



December 2005

PI-07-05

National Identification System: Do We Need One?

Introduction

Running a government is no easy task. Law enforcement, service delivery and social security benefits avilment entail voluminous documents that have compelled states to devise tools that simplify and manage these tasks. One such device is the establishment of a national identification (ID) system.

In the Philippines, several proposals though varied in scope and coverage, seeking to implement a national identification system have been filed in the Senate and in the House of Representatives. Recently, President Gloria Macapagal-Arroyo signed Executive Order 420 that requires all government agencies and government-owned and-controlled corporations to harmonize and streamline their identification systems. According to the EO, the purpose is to curb red tape in public transactions and attain efficiency in government operations.

As seemingly noble a goal as cutting red tape, a proposal to institute an ID system is a contentious issue. In the Philippines and elsewhere, civil libertarians, human rights advocates and militant groups have long claimed that an ID system violates a citizen's intrinsic right to privacy and could very easily be used by the government to keep track of a citizen's personal activities. In other words, it is a program that

strikes at the heart of a citizen's relationship with the state and has profound consequences for social order.

Amidst all the rhetoric, it is best to analyze the arguments presented by each side to lend clarity to each claim. This paper discusses the changing rationale for an ID system. It also provides an account of policy issues and problems in laying the groundwork for an ID system, by examining the views of those who support and oppose such a proposal. A brief account of the United States' experience is also provided. Finally, the paper argues that the government must not throw caution to the wind in putting up an ID system. The cost, policy and legal environment must be adequately studied so as to protect the citizens that it wants to serve.

The National Identification System and its Changing Rationale

In broad terms, a national identification (ID) system is a mechanism used by governments to assist public agencies in identifying and verifying the identities of citizens who are availing of government services or making public transactions. Usually, the citizen is assigned an identification number at birth or when he or she reaches legal age. Depending on the purpose for which the ID system was built, some countries include not only their citizens but also foreign

nationals who have become permanent residents.

Privacy International, a non-profit organization that advocates civil liberties, categorizes three types of ID systems (see Table 1).

Table 1. Types of National Identification Systems

| TYPE | DESCRIPTION |
|---------------------|--|
| Stand Alone | ID cards that are usually issued by governments undergoing political transitions such as military or emergency rule. |
| Registration System | The ID card contains information that is stored in a registration system managed by a government agency. |
| Integrated System | A card number is usually assigned to an individual as a form of identifier. Several government agencies are part of the integrated system. |

Source: Privacy International. *Identity Cards Frequently Asked Questions*. August 24, 1996

In countries that have stand-alone ID systems, citizens are required to present IDs to authorities as a form of an internal passport (Privacy International, 1996). Because of the information technology revolution that allows sharing of huge volumes of information among computer networks, it is the integrated systems that have become popular in recent years. As there are several agencies that are part of the system, the card holder can make several public and private transactions. For its part, the government issuing the card can use it for different purposes such as efficient public transaction and border control.

Group Classification

The concept of a national identification system was first instituted in countries with populations coming from diverse ethnic groups. The idea was to use the ID as a means of identifying people of a certain race, politics or religion. In the long run however, this mode of classification was used by oppressive regimes to discriminate against certain ethnicities or religion (Privacy International, 1996:2). It is for this reason that ID systems have long been resisted by human rights advocates mainly because some governments use it to identify particular groups for ethnic cleansing or genocide. For instance,

ID systems are said to have been used extensively in the Nazi regime and in Rwanda to carry out various crimes against humanity (Fussell, 2001).

Control of Illegal Migration

When illegal immigration became a huge concern for the United States, Australia and Europe in the 1990s, the use of ID systems to curb the onslaught of illegal immigrants was explored. The plan was to put up a national registry system which could be used by employers to verify the identity of a prospective employee through his/her national ID (Miller and Moore, 1995). These proposals were archived because they met stiff opposition from civil libertarians both within and outside the government.

Tax Evasion and Welfare Fraud

In Australia and New Zealand for example, plans for an ID system that were aimed to curb tax evasion and welfare fraud were pushed in the 1980s and 1990s. Proponents believed that it will expand the tax base and weaken the black market economy. However, the proposals were scuttled by campaigns launched by groups such as the Australian Privacy Foundation which fought the planned ID system on privacy issues (Scheeres, 2001).

