IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. IV (Mar – Apr. 2015), PP 24-31
www.iosrjournals.org

The Cyberspace and Intensification of Privacy Invasion

U. Mbanaso, PhD; and E.S. Dandaura, PhD.
Centre for Cyberspace Studies, Nasarawa State University, Keffi

Abstract: *The widespread adoption of cyberspace for exceptional socio-economic activities, especially as it is connecting populations around the globe in ways never foreseen is raising fresh security issues. What is fuelling this embracement, is the pervasiveness of social media and innovative mobile computing devices. This has not only changed our ways of life, but also blurs the lines that define the way governments run, business are conducted as well as the way we use and share information. Yet, these new ways of services and interactions, are raising new threats in terms of privacy, integrity, confidentiality and trust. Cyberspace transactionscut across national boundaries, in many cases, without any form of existing trust relationships of any sort. Again, the explosion in mobile computing is extending the influence of social web; the manner in which content is shared and accessed is now defining a symbol of new global status, affecting and merging the realm of personal and business life. Besides the threats from criminal minded people or group, deliberate efforts by states to dominate (or show supremacy) with the potential to halt other states economically, politically or militarily, lies intensified privacy invasion that is unfamiliarto the unsuspecting technology user. This paper explores the different levels at which users of cyberspace are exposed toprivacy invasion, the consequences and manner in which some of the risks can be mitigated even as we continue to record steady upswing of mobile computing by cyberspace users.*

I. Introduction

Cyberspace and its infrastructure have continued to enable exceptional socio-economic opportunities, connecting populations worldwide in ways never foreseen (ITU, 2009). It is now commonly known that modern businesses and governments are unable to function without increasingly relying upon this new domain. That is, the machinery of governments, critical national infrastructure (CNI) – including theindispensable delivery of telecommunications, electricity, airport navigational systems, and banking as well as straightforward life of individuals are heavily dependent on proper function of cyberspace infrastructure (The UK Cyber Security Strategy, 2011). The implication is that it has created a paradigm shift i.e. the worth of tangible resources and intangible assets are therefore blurring.

Behind these overwhelming gains also lie uncertainties and perils. The Cyberspace and resources that we now trust can be compromised or impaired by criminal minded people in an unimagined fashion. There is also growing concern of deliberate efforts by states to dominate (or show supremacy) with the potential to halt other states economically, politically or militarily. Besides these known threats, is the intensified privacy invasion that is uncommon to the unsuspecting technology user.

The wave of development resulting from the convergence of information technology and communications (ICT), the rapid evolution of Mobility and Social Networksis unarguably altering the cyberspace landscape. Conversely, advances in coretechnologies that are fuelling reduction in production cost, suggest that accessing the cyberspace will become increasingly inexpensive and stress-free worldwide. The aftermath is that more and more people around the globe ultimately rely on cyberspace systems for daily life. Equally, the rapid upturn and sophistication of mobile technologies has resulted in swift change in the manner cyberspace resources are presented and interacted with.

Yet, fresh security issues such as privacy, integrity, confidentiality and trust (Bertino, Ferrari, &Squicciarini, 2004) raise concerns as borderless cyberspace span across nationalfrontiers, without any form of existingtrust relationships of any sort.Interactions in cyberspace raise an interesting paradox. On the one hand, applications (apps) require identity/attribute related information of users in order to offer users services. On the other hand, users supposedly should not disclose their information or attributes to a remote applicationwithout determining in advance whether the app's provider (AP) can be trusted to comply with their privacy preferences. In spite of this, this attribute demandis typically unilateral and provider-centric, in the sense the AP assigns the access rights, makes the access control decisions, and determines the privacy policy. However, in closed systems, where a sort of pre-relationship exists among interaction parties, privacy threats are of less concern than in cyberspacerealm comprising several parties who may not share any pre-existing knowledge or trust relationships. Consequently, it implies that the growing privacy invasion can undermine the security and safety of an individual. It raises a number of social, cultural, legal and technical issues, which, arguably, make protecting individual privacy across cyberspace environment more challenging. Therefore,the use of personal identifiable information (PII) that is likely to be traceable to an interaction entity raises privacy questions. An individual is associated with a diverse set of attributes and/or properties, which are often open to misuse and abuse. That is, the individuality is associated with a range of information that raise privacy concerns including driver's license, street address, postal address, national identity, marriage certificates, email addresses, telephone numbers, membership certificates, vehicle plate numbers, job functions, affiliations, photographs, social network handles etc. Additionally, individual activities can generate information that can be traceable e.g. when an individual purchases an item online, and is given a proof of purchase, e.g. a receipt, this can later be linked to that individual and may be used in a manner that is undesirable. In cyberspace, especially with proliferation of mobile apps and social webs, privacy invasion is on the increase and existing protection mechanisms are just inadequate.

