



National Identity Card: The Dilemma between Social Opportunities and Threats

Khan A

Dhaka, Bangladesh

ABSTRACT

Biometric national identity card schemes are increasingly becoming common around the world and considered as an essential social component of our time. It is assumed that providing national identity cards to all the citizens will help governments to combat various social malice such as terrorism, illegal immigration, fraudulent activities, and accelerate social service delivery. Nevertheless, the introduction of national identity card has been a matter of academic and policy debate. This paper, based on a review of the literature, portrays a general overview and the current state of knowledge and understanding about the issues and concerns associated with national identity schemes. Although the use of biometric technology-based national identity schemes need not or do not face refusals, the unintended, unwelcome and unanticipated consequences on society of such a high-tech scheme must be critically considered to ensure utmost benefits to the society. It is also suggested that in order to combat or control social threats and vices, social resistance is more important than the introduction and use of high technology.

KEYWORDS: *Identify cards, Biometric, Security, Cost, Opportunity, Threat*

1. INTRODUCTION

In the wake of the influx global migration, tremendous threat of terrorism, crime and fraud, and the demand for modernisation of public services, many governments around the world are nearly unanimous in their silver bullet: identity policy (Whitley & Hosein, 2010). The basic function of a national identity system is to link a stream of data with a person (Clarke, 1994). Identification is defined as the act of identifying, the state of being identified or something that identifies one (Clarke, 1994). The verb identify is linked to the noun identity, such as in the case of the term identity card which can be used to identify someone belonging to a particular group (Micheal & Micheal, 2006).

When a governmental identification system exists, then an official identity is produced which can then be reproduced in subsequent identification processes. The state makes use of instruments for compulsory registration and identification for each one of its citizens in order to establish such an identity (Hornung & Roßnagel, 2010). Issuing National Identity (ID) cards to the citizens is a measure of such identification. Modern bureaucracy demands that all individuals of a particular society may be identified in such a manner so that they are entitled to call themselves citizens. Without identification, one cannot perform the responsibilities of citizenship such as voting, nor enjoy the benefits, such as protection against external or internal threats to well-being (Lyon, 2009). As a matter of fact, the introduction of National IDs has made a difference to the lives of the citizens across the countries, and it will continue to make a bigger imprint on their lives in future (Islam, Baniamin, & Rajib, 2012). At this backdrop, this

review captures the arguments that are in favour of introducing biometric national identity cards in one side and highlights the controversies surrounding the issue on the other side. Finally, it identifies some specific risks and pitfalls associated with national identity card schemes.

2. BACKGROUND

Governments across the world are rushing to implement national identity systems. The aims of these systems vary widely, but the many proposals involve a push to create ‘perfect identity’ that will fuse the biometric details of every person with vast central databases containing personal information (Davies, 2005). It is said that biometrics, which is literally the ‘measurement of life’ refers to the technology of measuring, analysing and processing the digital representations of unique biological data and behavioural traits such as fingerprints, eye retinas, irises, facial patterns, hand geometry and body odours. It can be used for identification purposes of the individuals (Mordini & Petrini, 2007).

Around the world, biometric technologies are on the rise enforcing an integration of biometrics into the lives of citizens. Such technologies often leave citizens with no choice but to accept biometrics (Krupp, Rathgeb & Busch, 2013). There are some specific reasons that make biometric-based identity cards or smart cards a topic of great interest which include: i) more countries are starting to use them; ii) there is strong pressure to include biometric data for anti-terrorism and police purposes; and iii) the time now has come when the capabilities of electronic chips relating to electronic identity are ready to be used such as; electronic authentication and signature (Combet, 2004). After the 9/11 event, the issue

of issuance of national identity card has largely been staged on the global platform, and several countries such as the USA, the UK, the Netherlands, France, Italy, Greece and some Eastern European countries began to consider adopting smart national ID cards (Kitiyadisai, 2004). Very specifically, dangers associated with the social security problem like terrorism, illegal immigrations and unworthy claimants of public benefits have encouraged the governments around the world to impose ID cards of their citizens (Rule, 2005).