Identification Purposes

At present, several countries, rich and poor alike, are implementing a national ID system (see Table 2). However, the type of card, its purpose

Table 2. Selected Countries With National Identification Cards

| | | | |
|---------|-----------|------------|-----------|
| Germany | Honduras | Luxembourg | Poland |
| France | Guatemala | Portugal | Chile |
| Belgium | Kenya | Spain | Malaysia |
| Greece | Brazil | Italy | Pakistan |
| | | | Argentina |
| | | | Singapore |

Source: Tova Andrea Wang, "The Debate Over a National Identification Card," *The Century Foundation Issue Brief* (no date provided)

and the information it contains vary from country to country.

For most countries, the data contained in the ID cards are similar to information contained in credit cards or any employee ID. The amount of data contained in the cards depends on the purpose/s for which it is supposed to be used. Some use ID cards as part of employment requirements such as in Kenya and in Spain. In Belgium, the ID is used by citizens as proof of age when purchasing liquor and going to “for adults-only” places (Wang, undated).

In the Philippines, the idea of a national identification system was first brought up in the martial law years (OSETC Digest, 2005). The idea of Presidential Decree 278 was also to harmonize all government-issued identification systems into one national reference card. The decree covered Filipino citizens as well as foreign nationals. Since then, Philippine presidents except Cory Aquino have issued statutes with similar aims (see Table 3). President Ramos’ ID

system was stymied by a Supreme Court ruling nullifying the administrative order because it encroached on Congress’ right to legislate.

E-Governance

As information technology gained headway, governments saw the possibilities of e-governance in harnessing efficiency. IDs were linked with national registration systems and were no longer used only for identification, but also for the enhancement of public service delivery (Privacy International, 1996:3). Hence, countries that have long ago used ID cards are updating their systems into what has come to be called “smart cards” in line with newly-developed technologies. Smart cards are called as such because they contain a person’s biometrics stored in computer chips and combine several public and private transactions.

Among countries in Asia, the most ambitious is Malaysia. While its rationale for updating its card is to provide efficient public service delivery and protect against terrorism, the Malaysian government clearly takes pride in the fact that its ID card is touted as the most technologically advanced in the world. Dubbed as the “Mykad,” it combines “eight or nine commercial transactions on a single card and including driver’s license, health insurance, toll payment and ATM cash withdrawal” (CardTechnology,2005). At the same time, similar plans are in the pipeline in China, India, Thailand and the Persian Gulf States (ibid.).

Fighting Terrorism

In the aftermath of September 11, states scrambled to revise and update their internal security policies so as to cope with the changing security framework. Because the perpetrators were non-state actors and non-combatants, states realized that new measures must be employed to counter the dangers posed by terrorism. ‘Homeland defense’ as opposed to ‘national defense’ is now the name of the game.

Table 3. Presidential Statutes on National Identification System and Their Rationale

| Presidential Statute | President | Rationale |
|---|------------------|---|
| <i>Presidential Decree No. 278 - Instituting a National Reference Card System and Creating Therefor The National Registration Coordinating Committee</i> | Marcos | To ensure national security and convenience in the transaction of official business with government and private offices and agencies |
| <i>Administrative Order No. 308 - Adoption Of A National Computerized Identification System</i> | Ramos | To facilitate transactions with basic services and social security providers and other government instrumentalities |
| <i>Executive Order No. 420 – Requiring All Government Agencies And Government-Owned and Controlled Corporations To Streamline And Harmonize Their Identification (ID) Systems, And Authorizing For Such Purpose The Director-General, National Economic and Development Authority To Implement The Same, And For Other Purposes</i> | Macapagal-Arroyo | To reduce government red tape and enhance the integrity and reliability of government-issued identification cards in private transactions |

The United States' Experience

Interestingly, the most recent addition to countries that are implementing ID systems is the United States. For so long, according to the Electronic Privacy Information Center, efforts to install an ID system in the US have been staunchly opposed by privacy groups. In fact, moves to expand the use of the Social Security Number was consistently rejected in the 1970s and 80s. The Social Security Number (SSN) which was established in 1936 was created specifically to serve as a nine-digit account number to facilitate the implementation of the Social Security System. It is used to monitor benefits availability and the contribution of individual members of the US Social Security Administration.

