Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.6, No.9, 2016

Information Privacy: Issues, Concerns and Strategies

Arinze, Uchechukwu Christian
Department of Computer Science, Faculty of Physical Sciences,
School of Postgraduate Studies, University of Nigeria, Nsukka

Ezema, M.E.
Department of Computer Science, Faculty of Physical Sciences,
School of Postgraduate Studies, University of Nigeria, Nsukka

Abstract
The twenty-first century globalized world is characterized by an explosive and exponential growth of data and information that is generated from diverse heterogeneous sources and stored in various formats about all kinds of human endeavour for use in decision making and policy formulation. With this phenomenal growth in information comes with it privacy concerns which have legal implications. This research seeks to comprehensively review critical issues in information privacy, defining key terms like Information, Privacy, Personally Identifiable Information and Expectation of Privacy, this paper will also examine types of personally identifiable information that come under privacy concerns, privacy on the internet, categories of technology to address privacy protection in commercial information technology systems such as: P3P, and XACML. Privacy-enhancing technologies, privacy and the internet, areas of privacy, data and privacy laws of Nigeria and other countries and industry-standard information security requirements and frameworks like the Sarbanes-Oxley law (SOX), privacy issues of social networking sites will all be looked into, so as to broaden our knowledge on information privacy issues.
Keywords: Information privacy, P3P, XACML, Sarbanes-Oxley law.

1.0 INTRODUCTION

According to (Hilbert, M. & López, P., 2011), in 2007 alone the global capacity to store digital information on computer hard disks, smart phones, compact disks and other storage media totaled ***295 Exabyte***, that is 295 times a billion Gigabyte or 1,000 Petabytes, and a Petabytes is 1,000 Terabytes, and a Terabyte is about what you'd get in a desktop PC hard drive these days - this simply signifies just how digital and data-intensive the world has become. The trend is shown in Figure 1.1 below.

Two converging trends, one competitive and the other technological, are driving businesses around the world. To be successful in the increasingly competitive information global economy, firms and governments around the world depends on vast quantities of information to build strong relationships with current clients and to attract new ones. And to collect this information, information and communication technologies, (ICTs) are deployed which continues to increase in capability and to decline in cost allowing information to be used in ways that were previously impossible or economically impractical.

Technology enables business concerns to record the details of any customer transaction at the point of sale, (POS) terminal to store vast quantities of transaction data in their databases and data warehouse, and to use these data to execute marketing programs with a business partner or alone. It also enables the development of extensive customer database, making it possible to deal with clients as individuals. Instantaneous access to the customers' history by a customer service representative allows standardized, impersonal encounters with whoever answers the telemarketer phone call to assume the appearance of a personal relationship (Gutek, 1995). This scenario implies that the marketing strategies of successful companies and organizations largely depend on effective use of vast amounts of detailed customer transaction data (Bessen, 1993), (Blattberg and Deighton, 1991) and (Glazer, 1991).

