ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0068

Big Issues for a Small Piece: RFID Ethical Issues

Mai Al-Sebae & Emad Abu-Shanab
MIS Department, IT College, Yarmouk University, Irbid, Jordan
maisebae@hotmail.com & abushanab@yu.edu.jo

***Abstract*. Radio frequency identifications RFID is becoming a widely used technology in many sectors. Despite of its benefits from tracking humans and things, it raises ethical concerns. This paper will explore research related to the ethical issues of RFID technology like privacy and security, coercion and green RFID issues. It is important to raise awareness related to the importance and seriousness of this technology, where it requires more legal control and support. This paper proposes a framework for future research to help researchers understand the issues embedded in such phenomenon and facilitate future research. Conclusions and future proposed research are depicted at the end.**

Keywords: RFID, security and privacy, Coercion, IOT, Tag, Ethics, Green, proposed framework.

I. INTRODUCTION

Recently, Radio frequency identification (RFID) technology became one of the most influential and popular technologies that supports business objectives, where it started as a military tool for spying, and evolved to serve many fields like medical, social, and business. RFID technology uses radio waves to track individuals and objects and collect information about their behavior to help make important business decisions. Like any technology commonly used, its usage should be explored from economic, social, health and ethical views. In this paper, after defining RFID technology, its applications and its impact, we will focus on the ethical issues related to this technology, and its impact on people's acceptance of such technology

This paper will talk investigate the literature related to privacy and security of RFID, the coercive implant of this technology without the knowledge of the person carrying it, the justification and consequences of such use. Finally, the paper will explore green and environmental issues of RFID. A proposed framework for research is proposed to understand better this phenomenon. Conclusions and future research propositions are stated at the end.

II. LITERATURE REVIEW

A. What is RFID?

RFID is a technology for identifying people and objects automatically. RFID was at first introduced as a "sister" technology to replace barcode system for identifying items [1][2]. It has attracted considerable attention in recent years. RFID not only replaces the traditional barcode technology, but also provides additional features and eliminates boundaries that limit the use of previous alternatives [3].

RFID consist of tags, software and reader [4]. RFID tag is a small, microchip devised to transmit wireless data [5]. RFID tag is often formulated by a small chip for storing data and an integrated transmitter antenna [1]. Tags are identified wirelessly by the readers by using some protocol of identification executed by readers and tags [6]. These tags operate at different frequencies and for that there is a need to employ different transmission mechanisms with different read-ranges, capabilities and bandwidths to penetrate sight line barriers. Still most of its use is for proprietary systems with specific use cases [7].

The technologies proliferation of automatic data acquisition, such as sensor and RFID technologies, aimed at improving the integrated environmental information systems (IEISs), decision support systems (DSSs), and environmental management. Such active and enduring topic for the scientists, engineers, and public administrators, involves broad issues beyond the use of many technologies [8]. Internet of things (IOT) is actuators and sensors mixed with the environment around us seamlessly, and shares information across platforms to develop a common picture for operating (COP) [9].

There are two types of RFID tags: active tag, which has embedded power source within it [1]. The second is passive tags, which doesn't have internal energy source (such as a battery). Passive tags get all the needed energy for functioning from an electromagnetic radiation transmitted by a reader. Communication between tags and reader is based on the "backscattering" principle in which the reader transfers energy to activate the tag, and then the tag replay by backscattering its identification data to the reader [10].

RFID technology has many advantages, such as improving real-time information traceability and visibility, quick reading, long distance recognition, and free obstacles[11][12]. Despite all RFID advantages there are some limitations and resistance from some parties especially organizations concerned with health, privacy, social and ethical issues. Cultural and religious factors may affect technology acceptability when related to RFID chips implanting in people for identification [13]. Helen Duce, director of the

doi:10.15849/icit.2015.0068

RFID Centre at Cambridge University in England, says "We have a clear vision to create a world where every object from jumbo jets to sewing needles is linked to the Internet" [14].