II. Conceptualising Privacy

Privacy is viewed from divergent perspectives and as a socio-economic problem has impact on individuals, communities, governments and businesses. It is burdened by legal, sociological, behavioural, psychological, economic, political and cultural factors, which are subject to numerous expectations and interpretations as pointed out by Acquisti&Grossklags (2005). Certain compelling forces including economic benefits, enterprise business interests, national security, regulation and compliance, legislation and advances in technology affect these expectations. These raise the question of how realistically we can expect privacy protections, given the borderless nature of cyber environment. These forces when viewed from a socio-economic perspective explain why finding widely acceptable privacy measures isunlikely untenable. The fact that privacy is often perceived from dissimilar cultural backgrounds, resulting in an array of unfulfilled expectations and trust levels, further complicates the privacy problem space.

What is Privacy? There is hardly any agreed definition of privacy. In (OCED, 2014) privacy is defined as "the status accorded to data which has been agreed upon between the person or organisation furnishing the data and the organisation receiving it and which describes the degree of protection which will be provided". In Wikipedia, Privacy is defined as "the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively". According to (APF, 2012) privacy is defined as "data that enables a person to be identified either directly, or after integration or linkage with other data" .Yet, Clark (2006) defines privacy "as the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations". Going by these definitions, what is obvious is that privacy as an abstract concept is bound by space, and its characteristics span across multiple space as illustrated in figure 1.