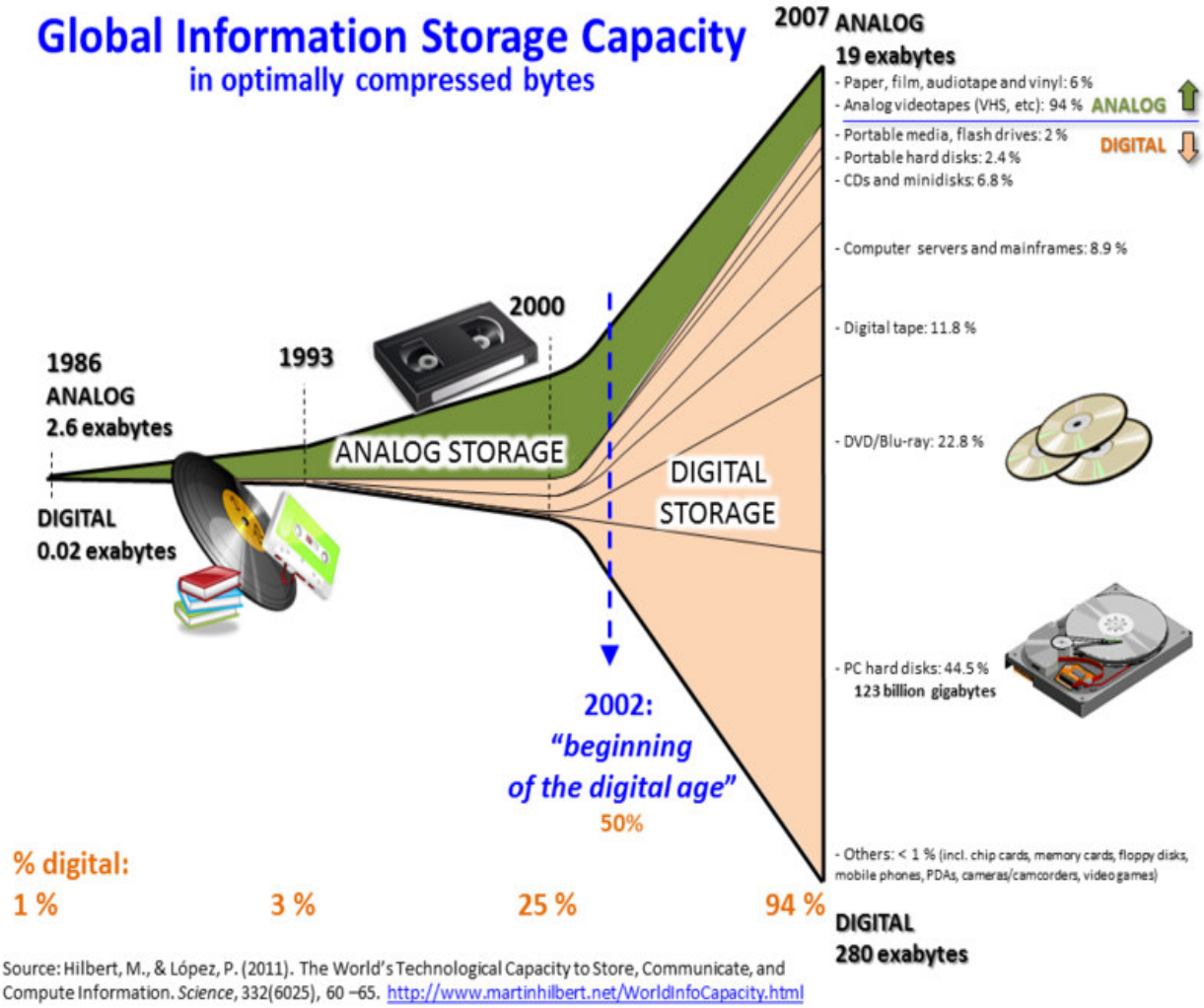

Figure 1.1: Growth of and Digitization of Global Information Storage Capacity

Table 1.1: Summary of Transaction Data Collected at Point-of-Sale (POS) Terminals by Transaction Processing Method

Transaction Processing Method	Representative Technology at Point-of-Sale	Transaction Data Gathered at Point-of-Sale
Manual (customer not identified)	Cash register without scanner	Date, retail location. amount of purchase
Manual (customer identified)	Cash register; credit card	Date, retail location. customer, amount of purchase
Point-of-Sale (customer not identified)	Cash register with scanner; inventory database	Date and time, retail location, items purchased. amount of purchase
Point-of-Sale(customer identified)	Cash register with scanner or mail order; credit card or customer account; inventory and customer databases	Date and time, retail location, items Purchased, amount of purchase. customer
Online (customer identified)	Computer-to-computer, credit card or customer account; inventory and customer databases	Date and time. Browsing patterns. items purchased. amount of purchase, customer

2.0 LITERATURE REVIEW

There is obvious tension or crisis that arises between the collection and use of personally identifiable information, (PII) that people provide in the course of most consumer transactions and privacy concerns. In today's electronic world, the competitive strategies of successful firms increasingly depend on vast amounts of customer data. But, formally the same information practices that provide value to organization also raises privacy concerns for individuals (Bloom et al, 1994).

Other pertinent questions information and privacy concerns raises include but not limited to: should the government compile dossiers on everyone in order to catch tax and welfare defaulters? Should the police be able to look up anything on anyone in order to stop organized crime? Do employers and insurance firms have rights? What happens when these rights conflict with individual rights? *Mary J. Culnan and Parnela K. Armstrong* both of School of Business, Georgetown University, Washington, D.C. U.S.A, in their seminal work entitled: *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An empirical Investigation*, hypothesized that clients will be willing to disclose personal information and have that information subsequently used to create profiles for marketing use when their concerns about privacy of their records are addressed by observing fair procedures, hence been ethical and circumspect in information management practices. Transaction data generated by customer contacts before, during and after the sale are a critical resource in the increasingly competitive global economy that is moving from a paradigm of mass production and mass merchandising to one of mass customization and personal service (Glazer, 1991 & Pine, 1993). Table 1.1 illustrates the data typically generated during a sales transaction. The richness of the data varies depending upon the technology employed, ranging from a cash register without scanning capability where essentially no customer data is recorded to an online service where all of the customer's "mouse tracks" are recorded (Miller, 1996).