In the UK, the bio-metric based national identity card was introduced after the enactment of 'Identity Cards Bill' for the purposes of the interests of national security; the prevention or detection of crime; the enforcement of immigration controls; the enforcement of prohibitions on unauthorised working or employment; and for securing the efficient and effective provision of public services (House of Commons, 2005). Belgium is one of the first countries in the world to implement electronic identity card scheme on a national scale with an aim to providing citizens a secured identity document, and also a brand-new digital signature and identification tool for faster and secure access to public and private services online (Gemalto, 2011). The Estonian ID card roll-out is known to be the most successful in Europe. It has been organised in public-private partnership and many applications are working with it such as; e-ticketing, drivers permit verification, health insurance, banking and digital signature and checking of bills (European Commission, 2006). Some Asian countries such as; the Philippines, Japan, Malaysia, and Thailand, have also made concrete attempts establishing an electronic smart ID card policy. For instance; the unrest in the south of Thailand and the increasing threat

of terrorism forced Thai government to go with a smart ID card scheme as a measure to counter terrorism (Kitiyadisai, 2004).

In South Asia, India has introduced the world's largest biometric-based identity scheme called 'Unique Identification' (UID) for its 1.2 billion people (Jacobsen, 2012). UID aims at giving the government a clear view of India's population, enabling the government to target and deliver services effectively, and achieving greater returns on social investments, monitor money and resource flows across the country (UIDAI, 2010 cited in Jacobsen, 2012). To fulfil ambition to become a Smart Nation, Bangladesh launched ID card programme in the nineties. Recently, such programme has been spread in a massive scale across the country. In Bangladesh, the impact of NID cards on the daily life of people are growing as the government has declared that citizens above 18 years age must acquire NID cards in order to receive 22 specific public and private services (Islam, Baniamin, & Rajib, 2012)¹. The major expected benefit of a National ID System in Bangladesh is to assist service agencies in public and private sectors to verify the identity of the service recipients in a streamlined and timely manner (Election Commission, nd).

¹In 2008 Government of Bangladesh specified through a gazette notification that NID have to be presented in case of 1) Issuance and renewal of a passport , 2) Driving license, 3) Trade license, 4) Tax identification number (TIN), 5) Bank accounts, 6) Business identification number, 7) Business bank account, 8) Beneficiary's owner account (Stock Exchanges), 9) Connection of utility services, 10) Telephone connection, 11) Mobile phone registration, 12) Internet connection, 13) Cable television connection, 14) Registration for public exams, 15) Marriage registration, 16) Loans, 17) Government Subsidies, 18) Government Allowances, 19) Buying land, 20) Selling land, 21) School admissions and 22) Lodging cases in court.

A. Khan

Despite having some concrete arguments in favour of launching identity cards at the national level, there are many controversies against each of the arguments. Some of the arguments as such have been stated below.

Potato (*Solanum tuberosum* L.) is the world's fourth-largest food crop, as it is an important staple food in the world after maize, wheat and rice (FAOSTAT, 2014). In Sri Lanka also, potato is considered as an economically important vegetable crop. Bacterial wilt caused by *R. solanacearum* is a major problem confronted by the potato farmers in Sri Lanka. It was recorded 5% to 25% loss of potato yield in Sri Lanka due to bacterial wilt (Kelaniyangoda et al, 1995). According to the Plant Protection Act No. 35 (Ministry of Agriculture, 1999), *R. solanacearum* is considered as a quarantine pest in Sri Lanka, since some of the strains of this species have not yet been reported, the existing strains also have a restricted distribution (Bandara, 1983; Kelaniyangoda, 1995) and the disease is officially controlled in the country. Introduction of the unavailable strains of *R. solanacearum* into the country may cause major outbreaks of diseases not only in potato but also in other crops in family Solanaceae and Musaceae, causing huge economic losses.

Potato is grown through vegetative propagation using potato tubers, which is also known as seed potato. Use of healthy seed potatoes is one of the most effective means to control bacterial wilt disease in potato (Hayward, 1991). Out of the annual total seed potato requirement, about 5% is produced by the Department of Agriculture; 55% is fulfilled by farmers' previous harvest; and the balance of 40% is imported by the private sector (Kelaniyangoda et al, 2004; Malathy et al, 2005; Nugaliyadde et al, 2005). Seed potato consignments imported to Sri Lanka are inspected visually for pests and

diseases at the port of entry. But the visual observation does not give a clear idea about the level of disease infection correctly. Therefore, planting of asymptomatic or latently infected tubers could lead to outbreaks of diseases at the field. Therefore, quarantine restrictions are imposed on import of seed potato, considering the danger of introducing certain pests and pathogens into the country (De Silva and Weerasinghe, 2000; Rajapakse et al, 2006).