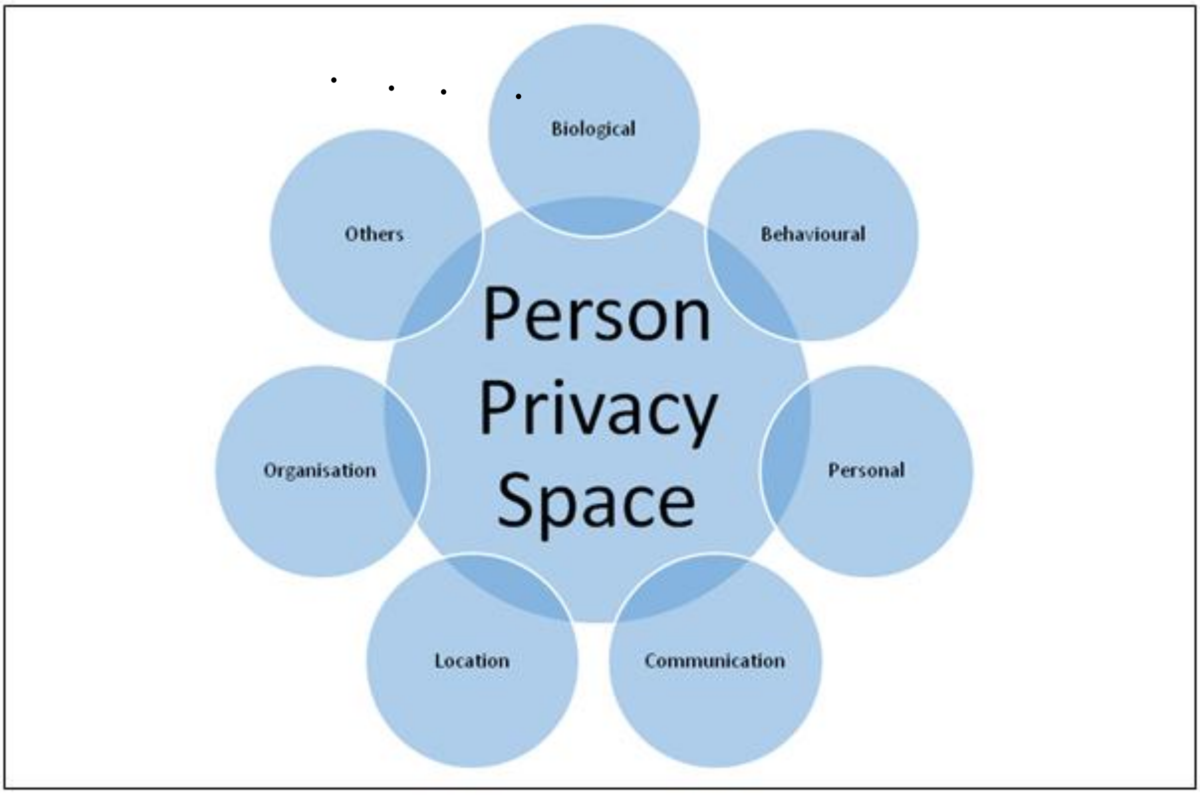


Figure 1: Person's Privacy Space

From the above, person identifies seven spaces that define the intricate nature of privacy. First is the Biological or Bodilywhich may refer to biological features of an individual such as biometric extractions, sterilisation, blood transfusion, which when used without owner'sconsent, constitutes privacy violation.Behavioural relates to sensitive personal characteristics such as sexual preferences and habits, political and social actions and religious practices, etc.that undesirable usage constitutes privacy violation and may harm the individual.

Similarly, Communicationin the diagram refers to traceable activities of an entity while using various digital media to interact or communicate, which disagreeablyresults in privacy intrusion that may compromise the individual security and safety. Personaloften related to the notion of 'data privacy' and 'information privacy', attributes or properties which are associated with identifying the individual or an entity directly, which undesirable use may endanger the individual security and safety.Location, on the other hand simply refers to information that can be leveraged to guess or track the position of an entity in real-time, or retrospectively; such that undesirable use constitutes privacy breach that can endanger individual security and safety.

Also, While, Organisation refers to those information associated with person's affiliation with an organisation that undesirable use is such that can undermine individual security and safety, Others represents elements of person privacy space not covered in this context.

The notion of privacy denotes personal identifiable information within person's privacy space that undesirable use has the potential to harm the data subject. It refers to any piece of information associated with appearance, personality, knowledge and characteristics that describe an individual (or an entity) as described by Mbanaso (2007). To this end, the following is provided for clarity:

i. Personal Identifying Information is information that may be used to establish the identity of an individual (or an entity).
ii. Personal Identifiable Information is information that may be associated with an identifiable individual (or an entity).
iii. Personal sensitive Information is information that may be used in a manner that causes harm to an individual with whom it is associated.

However, privacy and its risks are compounded by the poor perception and understanding of a technology user, plus the fact that in cyberspace, human value of privacy will continually be debased (Clark, 2006). This brings the user's inability to participate in privacy self-governance (Mbanaso, 2009)that is, in actual sense, the user does not really participate (or control) on how information of privacy nature is used. In many cases, users are not fully aware of the information held about them, where the information is stored, or the risks of undesirable usage. Debatably,a considerable number of individuals may be willing to exchange privacy for convenience or agree to release PII in return for small benefits or rewards as argued by Acquisti&Grossklags, (2005). For example, most of the free mobile apps in Google store, Apple store, or Windows store require unrestrained access to a number of privacy-invasive technologies (PITs) such as camera, contact address, GPS, SIM card information, and app users, naively clicks "I Agree" button without consideration of the consequences of their action. The incentive is simply that notion of 'free stuff'. Notably, Mbanaso (2007) argues the fact that users are not even sufficiently informed to make proportionate decisions or risks assessment concerning giving out their PII. Three main challenges attend an individual's privacy decision-making process. Firstly, poor perception caused by external factors: Third party collection and sharing of information without the individual's consent or even when the individual is not part of the transaction or interaction.

Secondly, Information that is applicable to the privacy decision process may be available to only a subset of the parties involved in making the decision. This can be called Information asymmetries. Thirdly, there is the issue of individual innate bounded rationality. This refers to the individual's inability to sensibly process a large amount of information in depth prior to making a decision.

Acquisti&Grossklags, (2005) also argue that "subjective perceptions of threats and potential damage, psychological needs, and actual personal economic returns" affect individuals' privacy decision making process. Nevertheless, the individual is faced with privacy realities and expectations, and any attempt to view privacy from an extreme standpoint could mean secrecy, anonymity and solitude (Mbanaso, 2009). The implication is that any move to attain absolute privacy could then result in total anonymity such as the absence of traceability, 'linkability' and 'observerability' of the privacy subject, which may potentially undermine national security in another dimension. Of course, these would result in the inability to conduct business where PII is needed in order to process and complete business transactions or interactions.