Advances in telecommunications and database technology mean that all transaction data should be accessible on a timely basis to everyone in the firm with a need for the data. For example, data collected about product returns in Europe can be used by marketers in the U.S. or by a plant manager in Mexico to address potential problems in product design or changes in customer preferences as soon as enough products are returned, and the aggregated data about these returns makes the organization aware that a problem may exist. Transaction data signaling increased sales or the success of an advertising campaign for a target market segment or even an absence of sales data where sales were expected serve the same signaling function to the firm. Because these individual transactions are in reality, "messages" from customers to the firm that should be distributed as appropriate to functions across the value chain, information systems that process these transactions are in fact organizational information systems (Culnan, 1992). Organizations can gain competitive advantage by collecting and using transaction data effectively (Glazer, 1991).

The use of transaction data as an organizational resource can create positive or negative outcomes to a firm, based on how the information is used. In positive terms, the use of transaction data to yield better customer service, higher quality products, and new products that reflect consumer preferences creates benefits for both consumers and the firm. The collection of detailed information on consumer preferences enables firms to engage in relationship marketing and to target offers more accurately based on their customers' specific interests (Blattberg and Deighton, 1991, Glazer, 1991).There is also a potential downside to the collection and use of greater amounts of increasingly detailed personal information. Ironically, the same practices that provide value to organizations and their customers also raise privacy concerns (Bloom et al. 1994).

Privacy is the ability of the individual to control the terms under which personal information is acquired and used (Westin, 1967). Personal information is information identifiable to an individual. As Table 1.1 illustrates, today's customers leave more electronic footprints detailing their behavior and preferences; their buying habits are easily profiled, and can be readily shared with strangers. If the firm's practices raise privacy concerns resulting from a perception that personal information is used unfairly, this may lead to customers being unwilling to disclose additional personal information, customer defections, bad word of mouth, and difficulty attracting new customers, all of which can negatively impact the bottom line.

The growth of the Internet and other online systems also makes it possible for consumers to engage in "electronic retaliation" if they object to a company's practices, by "flaming" the company directly by electronic mail (Bies & Tripp, 1996), or by posting negative public comments to a computer discussion group. As the text of Internet discussion groups are archived and can be easily searched by keyword such as company or product name, these negative comments live on long after they were posted. The challenge to organizations, then, is to balance the competing forces of the power of information with privacy in their dealings with their customers. The failure to use personal information fairly or responsibly may raise two kinds of information privacy concerns resulting from the inability of an individual to control the use of personal information. First, an individual's privacy may be invaded if unauthorized access is gained to personal information as a result of a security breach or an absence of appropriate internal controls. Second, because computerized information may be readily duplicated and shared, there is the risk of secondary use; that is information provided for one purpose may be reused for unrelated purposes without the individual's knowledge or consent. Secondary uses includes

sharing personal information with others who were not a party to the original transaction, or the merging of transaction and demographic data to create a computerized profile of an individual by the organization that originally collected the information (Culnan, 1993, Godwin, 1991, Foxman & Kilcoyne, 1993, Smith et al. 1996). This paper addresses the latter concern, secondary use, where organizations make deliberate choices about reuse of their customers' personal information, and where the customer may perceive the reuse as varying from their expectations for fair use, done without their consent, and therefore unfair.

2.0 TYPES OF INFORMATION THAT HAS PRIVACY CONCERNS

Various types of personal information often come under privacy concerns viz:

INTERNET

The growth of the internet has made connectivity, communication and sharing of information pretty easier. But with it comes growing concerns of information privacy. The ability to control the information one reveals about oneself over the internet, and also who can access that information, is at the root of internet information privacy concerns. Internet information privacy concerns include but not limited to whether email can be stored or read by third parties without consent, or whether third parties can continue to track the web sites someone has visited: another concern is which websites that are visited collect, store and possibly share personally identifiable information about users, with the invention of search engines and the use of data mining techniques it has created a capability for data about individuals to be collected and combined from heterogeneous sources very easily. In order not to give away too much personal information e-mails should be encrypted and browsing of web pages as well as other online activities should be done without trace by using *anonymizers* or, in cases those not trusted by open-source distributed anonymizers, so-called mix-net, such as I2P-*The Onion Router or TOR*.

CABLE TELEVISION

The advent of satellite communication technology has further contributed to information dissemination sources and its attendant privacy issues. What is the ability to control the information one reveals about oneself over cable television, and who can access that information are the main issues, for instance, third parties can track internet protocol television (IP TV) programs someone has watched at any given time. The addition of any information in a broadcasting stream is not required for an audience rating survey, additional devices are not requested to be installed in the houses of viewers or listeners and without the necessity of their cooperation audience ratings can be automatically performed in real-time.

MEDICAL RECORDS

People may not wish for their personal health records and information to be revealed to third parties. This may be as a result of their concerns that it might affect their health insurance coverage or employment chances. Or it may be that they don't like others to know about medical or psychological conditions or treatment procedures which would be embarrassing, revealing medical data could also reveal other details about one's personal life. Privacy breach, Physicians and Psychiatrist in many countries and cultures have standards for doctor-patient relationships which include maintaining confidentiality. In some cases the Physician-Patient privilege is legally protected. These practices are put in place so as to protect the dignity of patients and to ensure that patients will feel free to reveal complete and accurate information required for them to receive the correct treatment. The U.S has laws governing privacy of private health information, such as the U.S health information portability and accountability Act, HIPAA and the HITECH Act, while U.K has the Data Protection Act.