B. RFID Applications

RFID is used by a variety of applications, ranging from supply chain management (SCM) to library systems [6]. Retailers convinced that applications like RFID can improve customer services, allowing for real-time inventory management, reducing customer checkout time, and providing information for customized shopping during and after sale [15]. RFID chips are implanted in animals to track livestock, study wildlife behavior and locate missing pets. Amusement parks utilize technology to find lost children, and schools manage students' absenteeism. RFID also help locate, identify and monitor dangerous criminals, and also identify personnel military [4].

The success in animals-related applications has led to implanting RFID tags in humans. This might produce more dramatic outcomes than other application. However, its ethical issues become debatable when deciding the range of use/abuse because of RFID invasive nature [16]. RFID can be used in management of material, machinery, and men (M3). Management of material includes logistic and SCM, Inventory management, quality assurance, and waste management. Management of machinery consists of tracking machines and tools, machine operation and records, and machine maintenance records. Management of men includes access control, labor attendance records, and men safety [1].

From an ethical point of view, the most important issue is how such technology is used. Governments have considered RFID to track and control released parolees, convicts, and foreign visitors [16].In 2003, Wal-Mart enforced the adoption of RFID technology for its suppliers. RFID can be applied in inventory monitoring at retail-stores and it can be helpful for products replenishment on real time basis [17]. RFID applications are most likely to increase healthcare environment reliability [18], however, there are obvious privacy and security concerns related to storing medical and personal data. On the other hand, securing authentication of healthcare system/environment is still a challenge as it touches on issues of confidentiality, unforgeability, scalability, and location privacy issues [19].

RFID systems can be used in hospitals to verify patient's identity during medical procedures, locate equipment and collect data from staff workflow. RFID systems allow for the electronic tagging of inventory, assets, personnel, and patients, but there is a little empirical evidence on how to effectively implement such systems. RFID systems are not easily adapt to hospital settings because of its complicated infrastructure (in terms of equipment, space, personnel, and patients). Hospitals implementing RFID systems tend to experience two constraint types: 1) the technological system maladaptation to hospital settings, and 2)the organizational challenges for hospitals when utilizing the system [20].

Manufacturers are already using RFID technology in products that could putrefy during transportation due to extreme temperatures. The RFID reader will respond with data that indicates the state of product as well as its ID, when it interrogates the tag[3].Vehicle Traffic Congestion Estimation (VTCE) is another application of RFID, where a reader reads the tags installed on vehicles and transfer the necessary data to a database in a Central Computer System (CCS). CCS utilizes the data to locate the traffic congestion by following a specific procedure. However, it needs a high implementation cost compared to the devise, maintenance and installation cost [21].

C. Ethical Issues Of RFID

It's very important to judge any technology in terms of its ethical perspective because the compatibility and harmony of technology with morality (ethics) has a significant impact on its acceptance by the individuals and organizations at large. Three types of ethics are identified: computer ethics, information ethics, and cyber ethics [22]. This applies to the all ICT applications. Ethics aims to provide means to help discern what humans should do and how they should behave. It guides us to what is good or bad behavior, and deals with behaviors or actions rather than thoughts or feelings. It is also realized that what is an acceptable behavior in one culture might not be ethical in another [23].

Investigative panels in USA (including engineers and technicians developing RFID, military and commercial interests, and experts in ethics) should examine the directions of RFID and if the technology should be allowed to do that or not [16]. The following sections will examine three types of ethics that are related to RFID based on what has been reported in previous studies and they are: privacy and security, green RFID and Coercion of use.

i. Security and privacy

Research about ethical issues focused more on Internet security, like data theft and personal information hacking, and especially in business domains [23]. [24] Asserted that security is the protection of information systems holdings and controlling information access; he added that privacy means respecting individual's right to have information with an appropriate protection level. Despite the advantages of RFID, its application may challenge the privacy and security of organizations and individuals. However, the use of RFID systems raises new privacy and security issues. For RFID systems to become widely accepted by industry and end-users, security and privacy preserving authentication protocols are required [6].