The available conventional methods such as culture methods, biochemical assays, pathogenicity test, and biovar determination test are time consuming, labour intensive and not sensitive for the detection of *R. solanacearum* in asymptomatic potato tubers (Champoiseau et al, 2009; van Elsas et al, 2001; Priou et al, 2014). Immunodiagnostic methods such as enzyme - linked immunosorbent assay (ELISA) kits or commercially available immunestrips are used for rapid detection of *R. solanacearum*, but it cannot be used to identify sub-specific strains of *R. solanacearum* including races, biovars and phylotypes. Additionally, immunodiagnostic methods are not much sensitive to detect *R. solanacearum* in asymptomatic potato tubers (Elphinstone et al, 1996; Pradhanang et al, 2000) and sometimes give false positive results (Wullings et al, 1998; Llop et al, 1999). Polymerase chain reaction (PCR)-mediated DNA-based techniques are rapid, more sensitive and specific compared to immunodiagnostic methods and can be used for detection of ultra-low population of *R. solanacearum* in asymptomatic or latently infected potato tubers. Sensitivity has been reached to 10^2 - 10^1 cfu/mL (Llop et al, 1999; Ozakman and Schaad, 2003). The higher sensitivity of the PCR detection may be due to the amplification of living and dead cells or cells at viable – but – not - culturable (VBNC) state (Josephson et al, 1993).

3. MATERIALS AND METHOD

A comprehensive data collection has been conducted from wide range of literature published by various authors. Collected data made concise to analyse social opportunities and threats.

4. RESULTS & DISCUSSION

National identity cards of all sorts are controversial. The implementation of ID cards has raised resistance and objections in various countries (Kitiyadisai, 2004). Many of the arguments articulated in relation to national ID card schemes involve claims regarding the advantages and disadvantages of large-scale databases, connecting multiple databases and incorporating millions of people (Neyland, 2009). While the governments have drawn together a justificatory schema involving press releases, reports and claims for support from a variety of groups all designed to position the ID card as reasonable, feasible and necessary, anti-ID card groups have drawn together a similar coalition in opposition (Neyland, 2009). In the USA, the UK, Canada and Australia the proposals for introducing national ID cards and registry systems had raised serious debate with regard to control and privacy issues (Fussell, 2004). Interestingly, many ID proposals around the world are running aground because they have failed to win the trust of citizens. In their haste to implement powerful new identification and tracking technologies, governments are quickly discovering that civil liberties and privacy campaigners are finding a new and popular voice (Davies, 2005). Specifically, opposition to ID cards and their technical infrastructure typically emerges on both practical and principled levels. On a practical level, security, cost, efficiency, and effectiveness inform arguments against a card-

based identity system. The stated benefits of these cards are actually misleading. Critiques based on principle draw upon a civil liberties frame, highlighting how card-based identity systems facilitate increased state surveillance and act as a breach to constitutional or moral dignities by penetrating into the realm of civil liberty (Milberry,& Parsons, 2013).

There are many less-than-obvious risks and pitfalls concerning the use and misuse of national identity cards, and also some genuine problems with biometric registrations. For example; the assessment of London School of Economics, UK warns that biometric registration may have to be repeated every five years for much of the population. As people become aged, their biometrics change and become less reliable, and as a result of that, these people tend to face problems with the use of their cards. Hence, continuous updating of biometric information is needed (LSE, 2005).

Some other discrete problems can appear out of biometric-based smart card technology system such as; i) the recordability of fingerprints can be temporarily limited by injuries to fingertips or broken fingers and through dirty fingertips. A permanent loss of a fingerprint template could occur as a result of fingertips being burned or scarred. Intensive manual work or working with toxic agents can also destroy the fingerprint template; ii) the recordability of the face can be temporarily lost after major facial surgery; and iii) the recordability of the iris template can be temporarily impaired due to the dilation of the iris as a consequence of the taking of certain medicines. Permanent losses of recordability may occur as a consequence of eye diseases e.g., blindness, cataracts or glaucoma. In addition, enrolment is often made more difficult by drooping or narrow eyelids, which partially

A. Khan

cover the iris (Petermann, Sauter, & Scherz, 2007). These problems might result in a person not being enrolled in an identity system and also in denial of access to services-potentially disastrous for the individual concerned (Davies, 2006).

Probably the vulnerability with the greatest threat to smart ID card schemes is human error. This is amply illustrated by the chaotic handling of all kinds of personal and sensitive data by various government agencies. For example, such problem has been badly proved by the mishandling performance of the UK Government agencies. Human error can take place at any stage where humans interact with the scheme. During the enrolment processing, data can be incorrectly entered leading to confusion once the identity card has been issued. Likewise, during enrolment, biometrics can be poorly captured leading to a higher level of false rejects (Arora, 2008).