FINANCIAL

Information about an individual's financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts and purchases can be sensitive. This is because if criminals gain access information, such as a person's accounts or credit card numbers, that person could become the victim or target of fraud or identity theft. Information about a person's purchases, can reveal a lot about that person history, such as places he/she has visited whom he or she contacted with, products he/she has used, his/her activities and habits, or medications he/she used. In some cases corporations might wish to use this information to target individuals with marketing customized towards those individual's personal preferences something which that person may or may not approve. Further, to protect the general public, corporations and public-quoted companies are expected by law to comply with certain information disclosure and regulatory frameworks like the Sarbanes-Oxley law (SOX) and other disclosure laws that will be discussed later under industry security requirements, so as to avoid defrauding the investors that will not suspect anything fishy with their financial statements so as to make informed business decisions.

POLITICAL

Political privacy has been a serious concern since voting systems emerged. The open-ballot system makes it possible for political views and stand-points of voters to be known. In order to guarantee voter privacy the secret-ballot system was introduced. This is the simplest and most widespread measure or strategy to ensure that political views of voters are not known to anyone except the voters themselves. It is nearly universal in modern democracy and considered to be a basic right of citizenship.

EDUCATIONAL

Information privacy as it relates to the educational field, seeks to find ways to optimize the rich dataset it provide by using it in carrying out analysis on the exploitation of minors. For instance in the united kingdom in 2012 the education secretary Michael Gove described the national pupil database as a "rich dataset" whose value could be "maximized" by making it openly accessible, including to private companies. While Kelly Fiveash of The Register said that this could mean "a child's school life including examination results, attendance, teacher assessments and even characteristics could be available, with third party organization being responsible for anonymizing any publications themselves, rather than the data being anonymized by the government before being handed over. An example of a data request that Gove indicated had been rejected in the past, but might be possible under an improved version of privacy regulations was for "analysis on sexual exploitation".

3.0 CATEGORIES OF TECHNOLOGIES TO ADDRESS PRIVACY PROTECTION IN COMMERCIAL INFORMATION TECHNOLOGY SYSTEMS

As heterogeneous information systems with different privacy policies and rules are interconnected and information is shared, policy applications will be required to reconcile, enforce and monitor an increasing amount of privacy policy rules (and laws). There are two categories of technology to address privacy protection in commercial Information Technology (IT) systems viz: Policy Communication and Policy Enforcement.

1. **POLICY COMMUNICATION:** This technology uses the platform for privacy preferences (P3P).

Platform for Privacy Preferences Project (P3P): The platform for privacy preferences is a protocol allowing websites to declare their intended use of information they collect about web browser users. Designed to give users more control of their personal information when browsing, P3P was developed by the World Wide Web Consortium (W3C) and officially recommended on April 16, 2002. Development ceased shortly thereafter and there have been very few implementations of P3P. Microsoft Internet Explorer is the only major browser to support P3P. The president of TRUSTe has stated that P3P has not been implemented widely due to the difficulty and lack of value.

2. **POLICY ENFORCEMENT**: This privacy technology has types viz: the extensible access control marking language (XACML) and the enterprise privacy authorization language (EPAL) and web-service privacy (WS-Privacy) respectively.

Extensible Access Control Markup Language (XACML): This technology together with its privacy profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems. It stands for *eXtensible Access Control Markup Language*. The standard defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies. As a published standard specification, one of the goals of XACML is to promote common terminology and interoperability between authorization implementations by multiple vendors. XACML is primarily an Attribute-Based Access Control system (ABAC), where attributes (bits of data) associated with a user or action or resource are inputs into the decision of whether a given user may access a given resource in a particular way. Role-Based Access Control (RBAC) can also be implemented in XACML as a specialization of ABAC. The XACML model supports and encourages the separation of the authorization decision from the point of use. When authorization decisions are baked into client applications (or based on local machine userids and Access Control Lists (ACLs)), it is very difficult to update the decision criteria when the governing policy changes. When the client is decoupled from the authorization decision, authorization policies can be updated on the fly and affect all clients immediately. Version 2.0 was ratified by OASIS standards organization on February 1, 2005.The first committee specification of XACML 3.0 was released August 10, 2010. The latest version, XACML 3.0, was standardized in January 2013. The first version of administrative policy profile working draft was publicly released on April 1, 2009.