The RFID introduction adds a new dimension to debates over consumer's privacy by allowing tracking of products after the point of sale. The issues at pin depend on two factors: how the item is considered to be personal, and the item mobility. It can be argued that ethical concerns arise more from tagging a library book than tagging a soup can. Greater privacy risk comes from embedding a tag in eyeglasses worn by a consumer continuously, than from embedding a tag in a

doi:10.15849/icit.2015.0068

"sofa" that remains in place. However, RFID does not break privacy any more than bar codes and credit card use, unless hackers have access to readers and to the associated databases [4].

Several threats to RFID systems are reported like: Eavesdropping which means listening in secret to communication between reader and tag by an illegal user, which is resolved by producing changing values that don't allow attackers to access significant data if they acquired it [11]. Secondly, traffic analysis to intercepting messages to deduce valuable data from patterns in communication between the tag and reader, which can be solved by adding random number in the tag and reader communication information. Thirdly, replay attack means valid data transmission is fraudulently delayed or repeated, it's carried out by an adversary who retransmits the data and intercepts or by the originator. Finally, one of the most serious privacy problems of RFID systems is tracking attack by attacker who can track the user's location information and risk users privacy, which can be solved using random number or timestamp.

Another solution to protect privacy is a privacy-preserving authentication "DPM" protocol introduced by [6] for RFID tags; DPM introduces a repeated identification technique. The tag sends several randomized secret hash keys, and the tags are identified by the reader by eliminating entries that do not match the hash result in its database successively. Despite the advantage of the DPM-protocol by reducing the complexity during the authentication on the reader-side, a major DPM-protocol drawback, and many others, is in the requirement to evaluate a strong encryption hash function.

The RFID technology users can be partitioned into individual, business and government. All of these classes of users can use RFID in a different way that proved beneficial to the generic population. Private sector enterprises can generate revenue from the technology. Also, consumers can benefit from technology by reduced prices and enhanced quality of service. Both of them can make tradeoffs between convenience and privacy when it is the time for opt-out options [4]. RFID privacy concerns with misbehaving readers and the problem of harvesting information from tags behaving well [11].

Issues of data security continue to be a challenge to this industry's growth. Retailers wish to use RFID to provide improved services, while customers may be afraid of entering environments and interested in transactions that could compromise their privacy. Customers' trust is the most important factor for retailers who aim to establish an RFID item-level retail store [15].

[7] Conducted a study to distinguish between three approaches to address consumers' concerns of privacy: First, to kill RFID tags at store exits (business-controlled). Second, if they want to initiate reader communication, then lock tags and have user unlock them(user controlled model).Third, to let the network access users' RFID tags while privacy protocol adhering (network model). The author concluded that the majority of consumers want to kill RFID chips at store exits rather than using any presented complex technical solutions. In addition, the desire to kill RFID tags is not caused by the fact that consumers do not recognize the value or benefits of RFID services but because of its seamless and ease of use of such approach. Despite of the service value which can be realized by RFID, customers are willing to forget these advantages in order to preserve their privacy.

RFID must attain some goals regarding privacy and security. The following are reported in the literature: Tags must not compromise holder's privacy, information should not be available to unauthorized readers or be possible to build long term tracking connection between tags and holders, holders should be able to find and disable any tags they load to prevent tracking, the output of publicly available tag should be easily or randomized modifiable to avoid the long-term connection between holders and tags, contents of private tag must be protected, both readers and tag should trust each other, spoofing either party should be hard, provide a control access mechanism and a mutual authentication between readers and tags also provides a measure of trust, and finally, concerns of session hijacking and replay attacks need to be resolved [25].

ii. Coercion

Receiving an RFID tag is purely a matter of consumer choice, and raises few serious ethical issues. The most important ethical issue is the possibility that the chips might be implied or implanted under real coercion, with the deep aversion or at least unease with many individuals[13]. Three concerns are raised: First, health risks to patients, like emitting radio waves that could cause migrating throughout one's body, tumors, or requiring surgery to be removed. Second, privacy; explained in detail earlier. The third is coercion, which means that patients (subjects or customers) are chipped without knowing that[5]. For example people with dementia are at risk for this reason as they fall within the most commonly marginalized groups in society; they are older, generally female and have concerns of mental health [26].

