ETHICAL ISSUES IN MONITORING AND BASED TRACKING SYSTEMS

OTHMAN O. KHALIFA, JALEL CHEBIL, AISHA-HASSAN ABDALLH AND SHIHAB HAMEED

Electrical and Computer Engineering Department,
Kulliyyah of Engineering, International Islamic University Malaysia,
Jalan Gombak, 53100, Kuala Lumpur, Malaysia.

khalifa@iim.edu.my

ABSTRACT: Monitoring and based tracking systems use a variety of technologies to record and monitor the activities of humans. This can increase the risks to the privacy and security of individuals. The amount of information gathered about individuals is growing through the proliferation of surveillance cameras, sensors; microchips and Radio Frequency Identification RFID tags embedded in devices and products. Advances in electronic technologies allow companies and government agencies to store and process large amounts of information about individuals. The Internet provides the ultimate copier device, making this information easily available to millions. This paper highlights the ethical issues emerging with the new technologies in the monitoring and base tracking system. New regulations should be proposed to protect the individual privacy.

ABSTRAK: Pemantauan dan sistem berasaskan pengesanan menggunakan pelbagai teknologi untuk merakam dan memantau aktiviti manusia. Ini boleh meningkatkan risiko dari segi privasi dan keselamatan individu. Jumlah maklumat yang dikumpulkan tentang individu berkembang melalui proliferasi pengawasan kamera, sensor; mikrocip dan tag frekuensi radio yang diletakkan di dalam peranti dan produk. Kemajuan dalam teknologi elektronik membolehkan syarikat-syarikat dan agensi-agensi kerajaan menyimpan dan memproses sejumlah besar maklumat mengenai individu. Internet menyediakan peranti salinan utama, menjadikan maklumat ini didapati dengan mudah. Kajian ini memaparkan isu-isu etika yang baru muncul dengan teknologi baru dalam pemantauan dan sistem berasaskan pengesanan. Peraturan baru perlu dicadangkan untuk melindungi privasi individu.

KEYWORDS: *privacy implications; tracking systems; ethical issues; RFID*

1. INTRODUCTION

Monitoring and based tracking systems are an emerging technology with significant potential benefits to domains requiring automatic retrieval of information about objects, such as packages, people, store merchandise, books in libraries, spare parts in repair depots, histories of objects through the manufacturing process, and many other applications. As the technology of monitoring and based tracking systems become more complex and affordable, it is becoming much easier to monitor and track people. As result, the issue of privacy of the individual becomes more serious since the available technologies make it easier for some abuser to invade the privacy of people. This study discusses the issue of privacy to three types of monitoring and

based tracking systems: Radio Frequency Identification (RFID), Global positioning System (GPS), and Closed Circuit Television (CCTV).

In this paper, Sections 2 to 4 describe the RFID, GPS and CCTV systems technology used in monitoring and tracking system. The issue of privacy is also discussed. Section 5 presents the Islamic view for the privacy of the individual. The protection of privacy from the emerging new technology is discussed in Section 6. Finally, Section 7 concludes the paper.

2. RFID TECHNOLOGY

There are RFID is an electronic tagging technology that allows an object, a place, or a person to be automatically identified at a distance using radio waves [1-2]. An RFID system can be composed of three subsystems: An RF subsystem, an enterprise subsystem, and inter-enterprise subsystem (National Institute of Standards and Technology, 2007). The *RF subsystem* performs identification and related transactions using wireless communication. The *enterprise subsystem* contains computers running specialized software that can store, process, and analyze data acquired from RF subsystem transactions to make the data useful to a supported business process. The *inter-enterprise subsystem* connects enterprise subsystems when information needs to be shared across organizational boundaries.

Every RFID system includes an RF subsystem, which is composed of tags attached to or embedded in objects and readers that query the tags. The *tags* also referred to as *transponders* are small electronic devices that are affixed to objects or embedded in them. The components of the tag are: a microchip and an antenna. The typical tag size ranges from a postage stamp to a pager [3]. Each tag has a unique identifier. Important characteristics of tags include their identifier format, the source of their power, the radio frequencies over which they operate, their size and shape, and additional functionality they support, such as security features and connections to environmental sensors (National Institute of Standards and Technology, 2007). The RFID reader is a device that wirelessly communicates with tags to identify the item connected to each tag and associate the tagged item with related data. Both the tag and the reader are two-way radios, and each has an antenna and is capable of transmitting radio signals.