On the other hand, the implementation of smart national identity cards needs a huge financial involvement. For example; in the case of UK, LSE's (2005) report estimates between 10.6 billion pound and 19.2 billion pounds for a ten year rolling excluding public and private sector integration costs and possible overrun costs. The report further estimates that costs are also to be incurred for imparting training to the staff, establishing new facilities, buying expensive biometric equipment and updating biometric information. In this regard, NO2ID (nd) estimates that additional tax burden of setting up the scheme in the UK is around 200 pound. So, there remains a question whether citizens are ready to accept such additional cost in the form of increased tax. Besides, the consequences of losing one's card could potentially be a more serious problem and it can

negatively affect virtually every aspect in a person's daily routine (Smith, 2008), and such loss may be financially very disastrous.

In regard to personal liberty civil rights groups say that smart ID cards could easily violate personal privacy and deprive one of one's liberties. They are especially more concerned about corrupt or unauthorised government officials who could use personal data to manipulate and control people (The Nation, 18 April 2004, cited in Kitiyadisai, 2004). In reality, ID cards pose many risks to personal liberty which include: i) risks from the legal use of accurate information; ii) risk of reliance on false information; iii) risk of intentional creation of false information; iv) risks from illegal use of accurate information; v) risk of over-dependence on some feature of the system (Froomkin, 2008).

Smart identity card scheme invites social, economic and digital divides in society (Kitiyadisai, 2004), and it might lead to the formation of an unhealthy social system and can act as a breach of human rights. In the context of Thailand, Kitiyadisai (2004) notes that the smart ID cards would put marginalised and minority groups such as; hill tribe people, immigrant workers, illegal foreign workers, homeless people, refugees, and illiterate citizens at the other end of the social spectrum, making it harder for them to have access to social services and creating more difficulties in proving their entitlements and identities.

One of the strong arguments for many countries for going with smart identity card scheme is to shield against identity fraud. In fact, service providers need to ascertain one's identity to prevent fraud and harm. But the belief that smart NID cards could provide irrefutable

biometric matches without false positives and negatives is fallacious. Also, such systems can still be cracked, and the criminals and terrorists will find ample of ways to exploit them (Neumann & Weinstein, 2001). No security on any database can be guaranteed, particularly one that contains such amount of information which are likely to be accessed millions of time every day and data that changed on thousands of individuals every day. Captivatingly, nominally “secure”, trusted ID is more useful to a fraudster (NO2ID, nd). As with any large-scale IT implementation risks are omnipresent. National ID cards are just as vulnerable to attack as any other IT system especially when one considers smart ID cards and their respective infrastructure as a form of critical national infrastructure (Arora, 2008).

5. CONCLUSION

The benefits brought by the National ID system are yet to be fully proved and this system is inextricably allied with many risks and shortcomings. Without considering the probable risks and shortcomings, the introduction of National Identity Card on a large scale will only invite a lot of unintended, unwelcome and unanticipated consequences. Policymakers should make a careful assessment of those consequences, and should not be subjugated to the stereotyped notion “Others are doing, why not we”? Developing countries should seriously consider whether they have the luxury to go with such an intervention. These countries have many important responsibilities to accomplish for their citizens other than the mere introduction of the national ID card. In particular, social vices should be tackled by social measures, relying on ID card to tackle social vices might not be a very effective

solution. Technology is often least powerful to social forces. At the same time, social acceptance/non-acceptance towards biometric recognition, benefits and threats must be critically assessed before giving high importance or obligation to a particular policy issue like compulsory biometric scrutiny of the citizens for having national identity cards. Citizens must be given the right to say either ‘No’ or ‘Yes’ to sharing their personal information. The risks of identity fraud are common, and any personal damage caused by identity fraud cannot be reversed so easily. Over-collection of data not only increases the risks of leaks but also makes efforts more difficult to reverse.

REFERENCE

- ARORA S. National e-ID card schemes: A European overview, *Information Security Technical Review*. 2008; 13: 46-53.
- CLARKE R. Human Identification in Information Systems: Management Challenges and Public Policy Issues, *Information Technology & People*. 1994; 7 (4): 6-37.
- COMBET E. The Key to ID Cards: ‘Identity Card Usages’, not ‘Identity Usages’, Oxford International Institute. *Internet Issue Brief*. 2004; No 3.1.
- DAVIES S. The Complete ID Premier, *Index on Censorship*. 2005; 34: 38-43.
- DAVIES S. A Case of Mistaken identity, *Significance*, September. 2006; 114-117.
- EUROPEAN COMMISSION. eID in Estonia, <http://www.epractice.eu/files/documents/>

