International Journal of Internet of Things 2014, 3(1): 8-17
DOI: 10.5923/j.ijit.20140301.02

Internet Secrecy Laws and Its Implications on Developing Nations

Onifade O. J.[1,*], Osunade O. O.[2], Oyedele O. E.[3]

[1]National Centre for Technology Management, Obafemi Awolowo University, Ile-Ife
[2]Department of Computer Science, University of Ibadan, Oyo State
[3]Centre for Distance learning, Obafemi Awolowo University, Ile-Ife

Abstract What is being regarded today by everyone as internet started many years ago (in the early 1960's) as simple Network ideas intended to allow general communications among computer users.. The initial concept of the internet was based on the idea that there would be multiple independent networks of rather arbitrary design, beginning with the Advanced Research Projects Agency Network (ARPANET) as the pioneering packet switching network. As time went by, and as the technology advanced, internet also has gone through a serious revolution that has come with some sort of issues / challenges. One of such issues is concerned primarily with the internet security and how well can internet be regulated or controlled. As is generally believed by most internet users that the internet or the cyber space is such an *'open world'* with little or no control, but it has been proved over the years that the cyber world is not as open as people think, and that some form of measures have been and can still be put in place to regulate it. This work therefore address all these factors that can generally contribute to Internet Secrecy and the consequent effects this will have on the developing nations of the world.

Keywords Internet, Privacy, Information Communication Technology, Regulation, Developing Nations

1. Introduction

Information and communications technologies have become indispensable to the modern lifestyle. We depend on information and communications infrastructure in governing our societies, conducting business, and exercising our rights and freedoms as citizens. In the same way, nations have become dependent on their information and communications infrastructure and threats against its availability, integrity and confidentiality can affect the very functioning of our societies.

The security of a nation's online environment is dependent on a number of stakeholders with differing needs and roles. From the user of public communications services to the Internet Service Provider that is in charge of the infrastructure and handling everyday functioning of services, to the entities ensuring a nation's internal and external security interests – every user of an information system affects the level of resistance of the national information infrastructure to cyber threats. Successful national cyber security strategies must take into consideration all the concerned stakeholders, the need for the awareness of their responsibilities and the need to provide them with the necessary means to carry out their tasks. Also, national cyber security cannot be viewed as merely a sectoral responsibility: it requires a coordinated effort of all stakeholders. Therefore, collaboration is a common thread that runs through most of the currently available national strategies and policies.

Moreover, the different national cyber security strategies represent another common understanding: while national policies are bound by the borders of national sovereignty, they address an environment based on both infrastructure and functioning logic that has no regard for national boundaries. Cyber security is an international challenge, which requires international cooperation in order to successfully attain an acceptable level of security on a global level.

In a bid for different nations of the world particularly the very technologically advanced nations to protect their online resources and ensure strict security measures against cyber challenges, some developing nations might be put at disadvantage when it comes to having access to online resources and protecting themselves against cyber threat.

2. Brief Internet History

The first recorded description of the social interactions that could be enabled through networking was a series of memos written by J.C.R. Licklider of MIT in August 1962 discussing his "Galactic Network" concept. He envisioned a globally interconnected set of computers through which

* Corresponding author:
banjionifade@gmail.com (Onifade O. J.)
Published online at http://journal.sapub.org/ijit

everyone could quickly access data and programs from any site. In spirit, the concept was very much like the Internet of today. Licklider was the first head of the computer research program at DARPA (Defense Advanced Research Projects Agency), starting in October 1962.

While at DARPA, he convinced his successors at DARPA, Ivan Sutherland, Bob Taylor, and MIT researcher Lawrence G. Roberts, of the importance of this networking concept. Leonard Kleinrock at MIT published the first paper on packet switching theory in July 1961 and the first book on the subject in 1964. Kleinrock convinced Roberts of the theoretical feasibility of communications using packets rather than circuits, which was a major step along the path towards computer networking. The other key step was to make the computers talk together. To explore this, in 1965 working with Thomas Merrill, Roberts connected the *TX-2 computer* in Massachusetts to the *Q-32* in California with a low speed dial-up telephone line creating the first (however small) wide-area computer network ever built. The result of this experiment was the realization that the time-shared computers could work well together, running programs and retrieving data as necessary on the remote machine, but that the circuit switched telephone system was totally inadequate for the job, Kleinrock's argument for packet switching was confirmed.

Figure 1. TX-2 computer (Source: www.boerner.net/jboerner/?p=2846)

Figure 2. Q-32 computer (Source: ed-thelen.org/comp-hist/q32_2-.jpg)