In the succeeding years of its implementation, the government found other purposes for the SSN. For instance, in 1961 the Civil Service Commission started to use Social Security numbers to identify all federal employees. In 1962 the Internal Revenue Service started requiring taxpayers' Social Security numbers to appear on all completed tax returns. The Social Security Administration (SSA) disclosed Social Security numbers to the private sector until public outrage halted the practice in 1989.

The advent of the information technology revolution paved the way for the many uses of the Social Security number. According to a 1995 study by the Cato Institute, despite a provision in the 1974 Privacy Act prohibiting other uses of the number without congressional approval, the number is now required in availing of insurance, employment and drivers' licenses that it has technically become a sort of a 'national identifier' (Miller and Moore, 1995). During the Clinton administration, a 'health security card' was proposed but was also shelved even if the government assured "full protection for privacy and confidentiality."

However, in the wake of September 11, there was a growing consensus in the US that the security environment has changed. In fact the survey group Pew Research Center showed that the ID system has gained the support of majority of Americans (Jones, 2001). Nonetheless, for them, surveillance of phone calls and e-mails still remains a ticklish issue. Likewise, The Oracle Chair, days after the 911 incidents, urged the US government to install an ID system and offered his company's software services free of charge. But even then, the Bush administration, at least in public, was opposed to an ID system (ibid.).

Meanwhile, the USA Patriot Act of 2001, an anti-terrorism measure approved by the US Congress in the aftermath of September 11, sought for the development of biometric technology that can scan visa applicants. It was in May 2005 that a 'de-facto ID system' was signed into law by President Bush. The REAL ID Act mandates the creation of an 'electronically readable' and 'federally approved card' to people living and working in the US. Under the law, people living and working in the US will have to apply, through their state motor vehicle agency, for an 'electronically readable' and 'federally approved' ID card, which in effect replaces the old driver's license. In essence, it aims to re-issue the driver's license according to the standards of the Department of Homeland Security, a federal agency. Data to be contained in the card include name, birth date, sex, ID number, digital photograph, address. The Department of Homeland Security is allowed under the measure to add other features of the ID such as retinal scan or fingerprints. Mechanisms to prevent fraud and tampering will be inputted in the card.

What makes the ID unique from the previous driver's license is its standardization. At present, state driver's licenses in the US vary from state to state. Some states employ bar codes while others have magnetic strips. Some do not have both. This discourages enterprises such as banks and airlines from using this in their client transactions since this will not contribute to efficiency. However, with a uniform ID, Barry Steinhardt, director of the American Civil Liberties Union's technology and liberty program, says: "It's going to result in everyone, from the 7-Eleven store to the bank and airlines, demanding to see the ID card. They're going to scan it in. They're going to have all the data on it from the front of the card...It's going to be not just a national ID card but a national database." The US government will implement the measure in 2008.

A briefing paper issued by a US private think-tank argues that had there been an ID system in place in the United States, the September 11 terrorists, some of whom lived in the US and were on government watchlist, would have been caught had they tried to board a plane or purchase anything using their credit cards. An ID system would have meant that a computer chip embedded in the ID card could have easily identified anybody who is on a government watchlist (Wang, undated).

Today, as global terrorism remains on the rise, governments of the United Kingdom and the United States have revived proposals to put up a national ID system even in the midst of stiff opposition from various interest groups. In May, US President George Bush signed into law what is tantamount to a national ID program.

In the United Kingdom there is extreme pressure to shelve legislation for an ID system. The London School of Economics and Political Science, which was commissioned by the UK government to conduct a study on its Home Office Identity Card proposal, came out with a report urging the government to abandon the proposal. It argued that an ID system runs the risk of “failure of systems, unforeseen financial costs, increased security threats and unacceptable imposition on citizens” (LSE, 2005).

Issues and Problems: The Debate

A host of issues and concerns relative to the implementation of an ID system makes it a contentious measure. The following are some of the issues raised and the debate between those who support its implementation and those who are against it.

Human Rights and Privacy Issue

Civil libertarians and human rights activists reject the idea of a national ID card based on three reasons: “functionality creep,” the potential for misuse due to identity fraud, and the privacy

issue. The common denominator that runs through these arguments is the extent through which the government would hold power vis-à-vis its citizens.