Enterprise Privacy Authorization Language (EPAL): The enterprise privacy authorization language is very similar to XACML, but is not yet a standard. is a formal Language for writing enterprise privacy policies to govern data handling practices in IT systems according to fine-grained positive and negative authorization rights. It has been submitted by IBM to the World Wide Web Consortium (W3C) to be considered for recommendation.

Web service-(WS-PRIVACY): Web service privacy will be a specification for communicating privacy policy, it may specify how privacy policy information can be embedded in the simple object access protocol, (SOAP)

envelope of a web service message.

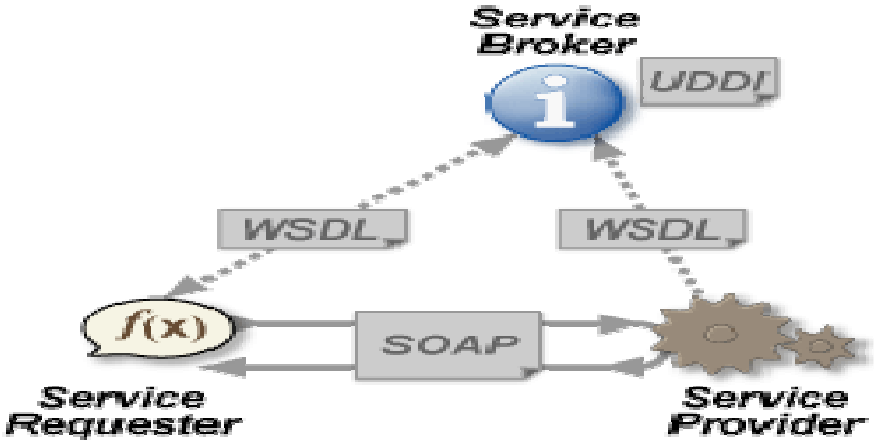

Figure 3.1: Web services architecture (Source: Wikipedia, 2015).

A web service as shown in figure.3.1 above is a method of communication between two electronic devices over the World Wide Web. A web service is a software function provided at a network address over the web or the cloud, it is a service that is "always on" as in the concept of Utility Computing. The W3C defines a "Web service" as: a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards and protocols. The W3C also states: We can identify two major classes of Web services *REST-compliant Web services*, in which the primary purpose of the service is to manipulate XML representations of Web Resources using a uniform set of "stateless" operations; and *arbitrary Web services,* in which the service may expose an arbitrary set of operations.

4.0 PRIVACY-ENHANCING TECHNOLOGIES

Privacy enhancing technologies (PET) is a general term for a set of computer tools, applications and mechanisms which - when integrated in online services or applications or when used in conjunction with such services or applications – allow online-users to protect the privacy of their personally identifiable information (PII) provided to and handled by such services or applications. Privacy enhancing technologies can also be defined as:

> *Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system* (Van Blarkom, Borking & Olk 2003).

5.0 Goals of PETs

PETs aim at allowing users to take one or more of the following actions related to their personal data sent to, and used by, online service providers, merchants or other users:

- increase **control** over their personal data sent to, and used by, online service providers and merchants (or other online users) (self-determination)
- **data minimization**: minimize the personal data collected and used by service providers and merchants
- choose the degree of **anonymity** (e.g. by using pseudonyms, anonymizers or anonymous data credentials)
- choose the degree of **unlinkability** (e.g. by using multiple virtual identities)
- achieve **informed consent** about giving their personal data to online service providers and merchants
- Provide the possibility to **negotiate the terms and conditions** of giving their personal data to online service providers and merchants (data handling/privacy policy negotiation). In Privacy Negotiations, consumers and service providers establish, maintain, and refine privacy policies as individualized agreements through the ongoing choice amongst service alternatives. In incentivized privacy negotiations, the transaction partners may additionally bundle the personal information collection and processing schemes with monetary or non-monetary rewards.
- provide the possibility to have these negotiated terms and conditions **technically enforced** by the infrastructures of online service providers and merchants (i.e. not just having to rely on promises, but being confident that it is technically impossible for service providers to violate the agreed upon data

handling conditions)

- provide the possibility to **remotely audit the enforcement** of these terms and conditions at the online service providers and merchants (assurance)
- **data tracking**: allow users to log, archive and look up past transfers of their personal data, including what data has been transferred, when, to whom and under what conditions
- facilitate the **use of their legal rights** of data inspection, correction and deletion

Existing PETs: Examples of existing privacy enhancing technologies are:

- **Communication anonymizers**: hiding the real online identity (email address, IP address, etc.) and replacing it with a non-traceable identity (disposable / one-time email address, random IP address of hosts participating in an anonymizing network, pseudonym, etc.). They can be applied to email, Web browsing, P2P networking, VoIP, Chat, instant messaging, etc.
- **Shared bogus online accounts**: One person creates an account for MSN, providing bogus data for Name, address, phone number, preferences, life situation etc. They then publish their user-ID and password on the Internet. Everybody can now use this account comfortably. Thereby the user is sure that there is no personal data about him in the account profile. (Moreover, he is freed from the hassle of having to register at the site himself.)
- **Access to personal data**: The service provider's infrastructure allows users to inspect, correct or delete all their data stored at the service provider.