Privacy has also raised a number of fundamental questions regarding so called personal data. For instance, which information can be classified as personal? Who should be the custodian of it? Who should control access to it and under what conditions? What is the context under which personal data should be accessed, i.e. for what purposes and what should happen afterwards? Other issues of concern include whether the techniques used during collection, processing and use are by any means legal as proposed by OECD, (2014).

Furthermore, other considerations comprise whether the data owner is fully aware about the data and the processing- consent, notice and awareness, the quality of data, i.e. is the data accurate and a true representation of the data subjects' attributes or properties as specified in (OECD, 2014).

Though some researchers and various privacy standards and principles (APF, 2011), (APF, 2012), (OECD, 2014) have been attempting to address these questions, development of efficient technical solutions that address the privacy concerns, remains a challenge that has continued to attract research inputs (APF, 2010). Another critical privacy factor is the inherent conflict between privacy protecting PII on the one hand, and the legitimate free flow of information on the other (OECD, 2014). This buttresses the point that absolute privacy will pose undue interference with the legitimate free flow of information as stated by OECD, (2014). Bearing these factors in mind, it can be argued that privacy protection can be viewed from two angles: the need to decouple identifying information from real world identities whenever practicable, and where it is impractical, the appropriate enforcement of privacy measures based on the individual's security preferences as argued by Mbanaso, (2009).

In the sections that follow, we discuss the multifaceted consequences of privacy invasion and thereafter examine privacy invasion from two perspectives i.e. Mobile devices and Social web covering the combine effect of both in digital space.

Some of the Consequences of Privacy Invasion

The consequences of privacy invasion are multifaceted. TheFreecom Dictionary(2015) rightly identifies privacy as "a basic human need, and invasion of privacy can have serious psychological and emotional consequences, including paranoia, anxiety, depression and broken trust". Privacy violation has both a legal and an ethical dimension. From the legal perspective, the invasion of an individual's privacy is considered a crime within the confines of the laws of most countries. It attracts as much as three years imprisonment or more in both the United Kingdom and the United States of America. In some countries it attracts an option of fine upon conviction. Even in Nigeria, an individual can secure a court order restraining another person from invading his or her privacy. The courts can also award damages for the invasion of his/her privacy for no just cause. Actions that could be regarded as violation of an individual's privacy in this context include sharing information with a third party or on the media on any matter that is essentially about an individual's personal life, health status, or any matter that could cause the person grievous psychological or physical harm, or result in a strain on the professional life of the plaintiff. Privacy invasion, in this context include the illegal appropriation, by false pretext of the plaintiff's identity to the advantage of the defendant. It also so includes portraying the plaintiff in a false light or at through undue disclosure of private facts about him or her. Since legally, individuals are granted the right to reasonable seclusion or solitude, any violation of such in whatever way by a third party is likely to be considered an offense before the law. An invasion of privacy can be even more upsetting when it is for pecuniary gains of the intruder. Consequently, in some countries, the courts can order payment of damages or even disgorgement, which in simple terms means the giving up of profits to prevent such unjust enrichments.

Psychology Today provides the ethical and psychological dimensions to invasion of privacy thus:

Adolescence is the phase in which people begin to develop a strong sense of privacy, and psychologists believe that allowing adolescents to create safe spaces of privacy where others are not allowed to enter without permission is crucial to helping them develop healthy boundaries later in life. Any invasion of privacy results in a violation of personal boundaries and a loss of trust, not only in the invader but often with the victim's own ability to set up and maintain boundaries to protect their privacy. A person whose privacy has been invaded may feel unsafe and out of control in their own life (Psychology Today, 2015).