[27] Concluded through a study about tracking dementia (Alzheimer's disease) through a transmitter that some patients were happy to wear the transmitter, but later rejected it because they did not want to be kept on a lead. A more relevant ethical justification was that the RFID device had the ability to reduce the time spent to find lost patients, and lessening the chances that would cause an accident. RFID also can identify patients and improve the accuracy and streamlined delivery of health care, but they may also introduce new ethical, medical and social, risks. In general concerns about implants have been largely theoretical and concentrate on the devices safety, patients' records privacy, and coercion to consent to the devices implantation [5].

Decisions about using RFID need to be made by a broader group of stakeholders than engineers and companies involved in the field. A commitment must be made to enclose the technology to people who choose freely to carry it and protect others from implied or coercive implantation [13]. But in cases when RFID could aid in finding missing persons,

doi:10.15849/icit.2015.0068

kidnaped victims, lost hikers, lost high-profile personnel and children there's a debate if people are chipped in coercion or by their choice [16]. Tracking such categories is necessary to protect them or protect others from them.

iii. Green RFID

Green IT is the study and practice of manufacturing, designing, and using computers, monitors, servers, storage devices, printers, networking, and communication systems effectively and efficiently with the least impact on environment. It includes environmental sustainability, energy efficiency economics, and total cost of ownership. It incorporates the disposal and recycling cost of technology. Green IT is also about IT application to create energy-efficient, environmentally sustainable business practices and processes. IT can support, leverage and assist other environmental initiatives and create green awareness also[28]. RFID could indeed be green by improving environmentally responsible practices related to IT. Organization should not focus only on adding "economic value" (such as preventing its spoilage and accurately tracking a perishable item), but save operations' energy ranging from growing, harvesting, packaging and refrigeration [29].

A study of 13 cases that used green RFID (such as Wal-Mart, Nestlé Italy, Rewards for Recycling, Recycle Ban, Concept2Solution, Smart Vareflyt, Truck Tag, DHL Smart Truck, Strawberry, Indisputable Key, The City of London School for Girls, Multi Life Cycle Center and Promise) employed the (MECI) framework which is a short cut for green categories (Motivation, Execution, Challenges and Impacts). Motivation refers to the reasons that drive the green RFID projects adoption such as financial, operational and strategic reasons. Execution; refers to processes and Strategy that get executed during the project such as Unit level, Project progress and Partnerships. Challenges; refer to the Difficulties (technological and informational) faced during project implementation. Impacts; refer to unexpected and anticipated consequences from project implementation like environmental sustainability, business value and Social responsibility. Results indicated that the RFID challenge is to sacrifice profit for environment benefit and vice versa.

In order to consider any development sustainable, it should meet the present needs without compromising the future generation's ability to meet their needs[30].Applications related to the development of RFID antenna were ignored while facing the interconnected issues of the eco-friendly and economic field tag comprising substrate [31].

[28] add that there are two waves of green IT: 1) Internally focused on IT products reengineering and processes to meet compliance requirements and improving energy efficiency. 2) Externally focused on sustainability-based IT innovations, business transformation, and enterprise-wide sustainability. The alignment between ICT processes and practices with the three core sustainability principles (reduce, recycle, and reuse) and innovatively using ICT in business processes is the key to leverage benefits of the enterprise-wide sustainability.

[10]talked about antenna RFID as a "green" electronics solutions, which is robustness, flexibility and eco-friendliness, outstandingly the proposed read range antennas make them an absolute choice for industrial far field ."green RFID" is challenging because the Increase in complexities of operational processes and the possibility of sacrifice on economic benefits have limited the diffusion of RFID technologies as green[32].