Future PETs: Examples of privacy enhancing technologies that are being researched or developed are:

- **Wallets of multiple Virtual Identifiers**; ideally unlinkable. Such wallets allow the efficient and easy creation, management and usage of virtual identities.
- **Anonymous credentials**: asserted properties/attributes or rights of the holder of the credential that don't reveal the real identity of the holder and that only reveal so much information as the holder of the credential is willing to disclose. The assertion can be issued by the user herself, by the provider of the online service or by a third party (another service provider, a government agency, etc.). For example:
    - **Online car rental**. The car rental agency doesn't really need to know the true identity of the customer. It only needs to make sure that the customer is over 23 (as an example), that the customer has a driving licence, that the customer has health insurance for accidents (as an example), and that the customer is paying. Thus no real need to know her real name nor her address nor any other personal information. Anonymous credentials allow both parties to be comfortable: they allow the customer to only reveal so much data which the car rental agency needs for providing its service (data minimization), and they allow the car rental agency to verify their requirements and get their money. When ordering a car online, the user, instead of providing the classical name, address and credit card number, provides the following credentials, all issued to pseudonyms, i.e. not to the real name of the customer:
        - An assertion of minimal age, issued by the state, proving that the holder is older than 23 (i.e. the actual age is not provided)
        - A driving License, i.e. an assertion, issued by the motor vehicle control agency, that the holder is entitled to drive cars
        - A proof of insurance, issued by the health insurance
        - Digital cash

    With this data, the car rental agency is in possession of all the data it needs to rent the car, it can thus, as an example, provide the unlocking code to the customer with which she can unlock the closet where the car key is kept. Similar scenarios are buying wine at an Internet wine store or renting a movie at an online movie rental store.
- **Negotiation and enforcement of data handling conditions**. Before ordering a product or service online, the user and the online service provider or merchant negotiate the type of personal data that is to be transferred to the service provider. This includes the conditions that shall apply to the handling of the personal data, such as whether or not it may be sent to third parties (profile selling) and under what conditions (e.g. only while informing the user), or at what time in the future it shall be deleted (if at all). As an example, it can be negotiated that personal data mustn't be handed out to third parties or that the data is to be deleted after 3 months following the end of the contract. While this negotiation takes place, the online service provider communicates his requirements about the minimum amount of data he needs to provide the wanted service. Additional personal data may be asked for, too, but will be clearly labeled as optional. After the transfer of personal data took place, the agreed upon data handling conditions are technically enforced by the infrastructure of the service provider, which is capable of managing and processing and data handling obligations. Moreover, this enforcement can be remotely audited by the user, for example by verifying chains of certification based on Trusted Computing

modules or by verifying privacy seals/labels that were issued by third party auditing organizations (e.g. data protection agencies). Thus instead of the user having to rely on the mere promises of service providers not to abuse personal data, users will be more confident about the service provider adhering to the negotiated data handling conditions.

- **Data transaction log**. Users can log what personal data they sent to which service provider, when and under what conditions. These logs are stored and allow users to determine what data they have sent to whom, or they can establish the type of data that is in possession by a specific service provider. This leads to more transparency, which is a pre-requisite of being in control.

6.0 INDUSTRY-STANDARD INFORMATION SECURITY

Security requirements have been a matter of individual concern until recently unless you were handing government or military data, there were few legal requirements. This is rapidly changing. A variety of laws have been passed to enforce the privacy and accuracy of data and information.

- **SARBANES-OXLEY (SOX) ACT**: The Sarbanes-Oxley Act enacted July 30th, 2002 (often shortened to *SOX*) is legislation enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. The act is administered by the Securities and Exchange Commission (SEC), which sets deadlines for compliance and publishes rules on requirements. Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records; rather, it defines which records are to be stored and for how long. The legislation not only affects the financial side of corporations, it also affects the IT departments whose job it is to store a corporation's electronic records. The Sarbanes-Oxley Act states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." The consequences for non-compliance are fines, imprisonment, or both. IT departments are increasingly faced with the challenge of creating and maintaining a corporate records archive in a cost-effective fashion that satisfies the requirements put forth by the legislation..This law requires that public companies strengthen and document internal controls to prevent individual from committing fraudulent acts that may compromise an organizations financial statements or reporting. The chief executive officer and chief financial officer must attest to the adequacy of the internal control and accuracy of the financial report. These officers are subject to fines and imprisonment for fraudulent reports. The details of sox include requirements for providing the information that is used to generate the reports and internal control that are used to assure the integrity of the financial information.
- **HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY** (HIPAA) ACT: This law is intended to protect personally identifiable health information from release or misuse. Information from release or misuse. Information holders must protect provide audit trails of all who access this data in the U.S.A. The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. HIPAA is also known as the Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPAA-Public Law 104-191), effective August 21, 1996. The basic idea of HIPAA is that an individual who is a subject of individually identifiable health information should have:
    - Established procedures for the exercise of individual health information privacy rights.
    - The use and disclosure of individual health information should be authorized or required.

