objectives set therein either as a minimum standard or as a guiding principle and be subsequently enforced.

The authority that is to be accorded to these rules and standards vis-a-vis the enactment of national laws and standards may vary according to the type of activity being regulated.

States will have to adopt international rules and standards as minimum standards in national laws, or they may enact standards more stringent than the global minimum.

Argument for Strategic Action Plan for African and ThirdWorld Countries

1. Regional Cooperation

The transnational nature of IT issues highlights the need for regional IT cooperation between States.The need for regional IT cooperation is accentuated by the lack of capacity by most African coastal States to individually address IT governance issues that present any degree of complexity. There is a need to establish real and effective regional IT cooperation in Africa, and there is a need for a more integrated regional approach and cooperation between African States with regard to IT governance.

Regional cooperation is perhaps the best avenue through which African States can achieve order in the governance of their net. The challenges of governing internet spaces can be daunting if handled unilaterally by individual States acting in its national interest.Through regional cooperation African States can pool both financial and human resources for use in the internet governance process. This will enable Africa to move in tandem with the rest of the world. African States can be as successful if they improve regional cooperation in governing their IT interests.

African States need to identify a forum in which they can chart modalities for regional cooperation in the governance of their IT areas. The AU, for instance enjoys considerable goodwill among African States. It could establish specialized organs through which the agenda can be handled. Alternatively, a mechanism for cooperation could also be fashioned after the Abidjan Convention.[39]

A first requirement for enhancing such regional cooperation is the identification of the possible areas of cooperation. These should focus on the common challenges facing African States in internet governance. Key among these are security and surveillance, and controlof data access.

The next step would be to identify the common goal and objectives to be reached by such regional cooperation. One of these objectives should be the integrated exploitation and governance of African net space and its resources for the common good of the people of Africa.

A strategic plan and policy for the regional cooperation should be developed at the continental level that maps out key actions to be taken in fostering regional cooperation. The strategic plan should outline the

[38](Bangemann Report, 1994).

[39] Convention for Co-operation in the Protection and Development of the Marine and Coastal environment of the West and Central African Region, 1984

priorities of the cooperation as well as identify the structures and institutions, both at national and regional levels, through which the plan can be realized. For example, African authorities should be encouraged to share information that could help to curb internet security problems and reduce incidents of internet based crimes.Africa's seemingly nonparticipation in IT governance issues at a global level is perhaps due to the lack of technical or human capacity by the African states- but this challenge could be overcome by a joint African state operation.

Training, research and exploration institutions must also be strengthened at a regional level, perhaps by means of an overall coordinating body that could ensure sharing of data and information on IT resources. An African regional disaster response institution should be set up under this arrangement to coordinate responses to IT-based disasters.

The long-term objective should be the establishment of a standing African internet guard and data regulatory service to compliment the national internet and data regulatory services.

A fund administered under this scheme of cooperation should be set up to finance the operations of regional IT cooperation organisations. The fund can be financed through contributions from member States out of the collection of licencing charges on net hosting and other facilities charges.

In view of their peculiar and ever-increasing challenges in the governance of their internet spaces, African countries must share intelligence and coordinate their internet surveillance, reconnaissance and security enforcement activities. The cooperation program should emphasise regional cooperation between member States to enhance internet security. The Common African Defence and Security Policy and the African Standby Force (ASF) should include an IT strategy to combat the increasingincidents of internet-based attacks that threaten the common good of theAfrican region. Africa's capabilities need to be assessed and appropriate elements placed at the disposal of the AU Standby Force. Till date no large peacekeeping operation within Africa has involved IT forces, even though such an arm could be used to help bring peace to Africa. Legitimate governments should be supported to ensure that criminal gangs who operate on the net do not have bases from which they can launch their operations.

African States should turn around the uncoordinated approach that has characterised regional cooperation in the governance of African IT interests by putting in place a better planned and coordinated approach that guarantees better results in the move towards maximizing their gains from the current global IT regime. Regional cooperation not only encourages maximum participation by the regional nations, but also favour cost effectiveness and transfer of technology to the developing nations.

Regional cooperation is an indefeasible part of the IT governance system as the regional level is the apt level for solution of motley of problems which transcend the limits of national jurisdiction but are not global in scope.

2. National Legislation Harmonisation

There is need for harmony of legislation of States that clearly and specifically contains how nations will go about discharging their duties and obligations under the international and regional frameworks. Moreover, States should ensure the enactment of such laws as impose standards and benchmarks in line with international benchmarks for the protection of the IT environment, the guarding of their sovereignty as well as the overall maximization of benefits accruing to them within international IT regime. Nigeria for instance, has the Communications Act, although this piece of legislation has not thoroughly addressed the issues in this discourse.

Perhaps, better still, it would make sense to create new and comprehensive legislation in line with what is obtainable in other jurisdictions, to deal with all the various issues arising from internet governance.

Besides this, it is imperative that states internalize the provisions of the international framework by local legislation particularly in places, like Nigeria, where the grundnorm[40] provides for a further legislative procedure before international law takes internal effect.

3. Capacity Building

Much of the problems that plague the third world countries is either caused or exacerbated by a deficit in capacity, especially manpower and resources to take advantage of opportunities and minimize vulnerabilities/limitations. Although the third world countries may have technology transferred to them from their industrialised counterparts under current IT regimes, the technology might not benefit them much as there is no point transferring technology without manpower on ground that understands the workings thereof or indigenous support technology on which the transferred technology can be built. Nigeria for instance will only have the oil and gas industry situation- all of the technology capable of transfer without adequate manpower to run it still results in an underdeveloped sector.

Capacity building would also entail developing and improving R&D and institutions devoted thereto.

4. Political Will

One of the prerequisites for beneficial participation is consistent and strong political commitments and stable political and security environment at the national level- that which is generally referred to as political will, the willingness and readiness to act by policy making and action taking along a certain line in the achievement of desired objectives. This will entail acting without fear of repercussions from their donor and aid giving countries, acting in the best interest of the citizenry without undue pressure from external influences, taking decisions and actions outside the influence of outside parties who make it a deliberate policy to constantly try to influence

[40]That is, the Constitution of the Federal Republic of Nigeria, 1999 (as amended), Sections 1 and 12

decisions and government actions.

In this context, it must be noted that nations can only build and exercise political will when internal capacity in terms of resources, materials, manpower and economy has been built and strengthened to such an extent that dependence on external support and assistance is only marginal because the level of influence external factors are capable of exerting on policies and decisions is directly proportional to the level of dependence on such external factors for aid.