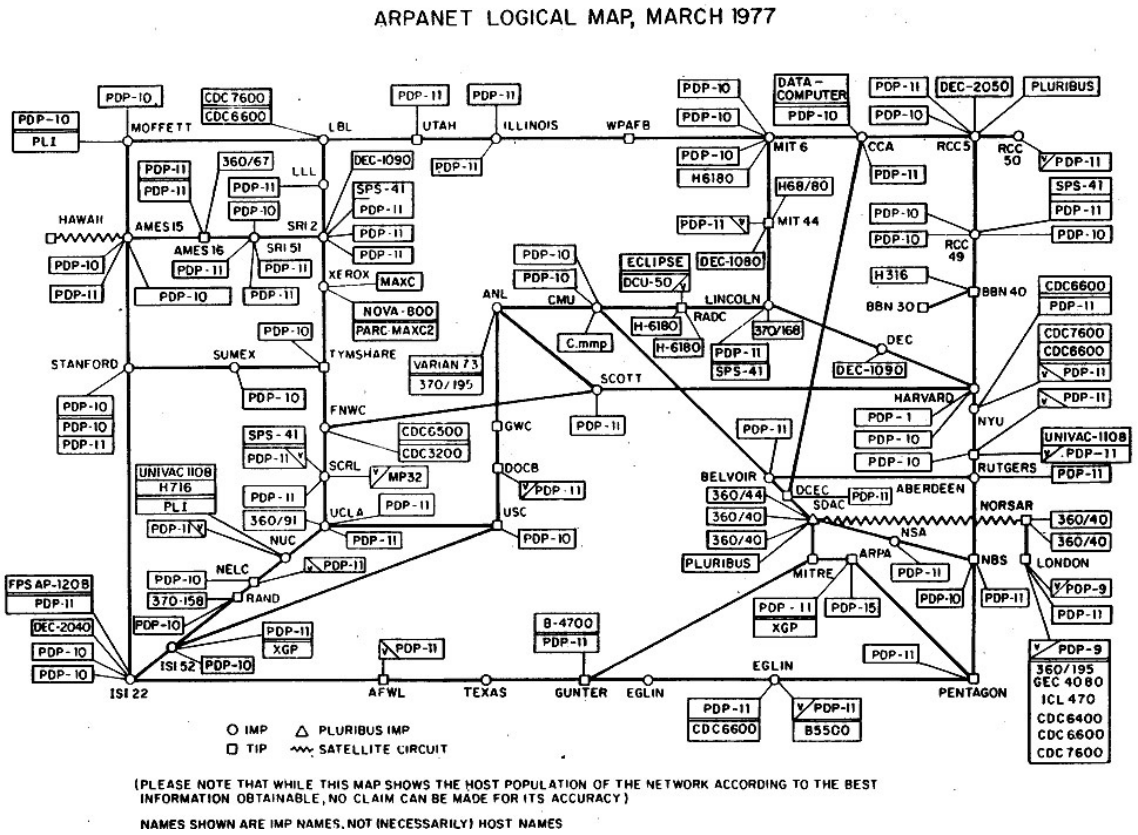

Figure 3. ARPANET Logical Map / Architecture (Source: en.wikipedia.org)

2.1. The Initial Internetting Concepts

The original ARPANET grew into the Internet. Internet was based on the idea that there would be multiple independent networks of rather arbitrary design, beginning with the ARPANET as the pioneering packet switching network, but soon to include packet satellite networks, ground-based packet radio networks and other networks. The Internet as we now know it embodies a key underlying technical idea, namely that of open architecture networking. In this approach, the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level "Internetworking Architecture". Up until that time there was only one general method for federating networks. This was the traditional circuit switching method where networks would interconnect at the circuit level, passing individual bits on a synchronous basis along a portion of an end-to-end circuit between a pair of end locations. It should be noted that Kleinrock had shown in 1961 that packet switching was a more efficient switching method. Along with packet switching, special purpose interconnection arrangements between networks were another possibility. While there were other limited ways to interconnect different networks, they required that one be used as a component of the other, rather than acting as a peer of the other in offering end-to-end service.

2.2. Circuit Switching Vs Packet Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit. Example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

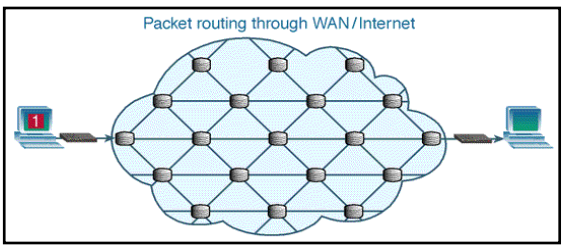

Figure 4. Packet-switched Network (Source: aafrin.com/2011/05/12/example-circuit-switching-vs-packet-switching)

2.3. Packet Switching

Packet switching breaks data into chunks (small data packets) and wraps the chunks into structures called packets. Each packet contains, along with the data load, information about the IP address of the source and the destination nodes, sequence numbers and some other control information. A packet can also be called a segment or datagram. Once they reach their destination, the packets are reassembled to make up the original data again. It is therefore obvious that, to transmit data in packets, it has to be digital data.

3. Common Online Security Threats

3.1. Viruses, Phishing and Identity Theft

Identity theft is considered the fastest-growing financial crime. It occurs when a thief assumes the victim's identity in order to apply for credit cards, loans or other benefits, in the victim's name, or uses this information to access user's existing accounts. The thief will accumulate massive debt or deplete user's current assets and then move on to another stolen identity. The victim, meanwhile, may end up thousands of dollars in debt, with a ruined credit history or with an empty bank account. Until cleared up, this can make it difficult to find a job, buy a car or home, obtain a student loan, or engage in other activities that depend on the use of good name.

