Internet of Everything (Ioe): Analysing the Individual Concerns Over Privacy Enhancing Technologies (Pets)

Asim Majeed
School of Computing, Telecommunications and Networks
Birmingham City University (BCU)

Imani Kyaruzi
Department of Business Administration
QA Higher Education (ULST)

Rehan Bhana
School of Computing, Telecommunications and Networks
Birmingham City University (BCU)

Shaheed Pervaz
School of Computing, Telecommunications and Networks
Birmingham City University (BCU)

Anwar Ul Haq
Department of Computer Science
QA Higher Education (ULST)

Mike-Lloyd Williams
Department of Business Administration
QA Higher Education (ULST)

***Abstract*—This paper aims to investigate the effectiveness of the provision of privacy of individuals through privacy enhancing technologies (PETs). The successful evolution and emergence of cyberspace with the real world through "Internet of Everything (IoE)" has led to the speedy progress in research and development of predictive analysis of big data. The individual's privacy has gained a considerable momentum in both industry and academia since privacy-enhancing technologies (PETs) constitute a technical means to protect information. Privacy regulations and state of law deemed this as an integral part in order to protect the individual's private sphere when the infrastructure of Information Communication Technologies (ICT) is laid out. Modern organisations use consent forms to gather individual's sensitive personal information for a specific purpose. The law prohibits using the person's information for purposes other than that of when the consent was initially established. The infrastructure of ICT should be developed in alliance with the privacy laws and made compliant as well intelligent which learn by itself from the environment. This extra layer embedded in the system would educate the ICT structure and help system to authenticate as well as communicate with the perspective users. The existing literature on protecting individuals' privacy through privacy-enhancing technologies (PETs) is still embryonic and does conclude that the individual's concerns about privacy are not fully considered in the technological sense. Among other contributions, this research paper will devise a conceptual model to improve individual's privacy.**

Keywords—privacy; privacy enhancing technology (PET); big data; information communication technology (ICT)

I. Introduction

In recent years, the evolving nature of information systems and the increased processing and storage of personal information in computer databases has made it necessary for ICT practitioners and policymakers to take the issue of "privacy" more seriously [23],[28]. In particular, the complexity of cloud computing brings a number of known and unknown uncertainties to both service providers and users [12], [19]. The expanding quantity of personal data means that the demand for cloud computing will continue to rise [29]. However, the downside to such developments is the realisation that personal information is constantly recorded and stored without individuals' consent, therefore, raising a number of concerns. First, the reasons for the collection and the storage of personal information are often neither unknown nor disclosed to the people involved prior to their collection and storage [13]. Secondly, although most software is international, there is no standard mechanism for examining the quality of the databases used to store personal information [9]. Third, there are no uniform ways of handling personal data at the international level and on technical standards, which can help to demonstrate compliance with legal and regulatory frameworks.

Although the term "privacy" seems to have a number of definitions which are sector-specific and tend to carry different meanings depending on varying contexts. The definition that best suits this paper is the one that defines privacy as the right for individuals to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed. According to Guilloteau and Mauree [13] it is suggested that "…Privacy refers to the right to self-determination, that is, the right of individuals to 'know what is known about them', be aware of stored information about them, control how that information is communicated and prevent its abuse".

The meaning of privacy to individuals extends beyond disclosure by suggesting that privacy is also a fundamental human right (see Article 8 of the 1950 European Convention on Human Rights). There are a number of privacy laws and regulations that have been in force since the introduction of the

Internet, however, since then, there has been a number of technological changes – the latest being the privacy challenges brought by the use of "cloud-computing". In recent years, there have been a number of definitions of cloud computing [23], [28]. In this paper, we adopt Badger et al, [2] definition that describes it as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Sen, [34] simplified it further by suggesting that cloud computing does the network connect a server firm that can host the services for users to it. There is a common consensus in most definitions – all pointing toward the direction that "cloud-computing" exist in a very dynamic environment and hence future definitions are likely to change based on circumstances and contexts [26].

For instance, Pearson, [30] suggests that "the adoption of cloud computing may move quite quickly depending on local requirements, business context and market specificities". Due to the increased complexities in data collection, storage and dissemination, the economic potential of cloud computing cannot be underplayed [3]. However, there are challenges that seem to accompany the "cloud". First, there is a notion that the data stored and collected is universal. Pearson, [30] has argued that there are some challenges to providing cloud-computing services including the need to comply with local and regional regulations, obtaining the necessary approvals when data is accessed from another jurisdiction, some additional complexity in terms of governance, maintenance and liability inherent to cloud, and a perceived lack of trust in cloud services. However, along with these challenges, our focus is diverted to the provision of privacy to individuals through privacy enhancing technologies [32].