In an experiment on the city of Grand Rapids for using RFID for green purposes, RFID tags allow for signing reject cart recycling and its related data of a specific customer and location. This provides a detailed ownership history, cart repairs, location, and allows monitoring city's cart asset during its useful life. They have now approximately 77 thousand carts on the street. They're able to produce specific participation rates to recycle refuse customers, something they weren't able to do with the reject bags; they were able to determine incinerator landfill tonnage diversions. They were able to measure efficiencies rout and allow for operational decisions to be quickly made. Finally, it maximized revenues from operating from recycling collections and refuse [33].

The literature reports some applications of green RFID projects; in Paris, more than one hundred thousand trees have an RFID tag that allows for an easier monitoring by municipality officials. Nestlé uses control temperature mechanisms to improve quality, reduce spoilage, and lower energy costs. Wall Mart Stores are working with men's jeans suppliers using RFID tags to be able to track these items to optimize its inventory management and indirectly reduce CO2 emissions [34].There are two approaches which may improve RFID support of green initiatives and sustainable development projects through the commitment to greening policies in RFID design or by contributing to some of the greening projects in general.

III. CONCLUSION

The main benefit of RFID is to identify people and things. It can largely enhance real-time information for decision making purposes. RFID is mostly used in SCM, heath care, traffic, and libraries. Researchers interested in the ethical side of technology are focusing more on privacy, security, coercion, and green issues. Privacy and security are attracting more research, while coercion is affecting the success or failure of such technology use. RFID raises a debate about the purpose and justification of this technology use without telling individuals. There is also great interest in green projects in line with institutions' care to highlight their interest in social responsibility and environment-friendly use of technology, where RFID provides great contribution for greening projects.

As we mentioned that RFID applications are becoming multi-purpose in helping organization and governments to track people, animals and objects. Each one of these categories has many uses and applicable examples as we summarized. The significance and sensitivity of privacy and security issues are increasingly attracting attention more than tracking animals

doi:10.15849/icit.2015.0068

and objects (unless these things are closely related to individuals). Similarly, the coercion issue is less significant when related to tracking objects and animals compared to humans.

This paper proposes a framework that map all the constituents related to the application of RFID. Such mapping guide future research and focus efforts towards a more comprehensive coverage of all issues related to the ethical issues of RFID. The frame work is built around three major dimensions: people, animals, and objects. People will be influenced by the security, privacy, coercion, and green IT issues. Humans are the most sophisticated dimension as they guard for future generations, and the environmental issues related to RFID. Animals are more related to environmental issues. Finally, objects are related to humans if they were implanted and used by humans, so some issues are common.

Research in RFID area needs to weigh the benefits of RFID vs. the cost of green IT issues and the risks of privacy protection. Such tradeoff is important to understand that the benefits realized from RFID need to be balanced against its risks and challenges. Keeping in mind the efforts by organizations in regard to social responsibility, it is important to keep revenue from RFID at acceptable levels. Finally, the RFID design needs to guard for the cycle of recycle, reuse and reduce.

This framework setup the stage for future research which can focus on areas depicted at the heart of the diagram. Also, technology adoption issues and trust are important to guarantee its success. Once researchers understood all aspects related to RFID implementation, they can better serve organizations employing it and future generations.