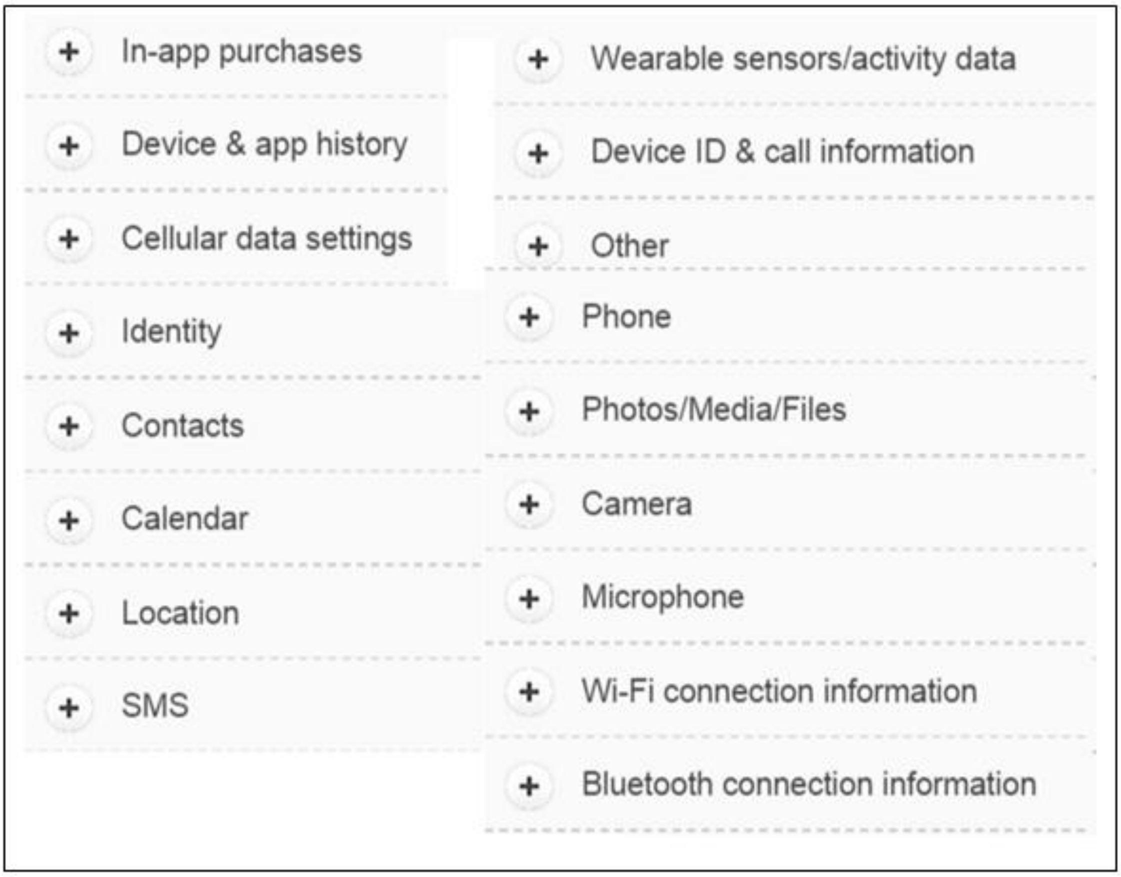
From the perspective of the cyberspace, invasion of privacy encompasses workplace monitoring, Internet surveillance, data collection, and other means of disseminating informationof private nature. Privacy violations in this case also manifest in the form of hacking, phishing, gossiping, data mining, harassment, and general abuse of personal data by third parties. Perhaps the exception to absolute protection from privacy invasion, in some countries, is the case of celebrities because by opting to voluntarily place themselves within the public eye, their activities are considered newsworthy so long as it is factual. However, in most American States, for instance, an otherwise non-celebrity has a right to privacy from: i) intrusion into his/her private affairs; ii) public disclosure of any embarrassing privacy information; iii) unsolicited publicity which puts him/her in a false light to the public; iv) identity theft or appropriation of a private individual's name or picture for personal or commercial gain of a third party.

Mobile Devices and Privacy Invasion

The emergent of smart-devices, or mobility with advanced capability and computing power has radically altered the way people access cyberspace resources. This surge in mobility as well as its popularity plus inherent relatively, relaxed security in mobile devices' operating systems, have created significant number of vulnerabilities and risks. Besides that it is very attractive targets for criminal minded entities, it has created a 'window' of opportunity for the escalation of privacy intrusion. Although mobile devices share many of the vulnerabilities inherent in traditional computer systems, the properties that make mobile device easy to carry, use, and modify, exposesit to an assortment of privacy exploitations.

Mobile devices give users easy access to email, chat, the internet, GPS navigation, and many other stunning applications. It is therefore, that the proliferation of mobile apps presented a powerful platform for privacy vulnerabilities that are unduly exploited. These kind of exploitations is highly unlikely to be averted by traditional security measures and apps users have little or no options at all. Technical security measures, such as firewalls, antivirus, and encryption, even when available in mobile devices are unlikely to prevent privacy violations.