II. Privacy in the Era of "Cloud" and "Big Data

Privacy in the era of "cloud" or "big data" has formed an agenda [34]. This is mainly due to the challenges of maintaining trust within a dynamic environment. According to Blaze et al, [4], [38] coping and preserving the privacy of digital identities and challenges are associated with continuous attacks on databases across the world that has forced a number of organisations to deny that their systems have been under attacks [34].

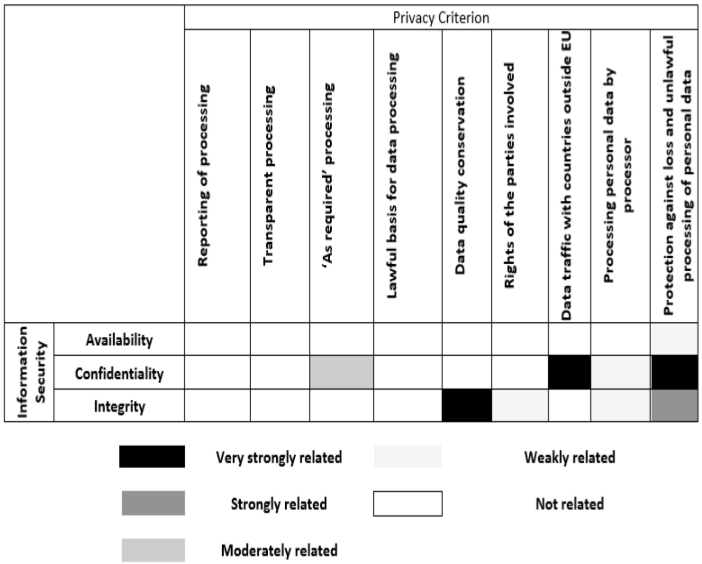
In this paper, our attention is particularly drawn to the "big data" or internally stored data that might be privacy-sensitive – hence the study of Privacy-enhancing technologies (PETs). The privacy enhancing technologies [14] are technologies that protect privacy by protecting personal data and preventing its unnecessary and/or undesired processing but also by making a user aware of the stored data, its processing and the related data flows [13]. PETs are seen as a way to maintain individuals` privacies by assisting data controllers' compliance with data protection principles, empowering individuals – by giving them easier access to and control over information about them and allowing them to decide how and when this information will be disclosed to and used by third parties [27].

There are a number of perceived benefits of using PETs. First, this is a cost-effective way of dealing with privacy issues from the onset rather than dealing with privacy and legal compliance issues at a later stage (or once the system is complete). Second, PETs are believed to act as "risk mitigators" using privacy controls incorporated into electronic information systems to supplement organisational procedures - thus providing additional safeguards to protect individuals' information from human error [27]. Third, PETs are seen as ways of building by maintaining the integrity of information held [7]. In this paper, four categories of PETs are examined; these include Encryption Tools (e.g., SSL), Policy Tools (e.g., P3P, TRUSTe), filtering Tools (e.g., Cookie Cutters, Spyware) and Anonymity Tools (e.g., Anonymizer, iPrivacy).

A. The Privacy Criterion: Information Life Cycle

The modern data information systems have changed the data protection risks as well as privacy concerns [38]. The new challenges have evolved and ICT can help to minimize and avoid challenges of data protection and privacy [16]. The privacy technologies have been the centre of attention of various researchers since 1970's. The concerns discussed were refining the privacy principles of identity protection and data minimization through pseudonymisation and anonymization [28]. These discussions led to coin a term "Privacy-Enhancing Technologies (PETs)" considering the full information life cycle from built-in privacy means. The features of data minimisation and privacy by default were stressed and addressed in particular when designing PETs [8].

TABLE I. Adapted from PISA Information Security vs Privacy [8]



		Privacy Criterion								
		Reporting of processing	Transparent processing	'As required' processing	Lawful basis for data processing	Data quality conservation	Rights of the parties involved	Data traffic with countries outside EU	Processing personal data by processor	Protection against loss and unlawful processing of personal data
Information Security	Availability									░
	Confidentiality			▒				█	░	█
	Integrity					█	░		░	▓

█ Very strongly related ░ Weakly related
▓ Strongly related □ Not related
▒ Moderately related

Different organisations implement various rules for measuring the information security and if they are not in compliance to privacy facts of individuals, alternative measures are required to be considered [1]. The attention must be paid to the process of system development especially in relation to those, which may cause privacy hazard in the infrastructure of ICT [22]. The current research is based on the assumption that there is no difference between the methodologies of system development for both private and public environments. Among other researchers, Spiekermann and Cranor, [31] has envisaged an integrated outlook of various techniques and methods with appropriate privacy compliance for the under construction systems. The envisaged model outlines the distinctiveness between Privacy-by-Policy, Privacy-by-Architecture and Privacy-by-Design.