According to human rights activists, an ID system can be a double-edged sword because it can suffer from “functionality creep” which means it can serve purposes other than its original intent. Thus, even if the original rationale for an ID system is simply to cut government red tape, a government may eventually use it as a mechanism for repression against political opponents or to discriminate on the basis of race or ethnicity. For instance, as mentioned earlier, the Rwanda genocide in 1995 was facilitated by the use of ID cards. Newspaper reports recounted that Rwandans who presented ID cards bearing a Tutsi identification were hacked to death by the Hutu militia.

While supporters claim that ID systems can be legislated to specifically state the purpose of its implementation, critics believe that this is not a guarantee. The context or political environment within which ID systems are implemented is not static, hence the potential for abuse is very great.

The advent of biometrics and microchips technology also has profound implications. Critics argue that the potential for abuse and invasion of privacy is even greater with the use of biometrics since it is vulnerable to identity fraud. The citizen is no longer in control of his personal information. For instance, the research claims that “facial recognition and iris scanning can sometimes be defeated by presenting a picture of someone else’s face or iris” (CRS,2005). Activists on the other hand, are more concerned with information security such as “unauthorized changes to or disclosure of biometric data stored in a central database or on an identity document” (ibid.).

Proponents of ID systems on the other hand contend that the use of a Personal Identification Number (PIN) such as that found in automatic

teller machines enhances data security and enables citizens to have control of the data they wish to reveal. In addition, they claim that identity fraud and disclosure can be prevented by investing in technology that will ensure the integrity of the system and minimize the potential for misuse. They also argue that laws can be enacted that can establish the rules on access, data storage and disclosure pertaining to the national database.

Aside from the issue of misuse, ID system opponents believe that the idea of a government tracking the activities of its citizens violates a citizen's intrinsic right to privacy. They say that a government intruding in the affairs of citizens is dangerous and has dire consequences for social order. Moreover, the extent of personal information that will be collected by the government and whether it really serves a legitimate aim is a cause of alarm to rights activists. Supporters of an ID system, on the other hand, contend that people who do not violate laws have nothing to hide and should therefore have no reason to fear a government monitoring their activities.

Crime Prevention

ID system advocates hail its benefits in combating terrorism, illegal immigration, crime and tax fraud. Because of the technology and data-driven nature of today's society, a national ID system could easily track offenders. ID supporters claim that the notion that citizens are being observed will enhance public order and as such decrease opportunities for crime (LSE, 2005). However, opponents belie this claim. The London School of Economics study on the viability of the proposed ID system in the United Kingdom points out that the police in developed countries believe that the lack of identification procedures does not pose a problem in investigation. It is evidence gathering and prosecution that remain as big obstacles for the resolution of crimes. Nonetheless, using crime trends across Europe

from 1995-1999(see Table 3), the LSE observed that there are fewer crimes in countries without ID cards (LSE, 2005:36). However, it argues that it is hard to conclude from the data if ID systems do affect crime trends.

Table 3. Crime Recorded by Police in EU Countries, 1995 – 1999

| Country | Recorded Crime % change | Drug-Trafficking % change | Homicides Avg 97-99, /100,000 | Terrorist Incidents ⁷⁵ 1968-2005 | ID Cards NC: not compulsory C: compulsory |
|-----------------------|-------------------------|---------------------------|-------------------------------|---|---|
| Eire | - 21 | +139 | 1.35 | 26 | No Cards |
| England ⁷⁶ | - 10 | - 6 | 1.45 | 165 uk ⁷⁷ | No Cards |
| Scotland | - 8 | + 9 | 2.10 | Uk | No Cards |
| Denmark | - 8 | - 56 | 1.20 | 28 | No Cards |
| Luxembourg | - 5 | + 23 | 0.83 | 5 | ID NC |
| Germany | - 5 | + 33 | 1.22 | 458 | ID C |
| France | - 3 | + 29 | 1.63 | 1027 | ID NC |
| Finland | - 2 | + 29 | 2.55 | 1 | ID NC |
| Spain | + 1 | - 12 | 2.60 | 1218 | ID C |
| Austria | + 1 | + 40 | 0.84 | 64 | ID NC |
| Sweden | + 2 | - 32 | 1.94 | 40 | ID NC |
| Netherlands | + 2 | + 119 | 1.66 | 77 | ID NC |
| Italy | + 5 | + 18 | 1.56 | 405 | ID NC |
| Portugal | +11 | - 9 | 1.39 | 51 | ID NC |
| Greece | + 14 | + 128 | 1.69 | 593 | ID C |
| Belgium | +18 | + 45 | 1.75 | 119 | ID C |