A. Khan

- cases/191-1170255573.pdf. Accessed 01 May 2018.
- ELECTION COMMISSION (nd.). NID Service Fund. <http://www.nidw.gov.bd/>. Accessed 01 May 2018.
- FOORMKIN M, CHANDER A, GELMAN M & RADIN MJ. The Uneasy Case for National ID Cards: Securing Privacy in the Internet Age, Stanford: Stanford University Press. 2008; pp: 295-324.
- FUSSELL G, WATNERAND C & MCELORY W. Genocide and Group Classification on National ID Cards. National Identification Systems: Essays in Opposition, Jefferson: McFarland & Company Inc. Publishers. 2004; pp.55-69.
- GEMALTO. The Identity Card Program in Belgium: The Keystone of e-Government. http://www.gemalto.com/brochures/download/gov_belgium_id.pdf. Accessed 01 May 2018.
- HOME OF COMMONS. Identity Cards Bill. <http://www.publications.parliament.uk/pa/cm200506/cmbills/009/2006009.pdf>. Accessed 01 May 2017.
- HORNUNG G. RONAGEL A. An ID card for the Internet – The New German ID Card with Electronic Proof of Identity, Computer, Law & Security Review. 2010; 26 (2): 151-157.
- ISLAM MR, BANIAMIN HM & RAJIB MSU. Institutional Mechanism of National Identification Card: Bangladesh Experience, Public Policy and Administration Research. 2012; (2): 1-13.
- JACKSON M. & LIGERTWOOD J. Identity Management: Is an Identity Card the Solution for Australia? Prometheus. 2006; 24 (4): 379-387.
- JACOBSEN EKV. Unique Identification: Inclusion and Surveillance in the Indian Biometric Assemblage, Security Dialogue. 2012; 43(5): 457-474.
- KITIYADISAI K. Manusya: Journal of Humanities, Special Issue. 2004; 8: 37-45.
- KRUPP A, RATHGEB C & BUSCH C Social Acceptance Of Biometric Technologies In Germany: A Survey. Proceeding Of 2013 International Conference Of The Biosig Special Interest Group (BIOSIG), Darmstadt, Germany . 2013; PP 193-200.
- LSE. The Identity Project: An Assessment of the UK Identity Cards Bills and Its Implications. London School of Economic. The Department of Information Systems. 2005; Version 01: 09.
- LYON D. Identifying Citizens: ID Cards as Surveillance. Cambridge: Polity Press. 2009.
- MICHEAL K & MICHEAL MG. Historical Lessons on ID Technology and the Consequences of an Unchecked Trajectory, Prometheus. 2006; 24(4): 365-377.
- MILBERRY K & PARSONS C. A National ID Card by Stealth? The BC Services Card Privacy Risks, Opportunities and Alternatives. British Columbia Civil Liberties Association. <http://www.christopher-parsons.com/Main/wp-content/uploads/2013/11/2013-National-ID-Card-by-Stealth.pdf>. Accessed 02 May 2018.

- MORDINI E & PETRINI C. Ethical and Social Implications of Biometric Identification Technology. *Ann Ist Super Sanita*. 2007; 43 (1): 5–11.
- NEUMANN P & WEINSTEIN L. Risks of National Identity Cards, *Communications of the ACM*, 2001; 44 (12): 176.
- NEYLAND D. Who's Who? The Biometric Future and the Politics of Identity, *European Journal of Criminology*. 2006; 6 (2): 135-155.
- NO2ID (nd). NO2ID Summary Briefing. <http://www.no2id.net/IDSchemes/NO2IDSummaryBriefingMay2005.pdf>. Accessed 02 May 2018.
- PETERMANN T, SAUTER A & SCHERZ C. Biometrics at the Borders—the Challenges of a Political Technology, *International Review of Law Computers & Technology*. 2006; 20 (1&2): 149–166.
- RULE JB. Time to Ask Questions about the Paths Opened by ID Cards, *Oxford Internet Institute, Internet Issue*. 2005; Brief No. 3.2.
- SMITH AD. The Benefits and Risks of National Identification Programme. <http://www.emeraldgroupublishing.com/learning/managementthinking/articles/pdf/nationalid.pdf>. Accessed 02 May 2018.
- WARREN A & MAVROUDI E. Managing Surveillance? The Impact of Biometric Residence Permits on UK Migrants, *Journal of Ethnic and Migration Studies*. 2011; 37 (9): 1495-1511.
- WHIETY E A HOSEIN G. Global Identity Policies and Technology: Do We Understand the Question? *Global Policy*. 2010; 1 (2): 209-215.