3.2. ADS, APPS, and Personal Privacy

Computers have the capability to collect a great deal of information about users, and to transmit that information to third parties including advertisers and advertising networks. America's online advertising industry generated about $31.7 billion in revenue in 2011, an increase of 22 percent over the previous year, according to media reports. This big and competitive business is fueled in large part by the buying and selling of personal data, such as Internet browsing habits and user characteristics.

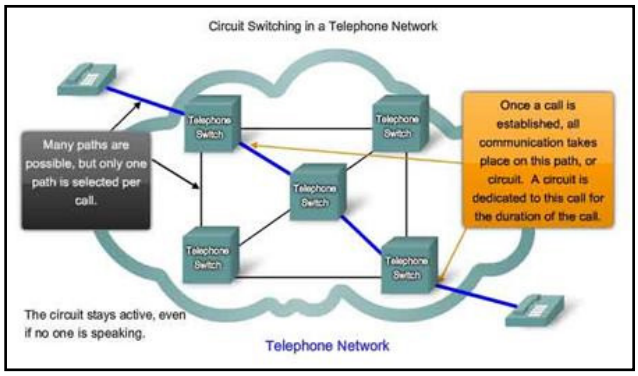

Figure 5. Circuit-switched Network (Source: highteck.net/EN/Basic/Internetworking.html)

3.3. Online Predators and Cyberbullies

A Perth Amboy man pleaded guilty in August 2012 to sexually assaulting two teenage girls he stalked through Facebook. The 29-year-old created a profile using a fake name, pretending to be 17. He "friended" the 14-year-old girls, and began sending sexually explicit text messages. One

girl met with him in person. The other rejected his advances–but by reading her Facebook status updates he was able to track her whereabouts. Both girls were sexually assaulted.

Befriending teenagers with a fake online identity. Gradually coercing them with friendly, then flirtatious, then overtly sexual messages. Using a victim's online posts to learn when and where she would be hanging out. These are common ways sexual predators use the Internet. One of the best-known cases of cyberstalking from the last decade is that of Jonathan Vance, who hid behind the screen name Metascape, according to media reports. He attempted to take over the Facebook, MySpace, and email accounts of more than 200 girls and young women, ages 14 to 26, and terrorized and blackmailed at least 53 of them into sending sexual photos of themselves.

4. Is the Internet Controllable?

Broadly speaking, Internet regulation today according to Froomkin, 2003, can be conceived of as involving three related spheres: Direct regulation of the internet infrastructure itself; regulation of activities that can be conducted only over the internet; and, regulation of activities which can be, but need not be conducted over the Internet. The first sphere: Direct regulation of the internet infrastructure itself, including: the standards of communication, the equipment used to provide and access Internet communication, intermediaries engaged in the provision of Internet communications, e.g. Internet Service Providers (ISPs). The second sphere: Regulation of activities that can be conducted only over the internet and which have no significant off-line analogues. An example is the regulation of anonymous online communication via anonymizing re-mailers. The third sphere: Finally, there is the regulation of the enormous category of activities which may or may not be conducted over the internet, e.g. e-commerce in both tangible and intangible goods. In many cases the Internet version of an activity often will simply be swept up in the general regulation of the type of conduct. (In some cases, however, the Internet version may be subject to special or additional regulation because the use of the Internet is seen as somehow aggravating an underlying problem or offense. An example of this is US attempts to regulate the provision of obscene or "indecent" content to minors via the Internet.

4.1. Phases of Internet Regulation

There are four phases of Internet regulation, which are the ***"open Internet"*** period, from the network's formation through around year 2000 and thereabout; ***"access denied,"*** through about year 2005; ***"access controlled,"*** through the present day (2013); and "***access contested***," which is the future phase of the internet.

4.1.1. Phase 1: The Open Internet (the 1960s to 2000)

The first phase, roughly from the Internet's initial formation in the 1960s through about 2000, is the period of the "open Internet." This term was intended to convey descriptive, predictive, and normative meanings. During this initial period of the network's development, the dominant theory – to the extent that anyone was thinking seriously about regulation at all – was that the Internet itself was a separate space, often called "cyberspace." The concept of cyberspace melded the creativity of the science fiction writer with the aspirations of the democratic theorist dreaming of a fresh start. As a descriptive matter, there was much truth to the argument: up until the late 1990s, most states tended either to ignore online activities or to regulate them very lightly. When states did pay attention to activities online, they tended to think about and treat them very differently from activities in real-space. The term proved inaccurate as a predictive matter. On a normative level, there is still salience to the concept of the open net that is worth continuing to bear in mind.

4.1.2. Phase 2: Access Denied (2000 to around 2005)

The second phase of development of the Internet, from roughly 2000 to 2005, is the "Access Denied" period. During this second era, states and others came to think of activities and expression on the Internet as things that needed to be blocked or managed in various ways. The thinking was that certain acts of speech and organizing online needed to be regulated like any other. The initial reaction, by states such as China and Saudi Arabia in the first instance, was to erect filters or other means to block people from accessing certain information. The world may appear borderless from when seen from cyberspace, but geopolitical lines are in fact well-established online.