B. Privacy-by-Architecture

The earliest possible stage of the system development project within information life cycle is intervened by this phase [23]. The technologies are implemented to minimize the personal data collection while keeping it anatomized and protected [20]. The system analyst evaluates the possible dimensions of data breaches at this level and appropriate measures are considered [24]. The procedures and rules are laid out in the form of specifications for the resulting blueprint. The system analyst who would help future users to avoid data breaches inadvertently could avert the pitfalls of programming functionalities.

C. Privacy-by-Design

The data protection policy makers have proposed the term of "privacy-by-design" [31]. This term was subsequently referred and used in various data protection policies as a recognized recommendation. Privacy-by-design is classified as a sub-part of privacy-by-architecture, which tests the development of Privacy Enhancing Technologies (PETs) at the conceptual paradigm allowing its compliance with ICTs [18]. Various researchers have studied PETs from different security aspects expressing the privacy possibilities for data management aiming to avoid the personal data breach through ICTs. The research led to believe that the users of using those services would be satisfied along with the service providers.

The suggested alternative solution involves interdependent stages since the data precision is decreased after the primary use of information. This solution expresses irreversible way to degrade the data. Among other researchers, Henze et al.,[18] that data degradation techniques could be implemented in five possible ways such as, suggests it: upgradable, user-oriented, ability-oriented, service-oriented and external data degradation. All techniques are responsible for built-in system functionality apart from user-oriented data degradation and it is held responsible for the process of data retention [19]. Along with other functionalities these techniques, rely on a single point of interaction to except external data degradation techniques. The entire life cycle of information is self-managed keeping one point of interaction for data degradation and this technique may lead to the privacy solution.

The fundamental issues linked to the implementation of this technique still urge the system architect to predict and ensure all the possible privacy breaches before its execution. These concerns may ensue during the whole lifetime of the ICT system [15]. The information technology is rapidly growing and this assurance is classified as highly contrived. On the other side, the privacy-by-architecture concludes that individuals have no right to say anything about their personal information. The individuals may have their perspective concerns and if they are not heard and managed up to their contents, this approach would be seen as an unwelcome outcome [25].

D. Privacy-by-Policy

The concept of privacy-by-policy keeps the central rule of "Notice and choice". The aim of delegating the information processes in the form of notifications, notices and privacy policies are educated to users. The users are flexible to make choices on their personal data to be used by the organisation on primary or secondary levels. The modern ICT's infrastructures use this rule as a common practice when deploying policies classified as "choice and consent". According to Spiekermann and Cranor, [31] this approach is connected with multiple problems of extensive policy documents of privacy and application of incomprehensive applications of millions of users. The privacy approach of "choice and consent" is quite famous within the modern businesses infrastructures, as this does not interfere within the existing layouts of using individual's personal information extensively [18].

III. Privacy Is Central to PETs and Cyberspace

We live in an information society where the use of personal information is constantly forming agendas – mainly, the question is whether since the information is in the open domain is free for everyone to use as they wish [36]. The right of privacy has been well documented in previous studies [27]. There are challenges associated with the use of PETs within the cyberspace environment. First, there is a recurring challenge as to whether computer experts and the technology could be used to protect individuals' privacy [21]. The answer to this is more complex and demands some empirical evidences.

For example, Rotenberg, [35] has argued that most practitioners tend to use Privacy Enhancing Technologies (PET) that create a technological framework that facilitates the disclosure of personal information, often without any assurance of protection or legal safeguards. He suggests that "these techniques which are often confused with true PETs are put forward by commercial firms and others as a "technical solution" to privacy when in fact they are designed to make it easier to obtain personal data" [29].