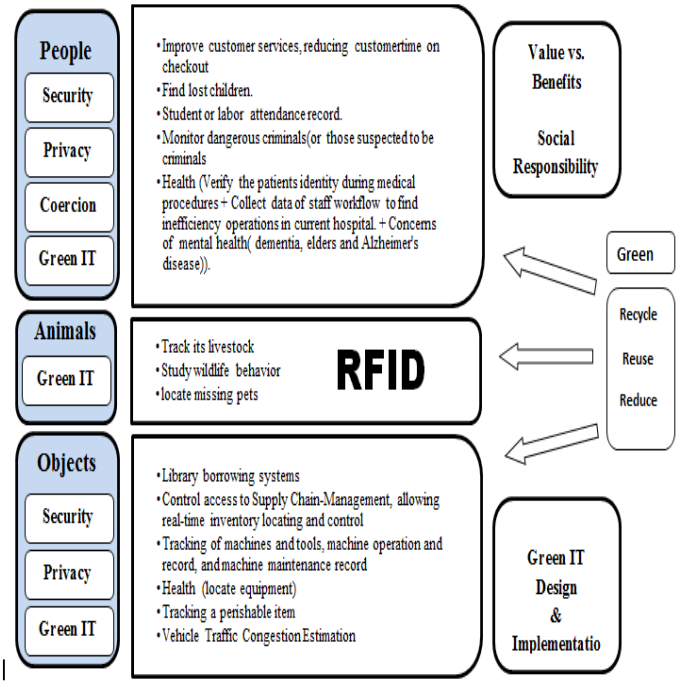

Fig. 1 How ethics is related to RFID

REFERENCES

[1] Lu, W., Huang, G. Q., & Li, H. (2011). Scenarios for applying RFID technology in construction project management. *Automation in Construction*, vol.20(2), pp.101-106.

[2]Bunduchi, R., Weisshaar, C., & Smart, A. U. (2011). Mapping the benefits and costs associated with process innovation: The case of RFID adoption. Technovation, vol.31(9), pp. 505-521.

[3]Want, R. (2004). Enabling ubiquitous sensing with RFID. Computer, vol. 37(4),pp. 84-86.

[4]Glasser, D. J., Goodman, K. W., &Einspruch, N. G. (2007). Chips, tags and scanners: Ethical challenges for radio frequency identification. Ethics and Information Technology, vol.9(2), pp.101-109.

[5]Monahan, T., & Fisher, J. A. (2010). Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices. International journal of technology assessment in health care, vol. 26(04), pp.370-376.

[6]Blass, E. O., Kurmus, A., Molva, R., Noubir, G., &Shikfa, A. (2011). The F_f-Family of protocols for RFID-privacy and authentication. Dependable and Secure Computing, IEEE Transactions on, vol. 8(3), pp. 466-480.

[7]Spiekermann, S. (2009). RFID and privacy: what consumers really want and fear. Personal and Ubiquitous Computing(Springer), vol.13(6), pp.423-434.

[8]Fang, S., Da Xu, L., Zhu, Y., Ahati, J., Pei, H., Yan, J., & Liu, Z. (2014). An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things. IEEE Trans. Industrial Informatics, vol.10(2), pp.1596-1605.

[9]Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, vol.29(7), pp.1645-1660.

[10]Amin, Y., Chen, Q., Zheng, L. R., &Tenhunen, H. (2012). Development and Analysis of Flexible UHF RFID Antennas for``Green. *Progress In Electromagnetics Research*, vol. 130, pp.1-15.

[11]Wang, M., & Pan, J. (2014). Authentication Test-Based the RFID Authentication Protocol with Security Analysis. *Sensors & Transducers*, vol.176(8), pp.1726-5479.

[12]Abu-Shanab, E. (2013). RFID Utilization in Libraries: The Benefits, Challenges and Future Directions. *First International conference "Libraries and Information Centers in a Changing Digital Environment,"* Amman, Jordan, October 29-30, 2013, pp. 1-17.

[13]Foster, K. R., & Jaeger, J. (2008). Ethical implications of implantable radiofrequency identification (RFID) tags in humans. *The American Journal of Bioethics*, vol. 8(8), pp. 44-48.

doi:10.15849/icit.2015.0068

[14]Smith, R.,E.(2013). New Cause for Concern: 'Internet of Things. *Privacy Journal*, vol.39, pp.3- 5.

[15]Yeh, H. (2013). Effects of RFID in Retailing on Customer Trust. *Journal of Service Science and Management*, vol. 6, pp.143-150.

[16]Labay, V., & Anderson, A. M. (2006). Ethical considerations and proposed guidelines for the use of radio frequency identification: Especially concerning its use for promoting public safety and national security. *Science and engineering ethics*, vol. 12(2), pp.265-272.