4.1.3. Phase 3: Access Controlled (2005 to 2013)

The third phase, from 2005 roughly to the present day, is the "access controlled" phase. Access controlled characterizes a period during which states have emphasized regulatory approaches that function not only like filters or blocks, but also as variable controls. The salient feature of this phase is the notion that there are a large series of mechanisms, at a variety of points of control that can be used to limit access to knowledge and information. These mechanisms can be layered on top of the basic filters and blocks established during the previous era. (Deibert and Rohozinski, in Deibert et al. 2010: 3 - 12.).

During this Access Controlled period, states have also increased the number of points of control that are possible on this network and their use in combination. The image of the *"Great Firewall of China"* is evocative and, to some extent, accurate as a descriptive matter. But it is misleading insofar as it tells only a small part of the story of control online, in China and elsewhere.

4.1.4. Phase 4: Access Contested (2013 and beyond)

We are headed into a fourth phase, called "access

contested." The key notion behind this new phase is that there is, and will be more, pushback against some of these controls. There is an ongoing contest over what this hybrid environment will look like over time. There is a growing political debate about the way in which these regulations are carried out by states around the world. At a state-to-state level, the militarization of cyberspace that has been happening over the last few years is an important part of this emerging narrative. The growing centrality of activities online to life in general is the primary driver of these contests. From the perspective of Internet users, online activity is increasingly a part of everyday life – not a separate sphere to which they travel occasionally, as if on vacation. States, too, have come to recognize that activities mediated by digital technologies are deeply important in economic, political, and cultural ways as a critical mass of their citizens, businesses, and NGOs come online. The metaphor of "cyberspace" as a space, akin to "real space," breaks down in this respect. The technological mediation of these activities changes some things – for instance, the technology brings with it specific affordances for the activist in getting her word out and the spy in snooping on Internet traffic as it passes – but it does not change the underlying dynamics of states, companies, individuals, and groups. In the "access contested" phase, the regulation that states have imposed in the earlier phases is giving rise to strong responses from the private sector and from other states unhappy with this regulation.

5. The Internet in Developing Nations

The last decade has witnessed an unprecedented diffusion of network technologies into developing countries. The technological discourse attending and encouraging the adoption of the new media, particularly the Internet, has centered on their potential to accelerate national development efforts, bring about favorable socio-cultural changes, and open up public spheres for free and democratic discourse (Hudson, 2000; Huff, 2001; Wei & Kolko, 2005; Gher & Amin, 1999; Fandy, 2000). Huff (2001, p.43), for example, suggests that "the presence of the Internet can be expected to transform politics and commerce, and will have a major impact on the conduct of government and economic affairs in developing countries."

5.1. The Evolution of Internet in the Developing Countries

The commercialization of the Internet has allowed the corporate to shift emphasis from producing and controlling material goods to controlling information. Information became "something produced, exchanged, and used within the framework of a market economy" (Agre, 2003, p. 755). This shift to an information-based economy has necessitated new information-based domains and new markets. This explains the intense competition among major technology industries to extend their control over universities, schools, libraries and other public spheres. The ensuing information revolution has generated a dynamic economic sector, incorporating web-based companies, virtual universities, cyber-stores, and so on. Even industries that do not rely heavily on information have utilized the Internet to propagate their merchandize, attract more clientele, reduce secretarial labor, and gain more profit through online sale activities. Commercial undertakings have become a characteristic feature of the World Wide Web in particular, shaping its design, tone, content, language, and usage. The economic boom introduced by the Internet in terms of flow of money, job creation and increased efficiency has given Western industries and business a competitive advantage in the regional and global marketplace. In fact, the Internet has helped renew Western economic hegemony through controlling the information capital, the lifeblood of the new information-based industries (Noble, 1998). These advantages have prompted the technology industries to internationalize the new medium, extending its reach to more than 1.24 billion international users within less than fifteen years (Internet World Stats, 2007). This technological explosion did not happen by chance, especially if we consider the huge profits that the electronic corporate giants (Google, Yahoo, Ebay, Amazon, etc.) have reaped from online business. According to the Silicon Valley Investment Indicators (2006), the net profit of each of the top ten electronic companies was above $ 1 billion in 2005. The internationalization of the Internet not only helped Western corporations extend their marketplace worldwide but also facilitated the world's shift to a more open and global society.

5.2. The Internet as a Tool of Economic Domination

Decisions to introduce the Internet into many developing countries, whether for government or public use, follow from the unquestioned assumption that network technologies are a prerequisite for bridging the technical and scientific gap with industrialized countries and, consequently, for "development." The implementation of the Internet was also stimulated by fears of exclusion from the global ICT world (Hudson, 2000; Anderson, 2000; Huff, 2001). The general sentiment for computerization among decision makers in developing country is reflected in Allotey's speech to top decision makers in Ghana: "we paid the price of not taking part of the industrial revolution of the late eighteenth century because we did not have the opportunity to see what was taking place in Europe. Now we see that information technology has become an indispensable tool. We can no longer sit down and watch passively" (cited in Sagahyroon, 1995, p. 164).

5.3. The Internet as a Tool of Cultural Domination

While the Internet diffusion into developing countries is highly profitable to the computer industry, "it is also an experiment with the basic symbolic and moral foundations of mainstream Western culture- and how these foundations are inter-generationally renewed" (Bowers, 1998, p. 112).

Obviously, the Internet and other information technologies carry the values and ideas of the Eurocentric society, which has played a critical role in the design and development of the media.