A. ICT and Privacy Enhancing Technologies

The information communication technologies (ICTs) and privacy are often expressed as opponents to each other [33]. The interaction between privacy and ICT is elaborated in this paper exploring the key detail of transmitting the privacy's conceptual framework to cloud environment. The concerns on individual's privacy are not new, as they have emerged more during the last half decade of Big Data and Internet of Everything [11]. Various books have been published and researches been conducted on the privacy issues concluding that there is no single rule which complies that the personal information is kept secure. These expressions mean that both new and the existing ICT systems may need to be re-assessed when deploying strategies. The Big Data breakthrough will be adopted into our society during the upcoming years. The continuous capturing of human environment information through sensors embedded within ICT will open new doors of privacy challenges [30].

The personal data of individuals, which used to be stored within organisational ICT systems, would now be residing on clouds in the future. In a traditional way, the term Big Data is associated with the information of users captured and contained by the ICT systems and various analytical tools are used to analyse it, which is the true form its smartness [5]. Information would be kept confidential and private by the organisations within the era of these technology developments. The privacy infringements implemented within ICT infrastructure are classified as "Law of Nature" which allows them to make choices as well. The organisations establishing ICT infrastructures to process data functionalities may not consider the individuals' privacy at the development phase but this may be applied in the operational phase.

B. *Formation of an ICT system: Privacy-Sensitive Paradigm*

Often with the system based on Internet of Everything there are added constraints in terms of power consumption, limited processing capacity and storage …. (Ibid, 2016) presented a conceptual model (User-driven Privacy Enforcement for Cloud-based Services in the IoE, UPECSI) to address these issues where Internet of Everything interact with cloud based services. One of the key elements of the presented model (UPECSI) was to give user control in a transparent way and the ability to make decisions in privacy settings at varying degrees, instead of accepting a privacy policy at the installation or induction of the service. The presented model was successful in highlighting the need for more control by the user in privacy policy and more user control over degree of services exposed to sensitive private information [10].

However, there seems to be a need for the continuous adaptation of the privacy policy in a dynamic changing environment of Internet of Everything based systems, and simply shifting the focus of privacy policy towards user may not fully address the privacy issues presented by such systems.

In many instances the user themselves would want their privacy policy to intelligently and seamlessly change as the context of use, situation and proximity is changed. In a fast paced dynamically changing and adapting scenario the complete reliance on user driven privacy policy approach may not prove adequate in fulfilling the demands of emerging systems based on IoE infrastructure. To this effect, Artificial Intelligence based approaches could have been injected in the IoE based systems where the Privacy Policy is not only intelligently adaptable but also has a capability to be trained by the user.

Hence, the abstraction layer is suggested for IoE based models where Privacy Policy is presented not as a static component in the system but has adaptable features to inform the services to what degree these can access the private and sensitive information. The training further trigger where behaviour, context of use, proximity, and situational patterns are transparently allowed to gain access at varying permissible degree and machine assisted technologies then reduce their reliance on user setting this information. This formation would be the case at the start of use of such system when the user would have been more involved in training the intelligent privacy components of IoE based systems.

The ISO certificates provide a measure of compliance for the standards in various sectors such as telecoms, energy, government etc. In 2014, 1,609,294 certificates were issued to management systems across the globe [20]. ISO/IEC 27002, [21] standard provide the framework for establishment of information security management system. The implementation of this framework enable the organisations to systematically preserve integrity and confidentiality of the information and manage the risks related to information security and privacy providing confidence to interested parties on information handling and security of data. The ISO/IEC 27001, [22] is designed to enable organisations to assess, implement and monitor security and privacy issues from internal and external contexts and at different layers of operation and management including understanding of needs and expectations of interested parties at holistic level.

The ISO27002:2013 is based on the guideline of ISO, [22] and framework enable organisations to implement the standard through instruments of control and objectives as provided in table 1. This ISO/IEC 27001: 2013 standard has major influence in directing the security and privacy policies and related structures for major corporates in telecom, service sector and government sector [16].

This framework has been adopted by many organisations around the world (more growth seen in China, India, EU and UK) saw a 7% growth rate from 2013 to 2014 with 23,972 certificates of standard issued by 2014. As the industry is experiencing a new shift towards IoE based systems, the importance of compliance and adherence to standards has become even more important even for small to medium size enterprise. The security and compliance standards needed to evolve in the wake of this shift and incorporate guidelines, measures and controls to keep the trust in the compliance of the standards by the certified organisations. As an example ISO/IEC 27002:2013 standard is discussed in relation to controls which may be needed to add to their existing set of controls for security and privacy compliance.