When a user visits an app store such as Google store, and chose an app to install, on clicking install, the app requests the user to give permission to enable it "access specific capabilities or information" on the user's device. Google groups a set of permissions on certain attributes of the mobile device as depicted in figure II. These attributes of a mobile system can be classed asPITs, and the user is not well-informed on how and what purpose thosePITs willbe used and to what extent. The pretext is that the apprequires those capabilities to offer a user, basic functionality and better user experience.Moreover, if the user declines to give the permission, the app will not be installed. The consequences is that the user has no option or bargaining power to negotiate or enforcehow those capabilities can be used subsequently.



+ In-app purchases
+ Device & app history
+ Cellular data settings
+ Identity
+ Contacts
+ Calendar
+ Location
+ SMS
+ Wearable sensors/activity data
+ Device ID & call information
+ Other
+ Phone
+ Photos/Media/Files
+ Camera
+ Microphone
+ Wi-Fi connection information
+ Bluetooth connection information

Figure II: Google Permission Group

Regrettably, emerging technologies are increasingly introducing privacy-hostile environment that unsuspecting user may hardly recognize the immediate privacy inadequacies, and the serious invasiveness.The app is unrestrained to gain access to PITs whenever it desires without further consent from the device owner. Incidentally, users use their devices for a number of activities including storing of sensitive data, such as email, calendars, contact information, passwords, personal notes, credit card details, location information etc. The repercussion is that the app after gaining the permission has unhindered access to personal information of sensitive nature.The lack of proportionate privacy controls on mobile devices capable of helping the user make on-the-spot informed privacy decision,is seeminglya gross privacy vulnerability and abuse.

Social Networks and Privacy issues

The rise of social web has revolutionised how people connect, interact, and collaborate.Undeniably, the usefulness of social networks such as Facebook, Twitter, Pinterest, LinkedIn, etc. is incredible.In a survey conducted by (Pew Research Centre, 2015), five major social network sites usage as of September, 2014 stand at 71% of adults use Facebook, 23% of adults use Twitter, 26% use Instagram, 28% use Pinterest, 28% use LinkedIn. The widespread use of mobile devices, particularly, smartphones, has further popularised the social web in an unbelievable manner. Over 40% of mobile device owners use a social networking site on their smart devices, with typical 28% on daily basis (Pew Research Centre, 2015).

The upsurge is driven by the combined effect of the social web and the convenience brought by mobility. However, there are divergent reasons people use social webs, includingto network with new friends, reconnect with old friends, keep relationships, build or promote a business or project, share in discussions about interesting topics, keep the public informed and other issues, etc.Aside these socio-economic gains lies huge security issues that can put the individual or an organisation in a weakening position or at grave risk. Unknown to the user, the increasingly use of these media is also growingprivacy invasion exponentially; information shared on the cyberspace has potential risks though the user is immediately unaware of the perils of divulging such personal sensitive information.

On a more serious downside of social webbing, is the fact that users may divulge information about other people without even understanding or considering the consequences. Posting comments or photos that undesirable usage, may compromise person’s privacy is potentially risky. In some cases, users post negative content about other people intentional or unintentional without apprehending the inherent negative consequences. In addition, social web has become a channel for carrying out cyber bullying, which in many cases leads to psychological pains.Questionably, there is a gamut of activities in the social media that promotes grave privacy intrusions in astonishing scale.

How privacy invasion put the individual at risk

The amount of sensitive information of personal nature collected, held and shared, misused or abused on the platforms of social mediaand mobile apps is unbelievably alarming. A quick assessment of privacy settings of many of these sites reveals the enormous grabbing of PII that cut across what Clark (2006) described as person’s privacy space. In particular, Facebook collects:

Things you do and information you provide, Things others do and information they provide, Your networks and connections, Information about payments, Device information, Information from websites and apps that use their Services, Information from third-party partners, etc. Facebook, puts out how the information is used for: Provide, improve and develop Services, Communicate with you, Show and measure ads and services, and Promote safety and securityFacebook (2015).

The implication is that once the user clicks “I agree” (acceptance of the privacy settings), the user has perpetually granted the provider i.e. Facebook,the permission to use the personal data for the stated purposes withoutfurther recourse to the user, regardless of if, the user’s privacy preferences change over time. Again, there is no opt-out option mechanism as stated by (OCED, 2014) in many of the privacy settings - the user must accept all of it or the service is denied as argued by Mbanaso (2009). Debatably, the provision of these privacy settings is merely a legal compliance that has no technical means to protect personal sensitive data from misuse or abuse. Figure II depicts the gamut of capabilities that can be exploited by a mobile app, meaning that a malicious actor can hide under this provision to inflict harm.