The paradox in the rush to embrace the network technologies by developing countries is that ICT importers hardly understand the culturally mediating characteristics of the technology (Bowers, 1998). Bowers asserts that computer technologies select Western cultural patterns for amplification, while other cultural experiences are reduced or eliminated altogether. He further contends that socializing non-Western people into the patterns of thinking amplified through the use of computer technologies "is a form of cultural domination". Because their structures reflect the culturally specific thinking ways of their developers, many Internet applications require users to adjust their normal ways of doing things in their local cultures (e.g., writing from left to right; relying more on symbols and sounds than on contextual clues and gestures in online interactions; linear progression in web reading, email writing, and other online activities; etc.).

5.4. The Internet as a Tool of Political Domination

As in much of the current development literature worldwide, discussions of the introduction of the Internet have focused extensively on the promise of the technology to bring about democratic transitions to developing countries (Huff, 2001; Hudson, 2000; Anderson, 2000; Ghareeb, 2000). Because it permits easy, inexpensive, and rapid exchange of information, the Internet, it is argued, empowers ordinary people to receive, produce, and circulate information and ideas, and thus helps to break up state monopoly of information and creates new public political spheres (Ghareeb, 2000; Fandy, 2000). In many cases, the common wisdom that the Internet will lead to positive political changes lacks any specification of the mechanisms through which the change might occur (Khalathil & Boas, 2003). Rather, as Khalathil and Boas note, "popular assumptions often rest on anecdotal evidence drawing primarily on isolated examples of Internet-facilitated political protests." The implicit starting point in the current discussions on the Internet's democratic potential is that the increased availability of information automatically leads to greater political participation. As Winner (2003, p. 594) puts it, a "serious misconception among computer enthusiasts is the belief that democracy is first and foremost a matter of distributing information."

6. Internet Secrecy / Privacy Laws

Internet secrecy law or policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data. Personal information can be anything that can be used to identify an individual, not limited to but including; name, address, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services.

6.1. Internet Secrecy Laws as applicable in Developed Nations (US as a Case Study)

Data privacy laws apply in most part of the world regardless of industry, source or region. In the US for example, there are several laws put in place to control how information and resources are accessed on the internet. Some of these laws, when fully enforced can seriously affect how people have access to some online resources. Some of these laws are as highlighted below:

The Children's Online Privacy Protection Act (COPPA): The Children's Online Privacy Protection Act affects websites that knowingly collect information about or target at children under the age of 13. Any such websites must post a privacy policy and adhere to enumerated information-sharing restrictions. COPPA includes a "safe harbor" provision to promote Industry self-regulation. Congress, under the Clinton Administration, and the Federal Trade Commission (FTC) initially focused their attention on protecting the privacy of children under the age of 13 as they visit commercial websites. Not only are there concerns about information children might divulge about themselves, but also about their parents. The result was the Children's Online Privacy Protection Act (COPPA). This type of Act in developing nations of Africa where child abuse is imminent and children are being defiled on daily bases may reduce the risk of children vulnerabilities.

***The Family Educational Rights and Privacy Act (FERPA*)**: Among its several purposes, the Family Educational Rights and Privacy Act (FERPA) was enacted to protect the privacy of students' education records, to establish the rights of students to inspect and review their education records, and to provide students with an opportunity to have inaccurate or misleading information in their education records corrected. FERPA also permits the disclosure by an institution without a student's prior consent of so-called directory information about that student. Students have the right to file complaints with the Department of Education's Family Policy Compliance Office concerning alleged failures by an institution to comply with FERPA.

Protection of Pupil Rights Amendment (PPRA): The Protection of Pupil Rights Amendment applies to any "local educational agency" that receives funding from the U.S. Department of Education. A "local educational agency" means an elementary school, secondary school, school district, or local board of education that is the recipient of funds from the U.S. Department of Education (ED). It does not include postsecondary institutions. PPRA also applies to research funded by the Department of Education. The focus of PPRA is on the requirement for parental consent for the collection of certain sensitive information, such as medical data or sexual attitudes or practices from school children via

surveys and evaluations.

6.2. Electronic Communications Privacy Act (ECPA)

Since this law is setting standards for how the government can access digital information of citizens passed in 1986, technology has changed dramatically, but the law has not. Proponents of ECPA reform say the most egregious portion of the law involves the rights the government has to obtain electronic files without needing a warrant. "A paper letter sitting in your home or office drawer has a significantly higher level of constitutional protection compared to an email right now," says Robert Holleyman, president of the Business Software Alliance, who backs changes to ECPA to strengthen consumer and business privacy. ECPA allows the government to obtain access to digital communications -- including email, Facebook messages, information sitting in your public cloud provider's databases, and a variety of other files -- with only a subpoena and not a warrant once those items are 180 days old. To provide a scope of how much information companies hand over to the government, Google recently reported that it coughed up more than 18,000 requests for information from the government in the second half of last year alone. There is already movement afoot on Capitol Hill to change this. Last year, the Senate Judiciary committee passed an update to ECPA, but it failed to reach a vote on the full Senate floor. This month, members of the House of Representatives filed an update to ECPA, so the debate will ramp up again soon.