TABLE II. ADAPTED FROM (GUTIÉRREZ-MARTÍNEZ, [17] AND ISO, [22]

Category	**Control**	**Objective**
Policies and regulations of the organsiation	Information security policies (policies for information securiity,Review of the policies for information security)	"Direction accordance with business requirements, laws, and regulations."
	Organisation of information security ((Internal organization: Information security roles and responsibilites, segragation of duties, Contact with authorities, Contact with special interest groups, Information security in project management), (Mobile devices and telework: mobile device policy, Teleworking))	"To control the implementation and operation of information security."
	Human resources security ((Prior to employment: Screening, Terms and conditions of employment), (During employment: Management responsibilites, Information security awarenessm education and training, Disciplinary process), (Termination and change of emloyment: Termination or change of employment responsiilites))	"To protect the organization's interests ensuring that employees are aware of their information security responsibilities."
Privacy & Compliance	Asset management ((Responsibility for assets: inventory of assets, Ownership of assets, Acceptable use of assets, Return of assets), (Information classification: Classification of information, Labelling of information, Handling assets), (Media Handling: Management of removable media, Disposal of media, Physical media transfer))	"To ensure that information has an appropriate level of protection. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media."
	Access control ((Business requirments of access control: Access control policy, Access to networks and network services), (User access managemet: user registration and de-registration, user access provisioning, Management of priviliged access rights, Management of secret authentication information of users, Review of users access rights, Removal or adjustment of access rights), (User responsibilites: use of secret authentication information), (System and application access control: Information access restriction, Secure log-on procedures, Password management system, Use of privilged Utility programs, Access control to program source control))	"To ensure authorized user access for safeguarding their authentication information."
	Compliance ((Compliance with legal and contracual reqqurements: Idedtification of applicable legislation and contracual requirements, Intellectual proprety rights, Protection of record, Privacy and protection of personlly identifiable information, Regulation of cryptographic controls), (information security reviews: Independent review of information security, Compliance with security policies and standards, Technical compliance review))	
Integrity	Cryptography (Cryptographic controls: Policy on the use of cryptographic controls, key management)	"To protect the confidentiality, authenticity, and/or integrity of information."
	Physical and environmental security ((Secure areas: Physical security perimeter, Physical entry contorls, Secusring offices, rooms and facilities, Protecting against external and environmental threats, Working in secure areas, Delivery and loading areas), (Equipment: Equipment siting and protection, Supporting utilities, Cabling security, Equipment maintenance, Removal of assets, Security of equipment and assets off-premises, Secure disposal or re-use of equipment, Unattended user equipment, Clear desk and clead screen policy))	"To prevent loss, damage, theft, or compromise of assets and interruption to the organization's operations."
	Operations security ((Operational procedures and responsibilies: Documented operating procedures, Change management, Capacity management, Separation of development, testing and operational environments), (Protection from malware: Controls against malware), (Backup: Information Backup), (Logging and monitoring: Event logging, Protection of log information, Admisistrator and operator logs, Clock synchronisation), (Contorl of operational software: Installation of software on operational systems), (Technical vulnerability management: Managemtn of technical vulnerabilities, Restrictions on software installation), (Information systems audit considerations: Information systems and audit controls))	"To ensure correct and secure operations of information processing facilities and to protect against loss of data."
	System acquisition, development, and maintenance ((Security requirementss of information systems: Information security requirement analysis and specification, Securing application services on public networks, Protecting application services transactions), (Security in development and support processes: Secure development policy, System change control procedures, Technical review of applications after operation platform changes, Restrictions on changes to software packages, Secure developmetn environment, Outsourced development, System security testing, System acceptance testing), (Test data: Protection of test data))	"To ensure that information security is designed and implemented across the entire lifecycle of information systems."
	Supplier relationships ((Information security in supplier relationships: Information security policy for supplier relationships, Addressing security within supplied agreements, Information and communication technology supply chain), (Supplier service delivery management: Monitoring and review of supplier services, Managing changes to supplier services))	"To ensure protection of information that is accessible by suppliers."
Authenticity	Information security incident Management (Management of information security inceidents and improvements: Responsibilites and procedures, Reporting information security events, Reporting information security weaknesses, Assessment of and decision on information security events, Response to information security incidents, Learning from information security incidents, Collection of evidence)	"To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses."
Policies and regulations of the organization	Information security aspects of business continuity management ((Information security continuity: Planning information security continuity, Implementing information security continuity, Verify, review and evaluate information security continuity), (Redundancies: Availability of information processinf facilities))	"Continuity in information security management should be integrated into the master plan of the organization."

