American Research Journal of Business and Management
(ARJBM)
ISSN (Online) : 2379-1047
Volume 2016, 5 pages

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Research Article Open Access

Ethics and Smart Governments: The Case of National ID Smart Card in the United Arab Emirates

Dr. Akram Almatarneh

Assistant Professor of Business Administration
American University in Dubai (AUD)
United Arab Emirates
amatarneh@aud.edu

Abstract: This paper examines United Arab Emirates' national ID smart card, which was implemented as part of the smart government. An attempt will be made to examine the ethical issues of the national ID smart card with respect to individual privacy. These national ID cards were selected as a case study for several reasons. First, the national ID smart card is the largest smart government project to be implemented by the Federal Government (UAE). Second, the government agencies in UAE involved in this project possess the largest amount of personal information concerning all people residing in UAE (local or expats). Third, individuals are unable to make any transactions without presenting their national ID card. These transactions vary from applying for credit card, home loan, opening bank accounts, to renting a car. The individuals who are the subject of this project are unaware of how the smart card works. They also do not know how the technology will be used to collect, store, access, and transfer their personal information. Therefore, this paper firstly examines the specifications (types) of the smart card technology and addresses the privacy implications of this technology. The next part contains some examples of how smart card technology could affect individual privacy in UAE.

Key Words: Ethics, Individual Privacy, Smart Government, and Smart card.

INTRODUCTION

This paper examines UAE's smart card project, which was introduced as part of the country's e-government. An attempt will be made to examine the impacts of the project on individual privacy. The project was selected as a case study for several reasons. First, the national smart card is the largest e-government project to be implemented by the UAE government. Second, the government agencies involved in this project possess the largest amount of personal information concerning the country's citizens (national and/or expats). The government agencies participating in the project include, but not limited to: Roads and Transports Authority (RTA), Immigration Departments, Health Department and Central bank of the Emirates.

The individuals who are the subject of this project are unaware of how the smart card works. They also do not know how the technology will be used to collect, store, access, and transfer their personal information. Therefore, the next section firstly examines the specifications (types) of the smart card technology and addresses the privacy implications of this technology. The next part contains some examples of how smart card technology could affect individual privacy in UAE.

What is a 'smart card'?

A smart card is simply a plastic rectangle containing a microchip, and holding a certain amount of readable data.[1] It can be in the form of a memory card or a processing-enabled card. A memory card, which is the simplest form of a smart card, has limited capability to securely store personal information.[2] This type of card is usually used for repetitive transactions, and examples include the prepaid telephone card or a building access 'key'.[3] The processer-enabled card is more sophisticated. t has self-contained computer processing capabilities to store, manipulate, code, decode and access data.[4] Software and functions on the card can be updated or changed, without the need to replace the card itself. As for information storage, the smart card can hold significant amount of information equivalent to several full-size printed pages of information.[5] In addition, a smart card is capable of creating and modifying data and it can perform calculations and respond to external

[1] Simon Newman and Gavin Sutter, 'Electronic Payments- The Smart Card: Smart Cards, E-Payments & Law- Part I' (2002) 18(4) Computer Law & Security Report 235.

[2] Katherine M Shelfer and J. Drew Procaccino, 'Smart Card Evolution' (2003) 45(7) Communications of the ACM 83, 84.

[3] Mario Devargas, Smart Cards & Memory Cards (1992) 7, there are two types of memory cards: silicon based cards and magnetic medium based cards.

[4] Robyn A Lindley, Smart Card Innovation (1997) 15.

[5] Rina C.Y Chung, 'Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America' (2003) 4(2) Asian-Pacific Law & Policy Journal 519, 531.

signals due to the 'micro-controller' built into the card.[6] The term 'smart card' in this section largely refers to cards with processing capability.