6.3. Cyber Intelligence Sharing and Protection Act (CISPA)

CISPA stands for The Cyber Intelligence Sharing and Protection Act, a network and Internet security bill written by Rep. Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD) (H.R. 624). The bill purports to allow companies and the federal government to share information to prevent or defend against network and other Internet attacks. However, the bill grants broad new powers, allowing companies to identify and obtain “threat information” by looking at your private information. It is written so broadly that it allows companies to hand over large swaths of personal information to the government with no judicial oversight—effectively creating a “cybersecurity” loophole in all existing privacy laws.

At a basic level, CISPA dictates how companies share information about cyber threats with the federal government. Opponents to the legislation, like the Electronic Frontier Foundation (read an FAQ about CISPA from the EFF here), are worried about what they call inadequate privacy protections given the broad definitions of cyber threat.

Experts agree, private info not needed for sharing cyber threats with government Equally concerning, according to Mark Stanley, head of campaigns and communications for the non-partisan Center for Democracy & Technology (CDT), is that information companies turn over to the government goes to the National Security Administration, he says, which is a military division of the government.

6.4. Computer Fraud and Abuse Act (CFAA)

Internet freedom fighters mourned the loss of anti-SOPA (Stop Online Privacy Act) organizer and Reddit co-founder Aaron Swartz earlier this year. Swartz was facing prosecution under CFAA, which has since been referred to by some as "Aaron's Law." Reform-seekers believe CFAA- which was passed in the late 1980s and updated a decade later- is too restrictive in banning information sharing. Swartz, for example, was charged with stealing millions of scholarly articles and documents from an MIT subscription-based service called JSTOR, and could have served jail time.

Generally speaking, CFAA makes it a federal crime to access and share protected information. Organizations like the EFF have called for CFAA reforms for years, though, specifically to reduce penalties for CFAA violations and to install clearer definitions of what a breach of CFAA is. It's unclear where CFAA reform stands at this point, though. Washington inside-the-beltway blog Politico recently reported that the Obama administration has been reluctant to support reform efforts.

6.5. Trans Pacific-Partnership Agreement (TPP)

While all the other internet-related privacy laws highlighted above are pertained only to U.S. legislative law, there is an international debate ongoing to establish standards for online sharing among countries on either side of the Pacific. Technology advocates are worried about what the TPP will mean for digital copyright laws both in the U.S. and internationally.

The TPP involves nine countries along the Pacific Rim, including the U.S., Peru, Chile, Vietnam, Singapore, Malaysia, Australia, New Zealand and Brunei, and soon Japan and Canada. The agreement could expand U.S. intellectual property (IP) standards to other countries, while reinforcing existing IP laws in America.

6.6. Stop Online Piracy Act (SOPA)

SOPA, an acronym for the Stop Online Piracy Act is a proposed bill that aims to crack down on copyright infringement by restricting access to sites that host or facilitate the trading of pirated content.

SOPA's main targets are "rogue" overseas sites like torrent hub The Pirate Bay, which are a trove for illegal downloads. It is hard for U.S. companies to take action against foreign sites. The Pirate Bay's servers, for example are physically located in Sweden. So SOPA's goal is to cut off pirate sites' oxygen by requiring U.S. search engines, advertising networks and other providers to withhold their services. That means sites like Google wouldn't show flagged sites in their search results, and payment processors like eBay's (EBAY, Fortune 500) PayPal couldn't transmit funds to them.

Those that Opposed the law (SOPA) claimed that the proposed legislation threatened free speech and innovation,

and enabled law enforcement to block access to entire internet domains due to infringing content posted on a single blog or webpage.

6.7. Protect IP Act (PIPA)

PIPA, the PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act) is an amendment/re-write of the failed Combating Online Infringement and Counterfeits Act (COICA). Under the proposed law, PIPA, would give the government and copyright holders tools to prevent access to *rogue websites* that are dedicated to counterfeit goods or infringe the intellectual property act. The bill was introduced on May 12, 2011 by Senator Patrick Leahy.

On January 18, 2012, several thousand websites opposing the law, including Reddit, Boing Boing, Wired, WordPress, Wikipedia and Mozilla Firefox launched a service blackout in protest of PIPA and another similar controversial bill, the *Stop Online Piracy Act (SOPA)*. During the service outage, participating websites closed down their websites and left readers with information about SOPA and PIPA, citing examples of what "could" happen if the SOPA/PIPA bills were passed.

7. Internet Secrecy Laws and the Developing Nations

It has been obviously put forward that most developing nations do not have standard, well-laid down legislations on internet privacy / secrecy like other advanced countries like United State, U.K, Germany, etc. Criticism of internet privacy as a global human concern focuses on how internet privacy is a modern concept that only applies in modern contexts. That is, the importance of internet privacy in developing countries may be limited by the lack of adequate industrialisation. In turn, without development there is no need for privacy. The argument here is that internet privacy is always technology-dependent and our conceptualisation of many developing countries is that they are well behind on technological development.

This view of the world does not reflect the current state of affairs in most developing nations nowadays, because the fact that most developing nations do not have a good and standard legislations in the area of internet privacy does not mean that such countries are not vast in internet-related technologies; in fact, Information and communications technologies are spreading quickly in the developing world.