IV. Analysis and Discussion

The business models are transforming on a massive scale and this has changed their environment in which they exist and operate. This change has not left service providers free in their actions. The businesses and organisations are moving onto social media and a lot stress and emphasize has been accosted on the user's personal information exploitation. Millions of users have enrolled on various social media sites disclosing their personal information of highly sensitive nature unwittingly. The predictive analytic tools and cloud environments do not provide the privacy like PET integrate. The service providers could facilitate the users' demands and in return, the organisations could make huge revenue. The models of processing the user's personal data are more dependent on investments in cyberspace and PET. The internet companies have evaluated the sensitive information as an instrumental key to their success.

Although the businesses are operating in a model to provide privacy to the users' information but still the users have no obligations to give up their privacy and in this case, businesses would remain profitable. It is doubtless that the privacy and consent models would pose high threats on the business models as well as performances. This increased exposure of ICT as the way to privacy related problems forgoes the idea that it may well not resolve the entire problem, as cultural and social features are inextricably intertwined from the users' perspective. The privacy enhancing technologies defy the personal factors at a sufficiently elaborated level. This also leads information-processing negotiation from the consent perspective especially within the virtualised and cloud based environments.

The parties involved within the privacy awareness of information management have formed various concerns for individual privacies protection laws. The structural movement of cloud-based environments to service-oriented ICTs from ownership-oriented has made the individual privacy resolution almost impossible. The technological and legal aspects are well established and attended by PET but it deals with only certain parts of the ICT infrastructure. While looking at the existing situation from the real life perspective, it is assumed that the responsibility not only depends on ICT infrastructures but also assignable to user behaviour and their consents. The subject is not fully adhered to even after the implementation of procedures of privacy-by-architecture and privacy-by-design. The problem persists and shared between the development methods of ICT infrastructure and individuals who may be thinking that their information would be accessed by whom.

The social interactions are classified as highly volatile source of exploiting the personal sensitive information, which concludes that privacy is extremely implicit and inconclusive and that an ICT infrastructure as well as PET may not be able to defy the subtleties appropriately. Although ICT has evolved tremendously within the current age but still given the current state of technology, it is not feasible to asset pressures on system analyst and developers to exonerate the systems to express the privacy concerns. The development of PET should be moved onto the new conceptual frameworks of privacy-audited and privacy-aware systems. It is envisaged that instead of yielding blind trust, it is always better to go with informed consent when individuals establishing connections with ICT infrastructures through PET and disclose personal sensitive information.

A. *Envisaged Model Meets New Privacy challenges*

As Internet-based tracking and profiling technologies increasingly expand the ability for e-commerce vendors to collect, store, process and exploit personal data, privacy concern has been identified as a major factor hindering the growth of technologies to protect those. The concerns centre on the confidentiality of accumulated individual personal information and potential risks that individuals experience over the possible breach of confidentiality. The need to protect privacy has led to many initiatives, some behavioural and some technical. Behavioural initiatives generally include providing assurances through privacy seals, government regulations, or addressing individuals' concerns for information privacy, which have been shown to affect trust. While these approaches to protecting privacy are interesting, this paper focuses on an IT artefact that provides one technical solution to the online privacy issue. This approach is in line with a recent review of the privacy literature that highlights the need for more design research in the information privacy domain.

Information is a valuable source and most modern businesses rely on effective use of information for their processes, market reach, customer satisfaction and competitive advantage [9]. This demand for the valuable information puts strain on privacy and data related to personal liking, disliking, and behaviour. Etc. Information system has brought huge success to businesses in achieving their goals. The information system gathers process, distribute, utilise and interact with information [6]. The success of information systems is dependent on channelling communications effectively between different components of such system including people. The information security is an established discipline and with well-defined procedures and measures to this effect.

The Internet of Everything IoE is infusion and interconnectedness of information systems, ICT services/devices and sensor technologies resulting in vast amount of data constantly being generated and updated constantly [29]. This transformation is beginning to break the norms and new systems are based on IoE and are increasingly becoming part of our daily lives, for example smart watches, health and activity monitors. The proximity based services provided by apps using geolocation sensors, remote controlling of home heating system, and intelligent sensors in vehicles, smart rail tickets– the list is endless in many field stretching from leisure, medicine to transportation. The existing security and privacy practises are ill equipped to meet their objectives in the wake of this new shift from information age to the age of IoE [29]. IoE present endless opportunities for the malicious exploitation of such systems e.g. a connected house on low energy consumption might suggest to a hacker that the property is vacant and this information could be used maliciously [37].