London School of Economics and Political Science. The Identity Project. An Assessment of the UK Identity Cards Bill and Its Implications. Interim Report. London, March 2005, p.36

In the Philippines as in other countries, the use of Tax Identification Numbers (TINs) as de facto national ID cards has been proposed to curb tax evasion and fraud (Baviera and Mendoza). According to the proponents, this could be used as a base for an integrated ID system. However, it has been argued that causes of tax evasion are often deeply rooted in human and organizational issues that technology may not be entirely capable of solving (Privacy International, 1996) such as non-declaration of true assets. Hence, although it may expand the tax base in such a way that it will cover the "underground economy," the presence of an ID system will not entirely solve the many persistent ills of the country's tax system.

As mentioned above, terrorism has been used as an overarching reason for the recent revival of ID proposals in several countries. In 2004, Privacy International showed that of the 25 countries that were affected by terrorism since 1986, 80 percent have identity cards, a third of which employ biometrics (see Table 4).

Table 4. Number of Terrorist Attacks and the Presence of Identity Card Systems in Selected Countries, 2004

| Country | No. of Attacks | Deaths | ID Card | Biometric |
|---------------|----------------|--------|---------|-----------|
| Afghanistan | 4 | 34 | Yes | No |
| Algeria | 41 | 280 | YES | No |
| Argentina | 2 | 129 | Yes | No |
| Bangladesh | 5 | 49 | Yes | No |
| Cambodia | 8 | 37 | Yes | Yes |
| Colombia | 90 | 400 | Yes | No |
| Egypt | 22 | 115 | Yes | Yes |
| France | 31 | 37 | Yes | No |
| India | 46 | 520 | No | No |
| Indonesia | 14 | 250 | Yes | No |
| Israel | 227 | - | Yes | Yes |
| Kenya | 3 | 267 | Yes | No |
| Morocco | - | - | Yes | No |
| Nigeria | 2 | 171 | Yes | Yes |
| Pakistan | 68 | 420 | Yes | Yes |
| Palestine | 240 | - | Yes | No |
| Peru | 31 | 40 | Yes | Yes |
| Philippines | 38 | 113 | No | No |
| Russia | 32 | 620 | Yes | Yes |
| Saudi Arabia | 10 | 30 | No | No |
| Spain | 51 | 250 | Yes | Yes |
| Sri Lanka | 27 | 440 | Yes | No |
| Turkey | 57 | 85 | Yes | No |
| Uganda | 12 | 42 | No | No |
| United States | 13 | 3650 | No | No |

Source: Privacy International: "Mistaken Identity; Exploring the Relationship Between National Identity Cards and the Prevention of Terrorism" (April 2004)

However, no correlation was established between ID cards and the prevention of terrorism. In the same vein, it is safe to assume that if the coverage of ID cards is confined to citizens of a particular country, then it will not deter foreign nationals from committing terroristic activities.

Technology Environment: The Use of Biometrics

The rapid advancement in information technology in the past decade has spawned a new generation of ID systems that are vastly different from its predecessors. The introduction of biometric ID systems is a case in point.

Biometrics is a state of the art technology that uses physical characteristics of persons as a means of identification.

Developed and used only in the last fifteen years, biometrics has been used for three purposes: for identity verification, identity discovery and identity exclusion (CRS, 2005: 2). Unlike traditional identification cards with photographs of the bearer, biometrics uses the physical characteristics of a person such as retina, fingerprint or voice.

Biometric technology is not without its limitations. Aside from the staggering cost, there are conditions that can affect its implementation. Specifically, some human features used in biometrics change as people age (LSE, 2005). It also cannot be used by individuals who lack relevant body parts or which have been damaged by disease or accidents such as those with failing eyesights (CRS, 2005). It can also fail in two ways: a false positive and a false negative (ibid.). False negative occurs when an ID system scanner yields a negative result in matching the identity of the person and his biometrics when in fact there is a real match. Thus, if this happens in criminal investigations, the real perpetrator