2.1 Applications and Benefits of RFID Systems

The RFID systems are used by the industry, the commercial companies and security. Typical applications include labeling products for rapid checkout at a point-of-sale terminal, inventory tracking, animal tagging, timing marathon runners, smart card, smart passport, secure automobile keys, and access control for secured facilities [4][5]. In the commercial sector, RFID tags on products are used to manage inventories and supply chains. RFID employs a numbering scheme called Electronic Product Code (EPC) which can provide a unique identification for any physical object in the world. In addition, RFID tags identify lost items, and even keep tabs on people; the data carriers have assisted with surgeries, prevented the abduction of infants, and tracked teenagers on their way to school.

2.2 Privacy Threats from the RFID

Privacy is a very important topic for consumer acceptance of technologies. The consequence for misusing the RFID technology may rise to privacy issues. RFID technology is so revolutionary that it offers less than ethical characters unprecedented opportunities for theft, covert tracking, and behavioral profiling. Without the appropriate controls, attackers can perform unauthorized tag reading and clandestine location tracking of people or objects. RFID devices can be used to locate and monitor peoples without their permission; building up a detailed profile of a person based upon items in their possession; or even to impersonate individuals by replicating their RFID tags. Criminals can also manipulate RFID-based systems (i.e. retail checkout systems) by either cloning RFID tags, modifying existing tag data, or by preventing RFID tags from being read in the first place. Tag deactivation is a minimum requirement to fulfill privacy protection.

In most cases, individuals present unique identification numbers in an authentication process, as evidence that they are who they claim to be. According to Glasser et al.[14], "RFID does not violate privacy anymore than credit card and bar code use, unless intruders have access to readers and the associated databases.". On the other hand, the tag or the reader can be hidden without the knowledge of the person. RFID tags could be hided affixed to people, goods and documents, and then used to monitor and track the movements of these items or collect a profile of the individual by aggregation of the tags in that individual's possession. If RFID readers were secreted affixed into exit doors or other certain places, then the people dos know when tags in their belongs are being read, or for what for.

RFID technologies are almost unique in their ability to impact personal privacy in any of the four 'dimensions' of privacy:

- *Territorial privacy*: RFID devices could be used to monitor the location of objects, collect data information about the items surround the individual, or track the movements of objects.
- *Bodily privacy*: RFID devices with built-in sensors could be used to monitor the health of an individual, or even be embedded in their skin to track their movements.
- Communications privacy: packages, a post letter could be tracked with an RFID tags and know the destination.
- *Data privacy*: RFID devices embedded in equipments are now commonly used as authentication mechanisms for computer users.

These impacts raise many equations and concerns regarding privacy, On the other hand, peoples argue that RFID technologies may be used to protect peoples and goods. In other words, RFID technology could be used for better human life quality.
The ethical element would be based upon:

- Respect confidentiality
- Don't "flame"
- Don't be anonymous
- Don't allow third party to access other's data
- Don't misrepresent or lie
- Follow government's general guidelines
- Consider presentation of message

3. GLOBAL POSITIONING SYSTEMS

A Global Positioning System (GPS) uses a constellation of GPS satellites that orbit the earth. These satellites broadcast messages on radio frequencies that consist of the time of the message and orbital information. A GPS receiver measures the transit times of messages from four satellites to determine its distance from each satellite, and thereby calculate its location. This type of location data helps police with their investigations, such as tracking down a criminal or even someone who is lost or missing. They can act as a safety device to protecting your family and loved ones. Location technology also helps locate stolen cars. The technology for these tracking devices is constantly improving. It can be of huge assistance to those navigating in unfamiliar territory. In the United States, law enforcement officials use GPS technology to track criminal suspects and parolees without their awareness. For example, they may attach to the individual's car a device such as Track stick, which is a GPS data logger integrated with Google Earth [1]. Law enforcement officials argue that GPS devices fall outside the scope of laws regulating wiretaps and similar forms of electronic surveillance because they do not record conversations [2]. Some states have considered requiring GPS devices on all motor vehicles, to track the distances that they travel. Then states could collect taxes from motorists, in proportion to their mileage, to pay for the construction and maintenance of highways [3]. These vehicle mileage taxes would replace gasoline taxes, whose revenues will decline as the number of electric and hybrid-powered cars increases. GPSs are used by businesses, such as package delivery services, to track employees who travel to multiple. The GPS System has a number of major benefits. However, there is some potential that tracking data can be misused, and can be considered an invasion of privacy.