The privacy data by the very nature is valuable in information age society, people are increasingly aware of this, and increasingly aware that without their explicit consent the modern system extracts their personal information and consumes to improve and target their services intelligently. The trend and benefits Internet of Everything brought and highlighted individual privacy concerns as a major obstacle in successful adoption of Internet of Everything as part of living experience at a wider scale [18]. Shifting the balance of privacy settings to individual user add complexity to the design and add burden on the individual user for the understanding and awareness of choices they make and related implication when opting for particular privacy choices or configurations. In many cases individual users are not fully aware of technical complexity of the system and processes in relation to privacy implications [18]. Finding the right balance between system centric and individual centric is a typical dilemma designers of the system face and this problem is exacerbated with the Internet of Everything thus adding complexity and points of pressure in the system in term of making decision for such issues.

V. Conclusion

The theme of this paper builds to form the basis of a dynamic ICT infrastructure, which helps individuals to be connected with each other while keeping the privacy of their personal information. Various searches been performed on databases to reveal that the privacy-awareness within ICT systems is still embryonic and various individual privacy aspects has not as yet been explored. The concept of individual privacy is expressed through laws and rules for organisations to inject privacy-aware concepts within their infrastructure. The professional and scientific committees have paid much attention on the development of various aspects of ICTs and it seems that the right of personal information privacy is lost within the boundaries of organisational amalgamations of laws and technological awareness.

In our view “Intuitive”, privacy and ICT privacy policies are clearly at odds, but legislators, service providers and the public concur in valuing privacy as essential to acceptance of information technology-based services. Providing proper privacy to individuals is therefore no matter of small concern. Making clear to all parties involved that their respective responsibilities cannot be delegated to ICTs is crucial. The infrastructure of ICT is developed in alliance to the privacy laws and made compliant as well intelligent which learn by itself from the environment. This extra layer embedded in the system would educate the ICT structure and help system to authenticate as well as communicate with the perspective users. Governmental, service providers and individuals’ concerns should be properly addressed to retain the privacy levels that form the essence of civil liberties and maintain freedom in society. To create a truly privacy-aware ICT, a holistic approach is needed in finding methods to shift control over information back towards the individual. Taking the ICT from an individual’s perspective as a starting point would allow for a first step towards a true impact analysis of ICTs on what is considered a building block of free societies.

References

[1] Anderson, A. (2005). A Comparison of Two Privacy Policy Languages: EPAL and XACML: Sun Microsystems Laboratories. from http://research.sun.com/techrep/2005/smli_tr-2005-147/ TRCompareEPALandXACML.html.

[2] Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: http://csrc.nist.gov/publications/drafts/800- 146/Draft-NIST-SP800-146.pdf (Accessed on: February, 2016).

[3] Birman, K., Chockler, G., & van Renesse, R. (2008). Towards a cloud computing research agenda, http://www.cs.cornell.edu/projects/quicksilver/public_pdfs/SIGACT2.pdf.

[4] Blaze, M., Kannan, S., Lee I., Sokolsky, O., Smith, J. M., Keromytis, A.D., & Lee, W. (2009). Dynamic Trust Management. IEEE Computer, Vol 42, No 2, pp. 44-52, 2009.

[5] Bennett, J. and S. Lanning (2007). The Netflix prize. In Proceedings of KDD Cup and Workshop.

[6] Beynon-Davies, P., 2013. Business Information Systems. 2nd edition ed. s.l.:Palgrave Macmillan.

[7] Bowers, K., Juels, A., (2009), Oprea, A.: HAIL: A high-availability and integrity layer for cloud storage. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS’09, pp. 187–198. ACM, New York, NY, USA (2009). DOI 10.1145/1653662. 1653686

[8] Borking, J. (2010) Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies, Deventer: Kluwer.

[9] Buyya, R., Yeo, C., & Venugopal, S. (2008). Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Retrieved January 21, 2016 from author’s website: http://www.buyya.com/papers/hpcc2008_keynote_cloudcomputing.pdf

[10] Cannon, J. C. (2005). Privacy: What Developers and IT Professionals Should Know: Addison-Wesley.

[11] G. Aggarwal, E. Bursztein, C. Jackson, D. Boneh, (2010), An Analysis of Private Browsing Modes in Modern Browsers, In: Proceedings of19th USENIX Security Symposium, Washington, DC, USA, pp. 79–94.

[12] Garfinkel T, Rosenblum M., (2005), When virtual is harder than real: Security challenges in virtual machine based computing environments. InProceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. CA, USA: USENIX Association Berkeley; 2005:227–229.