One difficulty with HIPAA is that there must be a mechanism to authenticate the patient who demands access to his/her data. As a result, medical facilities have begun to ask for Social Security Numbers from patients, thus arguably decreasing privacy by simplifying the act of correlating health records with other records. The issue of consent is problematic under HIPAA, because the medical providers simply make care contingent upon agreeing to the privacy standards in practice.

- **UK DATA PROTECTION ACT**: This act is intended to protect individual privacy by restricted access to individual identifiable data. It has eight (8) points one of which requires that data be kept secure and confidential. The 8 points are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
    - At least one of the conditions in Schedule 2 is met, and
    - In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. About the rights of individuals e.g.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- **FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA):** This law covers health and personal information held by schools.
- **CALIFORNIA BREACH LAW**: this law requires that an organization holding a variety of PII (for example credit card numbers driver's license, and government identity number) must provide safety and security measures to protect that information. If the information may have been compromised, the organization must notify all individuals involved. There are two laws, CA-SB-1386 and CA-AB-1950, which apply to organizations that hold PII. CA-SB-1386 is a California law regulating the privacy of personal information. The first of many U.S. and international security breach notification laws, it was introduced by California State Senator Peace on February 12, 2002, and became operative July 1, 2003. Essentially, it requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed).The bill mandates various mechanisms and procedures with respect to many aspects of this scenario, subject also to other defined provisions.
- **FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA):** This law is creating security guidance and standards through federal information processing standards (FIPS) documents that are managed by the national institute of standards (NIST). These standards are applied to organizations that are processing information for the U.S government.

7.0 DATA PROTECTION AND PRIVACY LAWS OF NIGERIA AND OTHER COUNTRIES COMPARED

A person's right to privacy is a fundamental human right that can neither be subsumed under law nor derogated from any nation's constitution; however legislation is still needed in most countries to provide a framework for its definition and regulation. In Nigeria, a citizen's right to privacy is spelt out in the Constitution of the Federal Republic of Nigeria (1999); Section 37 *'Right to Private and Family Life'* provides: *'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'* This statutory provision seeks to uphold respect for the Nigerian citizen's private affairs by protecting them from intrusion and unsolicited interference.

According to Privacy International (2007), there are four (4) aspects of privacy namely: *information privacy, bodily privacy, privacy of communications and territorial privacy*. To my mind, Nigeria's constitution provides adequate protection to its citizens on all four aspects, however several observers have been clamoring for a review of the country's privacy laws to address newer, more sophisticated threats to privacy, particularly in the area of information privacy. While we can all agree that privacy is the birthright of every individual, when it comes to defining what 'privacy' actually is? We all have widely different views depending on the context and environment we consider.

It is perhaps because of this ambiguity that many countries fuse the concept of privacy with one that's easier to define – data protection, giving birth to the understanding of privacy as management of personal information. As it stands now, Nigeria has no clearly spelt out legislative framework for data protection and it's a situation that has observers up in arms. To be fair to the government, there have been attempts to address this. In the past five years, two bills have been drafted and presented to the House of Assembly in an attempt to implement data protection.

In Nigeria, Part 10 of the draft Computer Security and Critical Information Infrastructure Protection Bill 2005 deals with identity theft while Part 11 deals with records retention and data protection. Section 4 provides amongst other things that "Any data retained, processed or Retrieved by the service provider at the request of any law enforcement agency under this Act or pursuant to any regulation under this section, shall not be utilized except for legitimate purposes. Under this Act, utilization of the data retained, processed or retrieved shall constitute legitimate purpose only with the consent of individuals to whom the data applies or if authorized by a court of competent jurisdiction or other lawful authority." This section raises a number of issues.

- The first being that part 11 is limited to personal data obtained from service providers only, as such it is restricted to communications service providers and not financial institutions or other industries
- Second, it is implying that in the event that an offence has been committed and needs to be

investigated, the data subject will be required to give consent before it can be used, this amounts to saying that a suspect must give consent to data being used against him/her!