There are two types of smart cards: 'contact smart cards' and 'contactless smart cards'. The information contained on a contact smart card can only be read if the card is inserted directly into a card reader. Contactless smart cards, however, use low-frequency radio waves to communicate with readers. Accordingly, they can be read from distance of about six inches, and can be read without being removed from a purse or wallet.[7]

Governments worldwide, including the United Arab Emirates, have been increasingly interested in replacing traditional identification (ID) cards with smart cards. For example, China is in the process of issuing in excess of 800 million contactless ID cards (called the Second Generation National ID Card) with no biometrics and no other applications. Further, a number of countries including: Malaysia, Brunei, Bahrain, Saudi Arabia, and Oman have adopted national ID smart cards using fingerprint technology.[8] In the US, and as a result of the events of 9/11, a heated debate over the introduction of a national ID smart card. On the one hand, its proponents point out that a national identification smart card would be more reliable than current forms of identification to be used to reduce illegal immigration and the crime rate.[9]

The smart card can be used to combat identity theft and abuse of welfare privileges, increase the efficiency of government services by centralising information, and even allow for rapid border crossings. Thus, the implementation of ID smart cards may be viewed as an investment in infrastructure to accommodate future technological advances that will facilitate more efficient interactions between people and government.[10]

On the other hand, opponents of a national identification smart card suggest that such cards do not guarantee that the apparent identity of an individual is that person's actual identity. In addition, it is impossible to create a biometric-based national ID card that includes information with a100 per cent accurate. Furthermore, opponents of a national ID smart card point out that there is no evidence that these ID cards will lead to a reduction in crime.[11]

The 9/11 tragedy, however, has had profound impacts on the American people's perception of privacy.[12] In May 2005, for example, President George W Bush signed the REAL ID Act of 2005,[13] which significantly changes driver's licences in the US. The REAL ID Act specifically mandated that, to be accepted as legitimate identification, documents by US federal agencies, and driver's licences and other cards issued by the State Department of Motor Vehicle (DMV) offices would have to incorporate a standard set of features, a digital photograph of the individual's face and tamper-resistant, machine readable technology.[14] These licences are required in a number of transactions, including opening a bank account, purchasing air tickets, entering a federal building, or receiving a government service, such as social security cheque.[15]

The Privacy Implications of Smart Cards in UAE

The use of smart card technology in UAE raises several privacy concerns. One concern is that a smart card that is used by several government agencies and/or private entities may lack a central data controller. As a result, it may be unclear who is responsible for the use, disclosure, accuracy and security of the information collected by the smart card technology.[16] For better understanding of privacy implications of smart cards, this paper demonstrates the following scenarios:

[6] Mario Devargas, Smart Cards & Memory Cards (1992) 9.

[7] Karel Neuwirt, 'Report on the Protection of Personal Date with Regard to the Use of Smart Cards' (Council of Europe, 2001) <http://www.coe.int/...ts/1Report_Neuwirt_smartcards_2001.pdf> at 13 June 2009.

[8] Zeinab Karake-Shalhoub, 'Population ID card system in the Middle East' in Collin J Bennett and David Lyon (eds), Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (2008) 129-30.

[9] Michael J Quinn, Ethics for the Information Age (3rd ed, 2009) 264.

[10] Rina C.Y Chung, 'Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America' (2003) 4(2) Asian-Pacific Law & Policy Journal 519, 520.

[11] Michael J Quinn, Ethics for the Information Age (3rd ed, 2009) 264.

[12] Marc Rotenberg, 'Modern Studies in Privacy Law: Privacy and Secrecy after September 11' (2002) 86 Minnesota Law Review 1115

[13] Real ID Act of 2005, USC 49 §30301 Pub. L.109-13, <http://epic.org/privacy/id-cards/real_id_act.pdr> at 29 December 2010.

[14] Kelly Gates, 'The United States Real ID Act and the Securitization of Identity' in Colin J. Bennett and David Lyon (eds), Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (2008) 218.

[15] Michael J Quinn, Ethics for the Information Age (3rd ed, 2009) 265.

[16] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008) 405.

(a) Scenario one: Sarah wishes to apply for a governmental position in Dubai as she has just obtained her university degree. At the age of 18, she suffered from depression and anxiety. Her smart card shows that she received multiple prescriptions for those health conditions. A month after applying for the government position, she receives a letter stating that her application was unsuccessful due to her past health condition.