SOPA could be problematic for some educational websites. For example, not all education technology apps and websites have the proper copyright permission for every single image or video they use. If they ever run into trouble that has legal ramifications, SOPA could play a role. It would also mean big problems for people looking to start their own education technology company. Young entrepreneurs worry its possibility of stunting intellectual and technological advancement.

Educational institutions may be restricted in how they use the Internet. It may affect how they harness the full potential of the Internet and reduce investment in Information Communication Technology.

Addressing the problem of copyright infringement is in the interest of all in the education sector. Intellectual property is essential to their mission; if they do not protect it, It makes their own work valueless, Moreover, the institution's bandwidth may be abused and its network resources misused to serve up content to downloaders all over the world. Illegal file-sharing can compromise networks with viruses, spyware and data security threats. It taxes the institution's resources in responding to infringement notices and engaging in disciplinary proceedings. It presents students with the prospect of facing legal action, and in some circumstances can even lead to potential liability for the institution itself.

Some other likely impacts could include:

- Any content that includes copyrighted content (such as webinar slides or white papers containing third party graphics, even if properly attributed) could potentially lead to a shutdown of the company's online presence.
- No free books and publications: Few people from developing nations particularly students, can afford to squeeze their credit cards, that is if they have them, to buy a book from an online shelve like amazon. Therefore all websites that currently offered such copyrighted books freely would come to a halt and our university, secondary students and researchers would have nothing to read.
- Network insecurity: Altering DNS results will make the network of institutions to be more vulnerable and may have small or no effect on infringement. Its impact is likely to be overbroad and result in blocking lawful expressions rather than infringements.
- Academic sites would be forced to be monitoring all activities of its users and prosecuting the defaulters.

7.1. The Internet Privacy / Secrecy Laws and the Associated Issues

Some of the internet privacy - related problems being faced by the developing nations can be categorized into two:

- *Issues arising from the strict application of Internet Privacy Laws*
- *Issues arising from the Laxity of Internet Privacy Laws*

7.2. Issues Arising from the strict application of Internet Privacy Laws

When strict internet privacy laws are in place, developing countries are bound to suffer a great deal, because as discussed below, a whole lot of activities going on in the developing countries are technology-driven.

Regulating the Internet through privacy / secrecy laws would automatically mean restricting the flow of information, as well as its exchange. It would suppress people from being

communicative and expressive, changing the way information is dealt with over the Internet.

It could also be argued that applying strict internet privacy laws may have a little control on the cyber-related crimes. Those who indulge in acts of abuse and illicit activity would only be forced to cover up their tracks better or go into hiding, if policies / acts came up to regulate Internet content. Some of other challenges associated with strict application of internet privacy laws are as explained below:

***Internet Privacy Laws can cause Economic Setbacks for the Developing Nations*:** The Internet provides a wealth of sources for information, products, and services of all types, making it a convenient place for consumers to research topics and make purchases, get free online resources, like open source software, educational contents, technological online collaboration, etc. With the issues of internet secrecy laws, all these will be put in check thereby having a negative effects on the overall economic output of the nation concerned.

In Nigeria for example, ICT contributed about 8% to the GDP in the country. The information and communication technology (ICT) sector continues to sustain its position as the fastest growing industry in the Nigerian economy. The sector has grown at an average of 34% per annum over the last 10 quarters, driven largely by the rapid expansion in telecommunication following the deregulation of the subsector in 2001. The industry's contribution to the Gross Domestic Product (GDP) is growing modestly from less than 0.5% in 2001 to 8% in 2014. With a population in excess of 170 million people, the ICT industry has the potential to drive the national economic growth at the much desired double digit rate. So any restriction placed by internet privacy laws will definitely hamper the economy.

7.3. Internet Privacy Laws and Political Issues

The widespread use of the internet has led to increased access to information and ability to communicate, to a higher level of participation and strengthened accountability. All of these aspects can deepen democracy and influence social and economic development. But these great opportunities also entail challenges to democracy. Surveillance of users' activities on the internet has been justified as crucial for national security. But internet control and mass surveillance of individuals may violate not only the right to privacy but also a series of other rights and freedoms – such as the freedom of expression, freedom of association and assembly, the right to information, etc. – and thus threatens to change peoples' use of the internet. Instead of being a tool for democratic development and empowerment, the internet could end up being a tool for increased control of populations on behalf of the state.

7.4. Issues arising from the Laxity in Internet Privacy Laws

There are many disadvantages associated with the Internet privacy laws. In reality, people have little privacy when using the Internet. For example, social networks provide little privacy protection. Facebook, as one of the most popular social networks, doesn't provide much privacy protection for their users. Facebook watches users and sees what kind of things they put in their profiles and what interests them. Facebook then shares this information with advertisers and these advertisers target the Facebook users and post their ads on their profiles to get their attention. Facebook has been changing its privacy policy to expose more personal information to a huge number of advertisers and marketers (Spring 2010).

Some more disadvantages of privacy and the Internet are **theft of personal information, spamming**, ***and security threats in terms of malware*.** When you use the internet, personal information can be stolen by many people. When you put things out online such as your name, credit card number, and where you live, these things are at risk of being used by other people (Pakhare 2011).