[17]Modgil, S., Patyal, V. S., &Agrawal, T(.2012). Technology Evolution in Supply Chain Management: BARCODE to RFID. *CPMR-IJT International Journal of Technology*, Vol. 2, (1), p.p27-32.

[18]Awawdeh, N. & Abu-Shanab, E. (2009). RFID in Healthcare Industry: A Strategic Framework for Implementation. A conceptual paper presented in the *Proceedings of the 4th International Conference on Information Technology (ICIT 2009)*, Amman, Jordan, pp. 1-18.

[19]Wu, Z. Y., Chen, L., & Wu, J. C. (2013). A reliable RFID mutual authentication scheme for healthcare environments. *Journal of medical systems*, vol.37(2), pp.1-9.

[20]Fisher, J. A., & Monahan, T. (2008). Tracking the social dimensions of RFID systems in hospitals. *International journal of medical informatics*, vol.77(3), pp. 176-183.

[21]Al-Naima, F. M., &Hamd, H. A. (2012). Vehicle Traffic Congestion Estimation Based on RFID. *International Journal of Engineering Business Management*, vol.4(2),pp .1-8.

[22]Ramadhan, A., Sensuse, D. I., &Arymurthy, A. M. (2011). e-Government Ethics: a Synergy of Computer Ethics, Information Ethics, and Cyber Ethics. *International Journal of Advanced Computer Science & Applications*, vol.2(8), pp.82-86.

[23]Salman, A., Saad, S., Ali, M., &Shahizan, N. (2013). Dealing with Ethical Issues among Internet Users: Do We Need Legal Enforcement. *Asian Social Science*, Vol.9(8), pp.3-8.

[24]Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International journal of the Computer, the Internet and management*, vol.10(2),pp. 1-22.

[25]Sarma, E. S., Weis, S. A., & Engels, D. W. (2002). White paper: RFID systems, security & privacy implications. Cambridge, MA: Massachusetts Institute of Technology, *AUTO-ID Center*,p.p1-16.

[26]Plastow, N. A. (2006). Is Big Brother watching you? Responding to tagging and tracking in dementia care. *The British Journal of Occupational Therapy*, vol. 69(11), pp.525-527.

[27]McShane, R., Gedling, K., Kenward, B., Kenward, R., Hope, T., & Jacoby, R. (1998). The feasibility of electronic tracking devices in dementia: a telephone survey and case series. *International journal of geriatric psychiatry*, vol.13(8), pp.556-563.

[28]Laplante, P. A., &Murugesan, S. (2011). IT for a Greener Planet. IT Professional, *I E EE Comp u t e r S o c i e t y*, vol. 13(1), P.P 16-18.

[29]Bose, I., & Yan, S. (2011). The green potential of RFID projects: A case-based analysis. *IT professional, I E EE Comp u t e r S o c i e t y*, vol.13(1),pp. 41-47.

[30]Corvalan, C., Hales, S., & McMichael, A. J. (2005). Ecosystems and human well-being: health synthesis. World health organization.

[31]Amin, Y., Chen, Q., Tenhunen, H., &Zheng, L. R. (2012). Performance-optimized quadrate bowtie RFID antennas for cost-effective and eco-friendly industrial applications. *Progress In Electromagnetics Research*, vol. 126, pp. 49-64.

[32]Yan, S., & Bose, I. Macau,(November 30 - December 4, 2009) RFID AS GREEN IT: LESSONS LEARNED FROM CASE STUDIES. *The 9th International Conference on Electronic Business*.,

[33]Angeles, R.(2013). Using the Technology-Organization-Environment Framework and Zuboff's Concepts for Understanding Environmental Sustainability and RFID: Two Case Studies. *International Scholarly and Scientific Research & Innovation*, Vol.7 (11), pp,1605-1614.

[34]Duroc, Y., &Kaddour, D. (2012). RFID potential impacts and future evolution for green projects. *Energy Procedia(Elsevier)*, vol.18, pp. 91-98.