(b) Scenario two: as a result of the above, Sarah decides to become a self-employed and purchases a commercial vehicle to work as transporter. When she approaches XYZ (a motor vehicle insurance company in Dubai), she was quoted with the highest premiums for car insurance. The company explains that this is due to her medical condition.

(c) Scenario Three: Sarah receives an offer to work in the banking industry. She met Mohammad who works in an insurance company XYZ. Sarah and Mohammad fall in love and decide to marry. However, Mohammad wants to add Sarah to his private health cover provided to him by his company XYZ. Mohammad discovers Sarah's medical condition when he enters her name into the XYZ systems. Mohammad then decides to call the marriage off.

The above scenarios show various uses of smart card linked to a particular individual. Widespread use of smart cards that are linked to identifiable individuals may mean that individuals no longer have the option of transacting anonymously.[17] The individual's every move could be monitored, yet he/she may not have any knowledge of this surveillance. Beyond privacy, such a state of affairs does not bode well for the exercise of other fundamental freedoms such as the right of association or the right to seek, receive and impart information, especially as the intimidation of surveillance can serve as a very restrictive force.[18] Further, widespread use of these cards could enable vast amounts of information about the activities of cardholders to be collected and stored. In the future, smart cards could:[19]

Generate records of the date, time and location of all movements on public and private transport systems, along with details of all goods purchased, telephone use, car parking, attendance at the cinema, and any other activities paid for by smart cards.

These records could then be used by smart card operators or third parties for a number of purposes, for example, to generate detailed profiles of individuals in order to market goods and services to them. Third parties, such as insurance firms, may also seek such profiles.[20] Furthermore, smart card could be used to aggregate sensitive information about individuals for purposes other than those for which the information was initially collected, which could compromise privacy.[21] The subsequent data aggregation generates a greater imbalance between the power of the data collection agency and that of the individual which is damaging to the individual's privacy. As a result, smart cards could eliminate the possibility of individuals refusing to give personal information to government agencies and this poses an exponentially greater risk to personal privacy.[22]

Smart cards may be used as either a technology of privacy or a technology of surveillance, depending on whether the information collected is encrypted, whether it resides only on the card itself, or transmitted to a central database facilitating tracking and monitoring of individuals' activities.[23]

Furthermore, the potential for 'function creep' has long been a concern in regards to the collection of personal information. 'Function creep' occurs when information gathered for a defined, specific purpose and recognised as being gathered for that specific purpose, is subsequently used to provide information pertaining to different objectives.[24] With the contactless smart ard, it is possible to read information without the cardholder's knowledge or consent.[25]

Finally, the security of a smart card system depends on the reliability and security of the various component of the system

[17] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008)404–05.

[18] UNESCO, 'Ethical Implications of Emerging Technologies: A survey ' (2007) 40.

[19] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008)405.

[20] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008)405.

[21] United States General Accounting Office, 'Electronic Government: Challenges to the Adopting of Smart Card Technology' (2003) 14.

[22] Alan S Reid, 'Is Society Smart Enough to Deal with Smart Cards?' (2007) 23 Computer Law & Security Report 53, 56.

[23] Ann Cavoukian and Don Tapscott, Who Knows: Safeguarding Your Privacy in a Networked World (1997) 78.

[24] Mark O'Brien, 'Law, Privacy and Information Technology: a Sleepwalk through the Surveillance Society' (2008) 17(1) Information & Communications Technology Law 25, 31.

[25] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008) 405.