III. What are at the Risks Involved?

i. Computing Device can be compromised: There is high likelihood that the user’s device can be compromised with little effort by malicious actors. It is practically easy to leverage social engineering, exploitation of social networking, mobile botnets, exploitation of mobile applications, and exploitation of m-commerce to compromise devices for immediate or later abuse.

ii. Personal Security and Safety: user’s personal sensitive information available on the social web or covertly obtained at real-time by mobile apps, may potentially endanger security and safety of the user. User’s address posted in profile, increases the chances that user’s house may be burgled. Family photos can risk the safety of children- a cyber-criminal can apply social engineering techniquesto lure a child into a dangerous situation. User’s current location tracked by GPS or cellular phone network tools has the potential to guess real-time activities of the user, which is inherently unsafe.

iii. Personal relationships: a user face the danger that someone else may post uncomplimentary or negative comments impulsively. Even when the poster realizes the mistake, it is unlikelythat retracting the content can undo the damage.In cyberspace, once information is divulged, there is high probability that the owner instantly loses control of who sees it, where it is propagated, or stored.

iv. Corporate data or Intellectual Property (IP): In some cases, users disclose corporate confidential information or IP on a social networking services unintentionally, and this action can result to serious negative consequences. In other cases, such information can equally be accessed by malicious people who have previously compromised user's system to further their nefarious activities.

v. Professional reputation: Incorrect comments, content or photos potentially can jeopardise person's reputation. These days, potential employers or adversaries can search for and obtain vital information about potential candidates and can be used undesirably. These include information that purports that one is unreliable, untrustworthy, or unprofessional, could hamper someone's career.

Actors

Criminalactors make greater use of social weband mobile apps, to spread malicious codes, compromisecomputing devices, or access personal information about a user's identity, location, contact information and other personal attributes or properties. It is possible for attackers to gather sufficient personal information that they can leverage to assume someone's identity or the identity of someone else in a contact. Personal details in many cases provide clues that attackers may use to guess answers to security or password reminder questions for email, credit card, or bank accounts. In the context of our discussion, there are many actors that fall under malicious actors i.e. anyone who seeks to obtain personal data without owner's consent with the intention to inflict a harm on the owner or other people can be classed as predators of privacy, including those who hack for financial rewards, competitive advantages or for political and national security.

Mbanaso (2009) contends that several attempts have been made to address privacy concerns especially when computer databases became widely used. In recent times, many of the privacy initiatives focus on web privacy activities, that is, purely on how websites collect, share PII and what they promise to do with PII. So far, privacy settings of these platforms in no way assures the privacy of personal data as there are no mechanism for real-time privacy self-governance- the app user has no mechanism to enforce its privacy preferences. To proportionately protect privacys, users and app providers require to determine in advance the assurance that the other party can act in a manner that is compatible with their own security preferences (Mbanaso, 2007).

The underlying assumptions that have led to the development of solutions that are typically unilateral and asymmetric, cannot provide users with proportionate privacy protections. In contrast, emerging threatspropel the need for a bilateral paradigm, simply because both the apps, and user entities may have privacy and confidentiality concerns of equal value. This has resulted in a new research area otherwise known as trust access management systems which employ trust negotiation concepts whereby communicating parties can reciprocally releasetheir security policies and credentials(Bertino, Ferrari, and Squicciarini, 2004) to negotiate and mutually agree on security or privacy preferences.

Furthermore, growing business requirements may demand the dynamic exchange of service requirements, contractual and service level agreements in order to assess the mutual benefits and associated risks before engaging in high-risk based interactions or transactions (Mbanaso, 2009). Enabling the runtime exchange of these security requirements requires a bilateral and symmetric infrastructure that will allow communicating peers to indicate their willingness to accept constraints imposed by the other party, before the latter is prepared to reveal their sensitive information. There is some overlap between users' privacy requirements and business requirements, meaning that privacy, confidentiality and trust are typically associated, as such, should be treated mutually.

Addressing confidentiality and privacy problems mutually and simultaneously, requires that interacting parties in cyberspace should have a uniform way of declaring their security requirements alongside the constraints they may impose on the use of their information before sharing it. This provision will ensure that parties evaluate the risks associated with giving out their information and determine the degree to which they are prepared to trust other participating parties. This entails the requirement for communicating parties to identify constraints and obligations they may wish to place on the others concerning the use of their resources or attributes.