[13] Guilloteau, S and Mauree, V (2012) Privacy in Cloud Computing ITU-T Technology Watch Report March 2012 Retrieved from: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

[14] G.W. Van Blarkom, J. B. (2003). Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents. Retrieved from e-Europe: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15263-00-2005-Apr.pdf

[15] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st annual ACM symposium on Theory of Computing, pp. 169–178.

[16] Gartner, (2013). ISO/IEC 27001:2013 Shifts Focus From the Effectiveness of Controls to Risk Treatment Plans. [Online] Available at: https://www.gartner.com/doc/2630435/isoiec--shifts-focus-effectiveness
[Accessed 14 February 2016].

[17] Gutiérrez-Martínez, J., Núñez-Gaona, M. A. & Aguirre-Meneses, H., (2015). Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002: 2013 Standard.. Journal of digital imaging, 28(4), pp. 481-491.

[18] Henze, M. et al., (2016). A comprehensive approach to privacy in the cloud-based Internet of Everything. Future Generation Computer Systems, pp. 701 -718.

[19] Hashizume K, Yoshioka N, Fernandez EB., (2013), Three misuse patterns for Cloud Computing. In Security engineering for Cloud Computing: approaches and Tools. Edited by: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M. Pennsylvania, United States: IGI Global; 2013:36–53.

[20] ISO, (2014). iso_survey_executive-summary. [Online] Available at: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014 [Accessed 14 February 2016].

[21] ISO, (2016). ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements. [Online] Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
[Accessed 14 February 2016].

[22] ISO, (2016). ISO/IEC 27002:2013 (en) Information technology — Security techniques — Code of practice for information security controls. [Online] Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
[Accessed 14 February 2016].

[23] Jaeger, P.T., Lin, J., and Grimes, J. (2008). Cloud Computing and Information Policy: Computing in a Policy Cloud? Journal of Information and Politics, 5(3): 269-283.

[24] Jensen, M., Gruschka, N., Herkenhoner, R., (2009), A survey of attacks on web services. Computer Science – Research and Development 24(4), 185–197.

[25] Kobsa, A., & Teltzrow, M. (2005). Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing Behavior.

[26] D. Martin & A. Serjantov (2004.), Privacy Enhancing Technologies: Fourth International Workshop, PET 2004, Toronto, Canada (Vol. LNCS 3424, pp. 329-343). Heidelberg, Germany: Springer Verlag.

[27] Madhub, D (2012) PRIVACY ENHANCING TECHNOLOGIES An Absolute Necessity for Effective Compliance with Data Protection Laws. Available at: http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Vol7_EnhancingTechnology.pdf (February, 2016)

[28] Mell, P., & Grance, T. (2009). NIST Definition of Cloud Computing. Retrieved from NIST www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[29] Maras, M.-H., (2015). Internet of Everything: security and privacy implications. International Data Privacy Law, 5(2), pp. 99 - 103.

[30] Pearson, S., Benameur, A., (2010), Privacy, security and trust issues arising from cloud computing. In: Proceedings of the International Workshop on Cloud Privacy, Security, Risk, and Trust, CLOUDCOM'10, pp. 693–702. IEEE Computer Society, Washington, DC, USA (2010). DOI 10.1109/CloudCom.2010.66

[31] Spiekermann, S. and Cranor, L.F. (2009) 'Engineering privacy', IEEE Transactions on software engineering, vol. 35, no. 1, pp. 67-82

[32] PrivacyChoice, PrivacyChoice Tracking Protection List, 2010.

[33] Richards, K. and E. Jones (2008). Customer relationship management: Finding value drivers. Industrial Marketing Management 37(2), 120–130.

[34] Sen, J. (2011a). A Robust Mechanism for Defending Distributed Denial of Service Attacks on Web Servers. International Journal of Network Security and its Applications, Vol 3, No 2, pp. 162-179, March 2011.

[35] Solove, D.J., Rotenberg, M., and Schwartz, P.M. (2006) Privacy, information, and technology, New York: Aspen Publishers Online.

[36] Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2007). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. In proceedings of the Sixth Workshop on the Economics of Information Security, Pittsburgh, PA.

[37] Want, R., Schilit, B. N. & Jenson, S., (2015). Enabling the Internet of Everything. Computer, Volume 1, pp. 28 - 35

[38] Zetter, K. (2010). Google hackers Targeted Source Code of More Than 30 Companies. Wired Threat Level. January 13 2010. Available online at: http://www.wired.com/threatlevel/2010/01/google-hackattack/ (Accessed on: February, 2016).