— that is, the security of the data pathways between the smart card and any reading, processing, storage or transmission system.[26] The 'working' component of the chip in the smart card contains information is specifically about the cardholder such as the person's health card information. The 'secret' part of the chip contains information that cannot be accessed by the cardholder without the use of a personal identification number or password. The 'super secret' part of the chip contains information and programs placed there by the chip manufacturer and/or the issuer of the card-the chip manufacturer can only access this area.[27]

The smart card proponents have argued that smart cards can actually protect individual privacy. In some situations, smart cards may certainly have an important role to play in keeping information secure, which may in turn enhance individual privacy. For example, access control smart cards have proved useful for computer networks. Passwords leave computer systems vulnerable to attack, but access control smart cards offer much more accurate identification and more details information about users' access right.[28]

Smart card proponents have also argued that smart card systems need to be introduced in order to reduce credit card fraud. But this is only a legitimate argument for upgrading the security of credit cards, not for introducing stored value cards (SVC) as a replacement for cash. The decision to add stored value functions to credit cards has a serious adverse impact on privacy, but no impact on security.[29]

Conclusion

In the light of new technologies advancement, including smart cards in particular, individual privacy become is seriously threaten by the implementation and use of these cards by government as well as private institutions. It is significant for smart cards' holders to become aware of threats and risks associated with the use of smart cards. The paper suggests for more research on the issue as well as developing safeguards and policies to regulate and control the access personal information stored on the smart cards. Further, it is recommend that UAE government create, a first-of its-kind-an independent commission with its main responsibility the maintenance and protection of individual privacy in the UAE.

References

Cavoukian, Ann and Tapscott, Don, Who Knows: Safeguarding Your Privacy in a Networked World (1997)

Chung, Rina C.Y, 'Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America' (2003) 4(2) Asian-Pacific Law & Policy Journal 519

Devargas, Mario, Smart Cards & Memory Cards (1992)

Gates, Kelly, 'The United States Real ID Act and the Securitization of Identity' in Colin J. Bennett and David Lyon (eds), Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (2008)

Hart, Caroline, 'Micro-Chipping Away at Privacy: Privacy Implications Created by the New Queensland Driver Licence Proposal' (2007) 7 Queensland University of Technology Law & Justice Journal 305

Karake-Shalhoub, Zeinab, 'Population ID card system in the Middle East' in Collin J Bennett and David Lyon (eds), Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (2008)

Lindley, Robyn A, Smart Card Innovation (1997)

Neuwirt, Karel, 'Report on the Protection of Personal Date with Regard to the Use of Smart Cards' (Council of Europe, 2001)

Newman, Simon and Sutter, Gavin, 'Electronic Payments- The Smart Card: Smart Cards, E-Payments & Law- Part I' (2002) 18(4) Computer Law & Security Report 235

O'Brien, Mark, 'Law, Privacy and Information Technology: a Sleepwalk through the Surveillance Society' (2008) 17(1) Information & Communications Technology Law 25

[26] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008)405.

[27] Caroline Hart, 'Micro-Chipping Away at Privacy: Privacy Implications Created by the New Queensland Driver Licence Proposal' (2007) 7 Queensland University of Technology Law & Justice Journal 305, 307.

[28] Privacy Committee of New South Wales, 'Smart Cards: Big Brother's Little Helpers' (The Privacy Committee of New South Wales, 1995) 25.

[29] Privacy Committee of New South Wales, 'Smart Cards: Big Brother's Little Helpers' (The Privacy Committee of New South Wales, 1995) 26.

Office, United States General Accounting, 'Electronic Government: Challenges to the Adopting of Smart Card Technology' (2003)

Quinn, Michael J, Ethics for the Information Age (3rd ed, 2009)

Reid, Alan S, 'Is Society Smart Enough to Deal with Smart Cards?' (2007) 23 Computer Law & Security Report 53

Rotenberg, Marc, 'Modern Studies in Privacy Law: Privacy and Secrecy after September 11' (2002) 86 Minnesota Law Review 1115

Shelfer, Katherine M and Procaccino, J. Drew, 'Smart Card Evolution' (2003) 45(7) Communications of the ACM 83

UNESCO, 'Ethical Implications of Emerging Technologies: A survey ' (2007)

Wales, Privacy Committee of New South, 'Smart Cards: Big Brother's Little Helpers' (The Privacy Committee of New South Wales, 1995)

Real ID Act of 2005, USC 49 §30301 Pub. L.109-13

Citation: Dr. Akram Almatarneh, *Ethics and Smart Governments: The Case of National ID Smart Card in the United Arab Emirates, ARJBM Volume 2016; pp:1-5*