With the advanced trend of GPS technologies in wireless devices in order to accessorize them with navigation features [6], many raised equation about such information of using this technology. With accounts of law enforcement officials remotely activating mobile devices of suspects for audio surveillance [7], it is not hard to imagine that the GPS data could also remotely and surreptitiously be read providing a ubiquitous surveillance device. The combination of motorists and mobile phone users form a huge majority of the urban population and citizens should not be victims of mass surveillance or privacy abuses based on location data. Rigorous ethical and legislative safeguards need to be implemented to protect future abuses of individuals privacy in this context. Location technologies are still in their nascent stages, therefore, from a technology point of view, it is important to dispel these privacy concerns right from the beginning, and focus on building in privacy protection within such systems so that as new applications become available, appropriate privacy measures are integral to them [6].

4. CLOSED CIRCUIT TELEVISION (CCTV)

CCTV cameras have become more advanced in recent years and it can now isolate and track identified targets, recognize number-plates, and eavesdrop on conversations. CCTV has spread in the last few years. CCTV cameras are now used not only on motorways, where you'll receive warning about upcoming cameras, but also on cash machines, housing estates, and car parks [8]. The Closed Circuit Television (CCTV) is considered as a technical solution to security problems. It can assist effectively in preventing, detecting, and/or prosecuting crimes ranging from

major terrorism to minor vandalism. With the help of CCTV, both public and private spaces can be made more secure. However CCTV cameras were not only used to prevent crimes, it also been used by employers wishing to check up on staff or ensure that customer service is up to the standard. In addition, they are used to monitor certain group of people or race without their knowledge. This may be an intrusion on privacy. It is largely this potential problem with CCTV that has been regulated against [9]. CCTV is found anywhere. Many has been permitted the use of CCTV in public areas including shopping malls, motorways and housing estates. Regulations require a sign providing information for contacting the camera operator wherever CCTV is used in a public area. These signs should be made visible when you enter a camera-monitored area [8].

5. INFORMATION PRIVACY: AN ISLAMIC PERSPECTIVE

As discussed earlier, tracking system technologies introduce new challenging privacy issues. Protection of personal information has become rapidly important in term of privacy. The advance in technology creates new security challenges related to the protection of personal information. It also provides information about guidelines that address the collection, use and disclosure of personal information. Privacy is an essential factor related to human right and freedom society. It is included in the foundation of the rule of law, patient confidentiality, lawyer-customer privilege, private property, and many other fields related to the autonomy of the individual. With the rapid development of new information and communication technologies in the 21st century, the ability of the government and the private sector to collect, record and "mine" personal information has grown exponentially. The critical change related to the privacy happen after September 11, 2001 incident, where legislators struggle to balance security against civil liberties, privacy is likely to remain an important social and political issue. The reality shows that protection of personal information has become with very low priority compared to security aspects, which leads to sever unfair treated for many innocents. One of the critical issues related to using monitoring or tracking systems is the collection of personal information for an illegal or unethical purpose which is against privacy.

Islam is the last religion revealed to the world, which is comprehensive, fair, and lead to goodness in this life and the hereafter. The privacy is one of the essential factors in Islamic life. Several verses in Quran as well as many saying from Prophet Mohammed (peace and blessings be upon him) mentioned directly or indirectly the importance of respecting the privacy of any person. Allah SWT request us to avoid suspicion, spy not on each other as shown in Quran “O ye who believe! avoid suspicion as much (as possible): for suspicion in some cases is a sin: and spy not on each other nor speak ill of each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay ye would abhor it...but fear Allah: for Allah is Oft-Returning Most Merciful” (Qur'an, 49:12).

The general text of the Qur’an on the prohibition of spying similarly means that all varieties of espionage are included. Furthermore the Qur’anic text on espionage is immediately preceded by an address to the believers to “avoid indulgence in suspicion, for surely suspicion in most cases is sinful, and spy not…” (Qur’an, 49:12). Espionage originates in suspicion, which is also to be avoided as far as possible, although the wording of the text is not as categorical on suspicion as it is on

spying. The text here seems to permit suspicion that is based on reasonable grounds [6]. The point, however, is that both are seen as a threat to personal dignity and a violation of the individual's right to privacy. The prohibition of spying also includes opening of personal letters and confidential correspondence. This is, in fact, the subject of a Hadith to the effect that "one who looks into the letter of his brother without his permission is like looking into the fire of Hell." (Al-Suyuti, Al-Jami As-Saghir, p. 165; Ibn Majah, Al-Adab Al-Shariyya, vol. 2, p. 166).