IV. Conclusion

Undisputedly, privacy as an abstract concept is a growing global concern that has continually attracted the attention of researchers. Thepersonal sensitive information, such as privileges, capabilities, propertiesor attributes i.e. all within person's privacy spaceas used in the cyberspace raise an interesting paradox. On one hand, in order to make the services and resources accessible to users, typical apps require valid and provable user's device capabilities, identities or attributes in order to provide the services. On the other hand, auser may not be prepared to disclose hissensitive information or attributes to a remote party without determining in advance whether the service can be trusted with such information. This is based on the fact that when a user gives out personal information, the user is unsure of the extent of propagation and use of such information once in the custodian of the collector. This paper hasexposedhow emerging technologies covertly invade privacy of users, and the inadequacies of current privacy settings that cannot grantee user's security and safety. As a result, a unified approach that can significantly provide mutual privacy, confidentiality and trust in Cyberspace environment is highly desirable and requires further research inputs.

References

[1]. Rodge Clark (2006), what is Privacy [online], Available from: http://www.rogerclarke.com/DV/Privacy.html [Accessed: 15th December, 2014]

[2]. OCED, (2014), Privacy Principles [online], Available from:http://oecdprivacy.org/ [Accessed: 15th December, 2014].

[3]. Rodge Clark (2001), Biometrics and Privacy, Available from:http://www.rogerclarke.com/DV/Biometrics.html [Accessed: 12th, December, 2014]

[4]. A. Acquisti and J. Grossklags, (2005) Privacy and Rationality in Individual Decision Making," IEEE Security and Privacy, vol. 3, pp. 26-33.

[5]. EU, (2002) Directive 2002/58/EC on Privacy and Electronic Communications, European Parliament and the Council

[6]. E. Bertino, E.Ferrari, and A. Squicciarini, (2004), Trust Negotiations: Concepts, Systems and Languages, IEEE Computer, pp. 27-34,

[7]. U. M. Mbanaso, G. S. Cooper, D. Chadwick, and A. Anderson, (2007) Obligations for Privacy and Confidentiality in Distributed Transactions, presented at Emerging Directions in Embedded and Ubiquitous Computing, Dec 2007, pp 69-81

[8]. U. M. Mbanaso, G. S. Cooper, D. Chadwick, and A. Anderson, (2009) Obligations for Privacy and Confidentiality in Distributed Transactions, INTERNET RESEARCH journal, Emerald. Special Issue: Intelligent Ubiquitous Computing: Applications and Security Issues, vol. 19

[9]. Australian Privacy Foundation (APF) (2012), The Collection of Third Party Data Through Networks such as Wifi, Available From:https://www.privacy.org.au/Papers/PosData.html, {Accessed: 15th January, 2015]

[10]. Facebook, (2011) Factsheet, Available from: http://www.facebook.com/press/info.php?factsheet) [Accessed: December 3, 2014]

[11]. Twitter, (2011) About Twitter, Available from: http://twitter.com/about [Accessed: December 3, 2014)

[12]. MySpace (2011)Fact Sheet , Available from: http://www.myspace.com/pressroom/fact-sheet/ [Accessed: December 3, 2014]

[13]. LinkedIn, (2011)About Us Available from :http://press.linkedin.com/about [Accessed December 3, 2014]

[14]. Pew Research Centre (2015) Available from : http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/, [Accessed: January 15, 2015]

[15]. Facebook, (2015) Available from: https://www.facebook.com/policy.php, [Accessed: January 17, 2015]

[16]. The UK Cyber Security Strategy (2011)Cabinet Office, Whitehall, London SW1A 2WH

[17]. Psychology today, http://www.psychologytoday.com/blog/mediaspotlight/201308/negotiating-the-privacy-mazeaccessed 2nd January 2015

[18]. Free Dictionary http://www.freecomdictionary.com accessed, March 3, 2015

[19]. Wikipediahttp://en.wikipedia.org/wiki/Privacy accessed 2nd January 2015

[20]. ITU (2009) Understanding Cybercrime: A Guide For Developing Countries, 1211 Geneva 20 Switzerland

[21]. Australian Privacy Foundation (APF), 2012, Protection of Privacy and Personal Data in Relation to Free Trade Agreements, Available From: https://www.privacy.org.au/Papers/DFAT-TTP-120907.pdf, [Accessed: 17th January, 2015]