- Another lawful authority is too wide a scope and should be restricted otherwise it leads to room for abuse. A brief comparison between Nigerian, European and US data protection legislations identifies a number of gaps in the Nigerian Bill. Notable of which are the following:
    - No definition of what constitutes personal data;
    - No identification of the right to privacy;
    - No definition of what constitutes data subjects rights;
    - No appointment of a regulatory body to redress breach (i.e. a Data Protection Commissioner);
    - No identification of the fact that organizations can also breach data protection rules;
    - No provision for circumstances where the personal data needs to be utilized without the consent of the data subject;
    - No provision, definition, or mandatory requirement of technical measures to mitigate data protection breaches. It is to be stated that in its current form the Bill does not adequately address Data Protection issues. For instance as we have seen in the United States and Europe, the legislations define what constitutes personal data, along with stating what the principles of data protection are. They also provide for adequate redress to persons that have had these principles breached. This is done through regulatory bodies that have appropriate power and are not afraid to use it. In the United Kingdom, the Data Protection Commissioner has the right to fine and also stop organizations from processing personal information where they do not comply with the provisions of the data protection Act. In the United States the regulatory bodies also have the power to fine organizations that breach data protection legislation. With these findings in mind, it is my recommendation that a stand-alone Data Protection legislation, which identifies the responsibilities of organizations, individuals and government in relation to obligations towards data protection, is written.

8.0 PRIVACY ISSUES OF SOCIAL NETWORKING SITES

The advent of Web 2.0 has caused social profiling and is a growing concern for Internet privacy. Web 2.0 is the system that facilitates participatory information sharing and collaboration on the Internet, in social networking media websites like Facebook and MySpace. These social networking sites have seen a boom in their popularity starting from the late 2000s. Through these websites many people are giving their personal information out on the internet. These social networks keep track of all interactions used on their sites and save them for later use. Issues include cyber stalking, location disclosure, social profiling, 3rd party personal information disclosure, and government information collection without the need for a search warrant.

9.0 CONCLUSION

In this paper I have been able to provide an overview of contemporary issues in information privacy focusing on defining key terms like Information, Privacy, Personally Identifiable Information and Expectation of Privacy, this paper will also examine types of personally identifiable information that come under privacy concerns, privacy on the internet, categories of technology to address privacy protection in commercial information technology systems such as: The Platform for Privacy Preferences (P3P), The Extensible Access Control Markup Language, (XACML), The Enterprise Privacy Authorization Language, (EPA) and Web-Service Privacy, (WS-Privacy) which all fall into two broader classifications of policy communication and policy enforcement respectively. Privacy-enhancing technologies, privacy and the internet, areas of privacy, data and privacy laws of Nigeria and other countries will be compared and industry-standard information security requirements and frameworks like the Sarbanes-Oxley law (SOX), HIPAA Act, U.K Data Protection Act, California Breach Law (CA-SB-1386), Federal Educational Rights and Privacy (FERPA)\ Act etc, privacy issues of social networking sites.

REFERENCES

Hilbert, M. & López, P. (2011): "The World's Technological Capacity to Store, Communicate, and Compute Information". *Science*, *332*(6025), 60–65.doi:10.1126/science.1200970, pp. 956-979. Available at:www.martinhilbert.net/WorldInfoCapacity.html (Accessed on June 2nd, 2014).

Samuel, D. W., and Louis, D. B. "The Right to Privacy," Harvard Law Review, 4 (5), (1890): 193-220, p. 195, citing Judge Cooley in *Cooley on Torts,* 2nd ed.

William L. Prosser**,** "Privacy," California Law Review, 48 (1960): 338- 423.

Mary, J. C., & Pamela, K. A. "Information Privacy Concerns, Procedural, Fairness, and Impersonal Trust: An Empirical Investigation, *Corporate America,* Chapel Hill, NC: University of North Carolina Press.

Bessen, J. (1993), "Riding the Marketing Information Wave," Harvard Business Review, 71, (September-October), 150-160.

James H. M. "How to Invade and Protect Privacy with Computers," in Carol C. Gould (ed.), *"*The Information Web: Ethical and Social Implications of Computer Networking*",* Boulder, CO: Westview Press (1989): 57-70.

Bloom, Paul N,, George R, Milne, and Robert Adler (1994), "Avoiding Misuse of Information Technologies: Legal and Societal Considerations,"

Li, Yuan (2011) "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," Communications of the Association for Information Systems*:* Vol. 28, Article 28.

Gutek, B. A, (1995), "The Dynamics of Service*",* San Francisco, A: Jossey-Bass, (2013, 03). Privacy Laws in Nigeria. StudyMode.com. Retrieved 03, 2013, from http://www.studymode.com/essays/Privacy-Laws-In-Nigeria-917251.html (2002, 07).

Sarbanes-Oxley Law. Retrieved 03-29-2013, from http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

Bies, R.J. (1993) "Privacy and Procedural Justice In Organizations," Social Justice Research, 6, 1, 69-86.

Philip, E.A., Marc, R. (1998) "Technology and Privacy: The New Landscape," MIT Press, Boston, Massachusetts, U.S