6. PRIVACY PROTECTION

New Methods for ensuring customer and staff privacy have to be developed. Any organization that pilots or implements the monitoring and based tracking systems may consider the consequences impact of the privacy aspects. Organizations that using the monitoring systems may gained some benefits through the use of these technologies in applications such as stock control, safety, security, commitment and loyalty management. However, privacy advocates may cause many adversities which may affect the members of the organization. Such problems could be avoided if the users avoid reputation damage and risk of legal action. Therefore privacy related issues should be considered prior to implementing of any emerging technology. This is can be done through a risk management process, which should address a number of key questions including: these technology be affixed to items that may used beyond the control of the organization. Is it necessary to keep or process privite information within these systems?

Is the consequence impact of a privacy incident outweighing the possible benefits arising from the use of technologies?
Can the organisation ensure that every member and sister organisation will keep the privacy of personal information, and use these systems in proper manner?

Since no amount of privacy or security measures that may control these systems, the abuse by authorised users may happens. An effective mechanism may be used to reduce the risk of privacy violation and protect both the individual and the organisation in the event of such problems.

7. CONCLUSION

Privacy protection becomes increasingly harder as the technology becomes more widely deployed. It is often demanded, but rarely implemented. Each time a new consumer technology is introduced, the protection of private data is seen as a burden to quick deployment. Privacy problems in Monitoring and Based Tracking Systems, such as the information leakage, traceability and impersonation are a challenging issues.

REFERENCES

[1] Evsenkorkmaz and Alp Ustundag, Standards, Security & Privacy Issues about Radio Frequency Identification (RFID), RFID Burasia 1st Annaual Conference, pp. 1-10, sept. 2007.

[2] N. C. Wu, M. A. Nystrom, T. R. Lin, and H. C. Yu, Challenges to RFID Adoption Management for the Globale Future, PICMBT, vol. 2, pp. 618-623, July 2006.

[3] Razaq, Wai Tong Luk, Kam Man Shum, Lee Ming Cheng, and Kai Ning Yung, Second-Generation RFID, Security & Privacy. IEEE, vol. 6, no. 4, pp. 21-27, july-Aug. 2008.
[4] Juels, RFID security and privacy: a research survey, Selected Areas in Communications, IEEE Journal, vol. 24, no. 2, pp. 381-394, Feb. 2006.
[5] Klaus Finkenzeller, RFID Handbook, Radio-Frequency Identification Fundamentals and Applications, Wiley, 1999.
[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, RFID Privacy Issues and Technical Challenges, Communications of the ACM, vol. 48, no. 9, pp. 66-71, Sept. 2005.
[7] Juels, R. L. Rivest, M. Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, In Proceedings of 10th ACM Conference on computer and Communications Security (CCS'03), 2003.
[8] Muhammad Usman Iqbal, Samsung Lim, Privacy Implications of Automated GPS Tracking and Profiling", IEEE technology and society magazine - IEEE Technol soc mag , vol. 29, no. 2, pp. 39-46, 2010.
[9] McCullagh, D & Broache, A 2006, FBI taps cell phone mc as eavesdropping tool , *CNET News*, viewed 10 April 2007, http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100- 1029_3-6140191.html
[10] http://www.yourprivacy.co.uk/CCTVSystems.html , viwd April 7, 2011.
[11] Ann Rudinow Sætnan, Heidi Mork Lomell and Carsten Wiecek, "Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations", *Surveillance & Society* CCTV Special (eds. Norris, McCahill and Wood) 2(2/3): 396-414, 2004.
[12] Floerkemeier, R. Schneider, M. Langheinrich, Scanning with purpose - suppporting the fair information principles in RFID protocols, 2nd International Symposium on Ubiquitous Computing Systems UCS, 2004.
[13] H. Lee, J. Kim, Privacy Threats and Issues in Mobile RFID, The First International Conference on Availability, Reliability and Security (ARES '06), 2006.
[14] J. Kim, E. Y. Choi, D. H. Lee, Secure Mobile RFID System Against Privacy and Security Problems, Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'07), 2007, pp. 67-72.
[15] D.J. Glasser, K.W. Goodman, and N.G. Einspruch, "Chips, tags and scanners: ethical challenges for radio frequency identification," *Ethics and Information Technology*, vol. 9, no. 2, pp. 101-109, July 2007.
[16] Katherine Albrecht, "RFID: Tracking everything, everywhere", http://www.michaeljournal.org/rfid.asp, viewed April 8, 2011.