Child pornography is another issue associated with internet privacy. Pornography is an industry that is booming in the porn genre, simply because we live in a world where mentally sick men and women that have an absent conscience when it comes to young kids, exist among us. The Internet has material all over the place, where the authorities have been able to trace / ban these websites from public viewing. But the problem is that it can still be viewed through streaming porn websites where these are viewable for free without any kind of membership with a fee.

Fraud, defamatory activities and other criminal activities spread like wildfire throughout the internet, where businesses and individuals would be protected against such viciousness if strict internet privacy laws were in place. Story will not forget *Cynthia Osokogu* quickly who was murdered by her Facebook friends at Festac Town in Lagos State, Nigeria on 21st July, 2012.

7.5. Cyber stalking and Location Disclosure

Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass. Cyber stalking is often accompanied by real time or offline stalking. Both are criminal offenses, and are motivated by a desire to control, intimidate or influence a victim.

8. Conclusions

Rapid expansion of the Internet as it does for developed nations, holds substantial promise for developing nations, which have and can still benefit greatly from the Internet's communication and information delivery capabilities to help meet various needs. The accelerating transition of information to electronic media is making information resources of the world available to an increasingly global

audience through the Internet. Developing countries have much to gain from that revolution in communication and information access.

The communications and information delivery capability of the Internet serves all sectors of society. The areas of education, health, social policy, commerce and trade, government, agriculture, communications, and science and technology all benefit from Internet access to information and to individuals through electronic mail. These two resources are interlinked and synergistic: individuals can visit and exploit relevant information sources, which often point to additional sources of information and to knowledgeable individuals.

The correlation between information, communication, and economic growth is well-known, making the usefulness of networks nearly self-evident. Electronic networking is a powerful, rapid, and inexpensive way to communicate and to exchange information. When networks are available, previously unanticipated collaboration seems to come into being almost spontaneously. The underlying cause seems to involve a latent demand that remains latent as long as joint work requires either the disruption of waiting for the mail, the continual retyping of texts transmitted by mail or fax, or the need to secure large budgets and approvals for extensive international travel.

Also, it has been demonstrated in a number of countries recently, the link between the free flow of information and movement toward democratization cannot be downplayed. Access to information affects political democratization efforts at the global level as well as within nations.

The Internet has been a powerful driver of innovation and productivity around the world. Policymakers should always consider carefully any legislation that could impact this powerful creator of jobs and economic growth and stakeholders all across the globe should be encouraged to fully participate in a policy decision of this kind.

It is very obvious from all the points made above that internet technology has a very big role to play in every sphere of life in the developing nations, therefore any laws that affect smooth flows of activities on the internet will adversely affect the growth and development in these nations.

REFERENCES

[1] Albirini, A. 2006. “Cultural perceptions: The missing element in the implementation of ICT in developing countries”. International Journal of Education and Development using ICT, vol. 2, no. 1, pp. 49-65.

[2] Judge Grants, 2004. “NY Pop-Up Company Preliminary Injunction against Spyware Law”.

[3] Associated Press, June 23, 2004, 06:06 (via Factiva).

[4] Wallace, Brice. 2004. “Deseret Morning News”, E01 (via Factiva).

[5] Utah Anti-Spyware Bill Opposed by High-Tech Becomes Law. Warren’s Washington Internet Daily, March 25, 2004 (via Factiva).

[6] Agre, P. 2003 “Surveillance and capture: two models of privacy”. In Wardrip-Fruin & Montfort (Eds.), The New Media Reader (pp. 741-60). Cambridge, MA: The MIT Press.

[7] Ross Anderson, 2003 “Trusted Computing”: Frequently Asked Questions, at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[8] Synovate. 2003 “Federal Trade Commission—Identity Theft Survey Report”. P. 30-31. [http://www.ftc.gov/opa/2003/09/idtheft.htm].

[9] Anderson, J. W. 2000. “Producers and Middle East Internet technology: Getting beyond impacts”. The Middle East Journal, vol. 54, no. 3, pp. 419–34.

[10] Michael Froomkin, A. 2000 “The Death of Privacy, 52 STAN. L. REV.”, available at http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

[11] Bowers, C.A. 1998. “The paradox of technology: what’s gained and lost?” Thought & Action, vol., 14, no. 1, pp. 49-57.

[12] Robert Kahn, Keith Uncapher and Harry van Trees. 1978. “Communication Networks Guest editor”. Volume 66, No. 11.

[13] Baran, P. 1964 “On Distributed Communications Networks,” IEEE Trans. Comm. Systems.

[14] Global Network Initiative. http://www.globalnetworkinitiative.org.

[15] “Global Voices Online”: http://www.globalvoicesonline.org.

[16] http://www.p3ptoolbox.org/tools/papers/IEFP3POutreachforDMA.ppt.

[17] www.NJConsumerAffairs.gov.

[18] http://www.cato.org/pubs/briefs/bp-065es.html.

[19] http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/FERPA.html.

[20] http://www.irb.pitt.edu/sites/default/files/PPRA_4.1.2014.pdf.

[21] http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act.

[22] http://www.buzzle.com/articles/pros-and-cons-of-internet-regulation.html.

[23] http://www.buzzle.com/articles/pros-and-cons-of-internet-regulation.html.