Table 5. Leading Biometric Technologies and Their Description

| Biometric Technology | Description |
|-------------------------|--|
| Facial Recognition | Analyzes features such as the eye sockets, cheekbones, and sides of the mouth |
| Fingerprint Recognition | Based on the pattern of ridges on the fingertips |
| Hand Geometry | Based on the dimensions of the fingers, joints, and knuckles |
| Iris Recognition | Analyzes the visible patterns in the colored iris of the eye |
| Retina Recognition | Captures and analyzes the patterns of blood vessels on the thin nerve on the back of the eyeball |
| Signature Recognition | Authenticates identity by measuring handwritten signatures |
| Speaker Recognition | Uses differences in peoples' voices from a combination of physiological differences in the shape of vocal tracts and learned speaking habits |

Sources: United States' General Accounting Office (GAO) United States' Congressional Research Service (CRS)

may go scot-free if authorities purely rely on the scanner's findings. False positive occurs when a person's biometrics incorrectly matches those of another person's. This usually results in the person's being wrongly accused of committing crimes. For their part, ID system supporters believe that this can be minimized by applying more stringent procedures in matching.

Cost Estimates

The huge cost entailed in implementing an ID system is the usual constraint faced by countries, especially those from the developing world such as the Philippines. It is estimated that implementing an ID system in the Philippines would cost P1.6 billion, according to computations by the Office of Representative Teddy Casiño. However, this is a conservative estimate considering that the proposal covers only the labor force. Moreover, the estimate covers only the cost of the ID and does not include the administrative costs such as the maintenance of the database, cost of registration, and the funds necessary to fix the unconsolidated databases of government employees (World Bank et al., 2003). Some proposals in the Senate offer conservative budgetary allocation for an ID system ranging from P20 million to P500 million. Even the cost of implementing EO 420 is not clear. What it says is that the budget will be sourced from budgets of participating agencies.

Ensuring effective implementation and the integrity of an ID system will require huge costs. The government should have a firm cost estimate for this project if it is bent on making an ID system work. Based on other country experiences, the cost can be prohibitive for a cash-strapped government. In the United States alone, the cost estimate of their ID system is about \$17.4 billion within its ten-year phased implementation (French, 2005). Ultimately, the cost of an ID system depends on the level of technology, the coverage and system specifications.

Administrative Efficiency

The most commonly used reason for having a national ID system is that it reduces government red tape and makes the delivery of public services more efficient. An ID system is particularly useful in public transactions involving a huge segment of the population such as voting and benefits availment. Studies however argue that an ID system may in fact disenfranchise a significant segment of the population. According to Demos, a public interest group in the US, a state law requiring voter identification based on driver's license in Indiana, Georgia and Arizona resulted in the disenfranchisement of people who do not possess motor vehicles or do not drive such as the disabled and the elderly. It is also difficult to see how an ID system can minimize fraud in voting and social security benefits availment if the endemic problems of the bureaucracy (overlapping of functions, lack of careerism, etc.) are unresolved. Interestingly, New Zealand, the country that is regarded as having one of the most efficient bureaucracies in the world, has no ID system in place.

Legal and Policy Environment

Aside from budgetary issues, the legal and policy environment must be adequately prepared to implement an ID system. In the Philippines the 1987 Constitution's concept of privacy leans more on the citizen's right to privacy in one's abode than privacy of one's personal information. The only laws that can be cited that somehow protects citizens against government intrusion in one's affairs are the decades-old Bank Secrecy and Anti-Wiretapping laws. Hence, should the government proceed with the planned ID system, Congress should pass a Privacy Law similar to that in the United States and a Data Protection Act such as in the United Kingdom to protect citizens rights over their personal information.

Other Issues

Meanwhile, the level of computerization in most Philippine government agencies is low. This can be gleaned from a recent study by the National Computer Center (NCC) on the use of information technology in government agencies. The study showed that as of 2003, 50 percent of national government agencies still use dial-up connections. Others still use outdated software. Moreover, only 14 percent of government offices use Pentium 4 computers. The study also showed that networking among government agencies is still not prevalent (NCC, 2003). As such, it is unimaginable how a proposed ID system which presupposes huge investments in information technology can even be thought of at this time.

Moreover, according to the National Statistics Office (NSO), ten percent of Filipino children are unregistered or do not possess birth certificates. This is a perennial problem that can pose a big constraint to a planned ID system as this would marginalize millions of Filipinos. The implications of the proposal to the welfare of indigenous people who often lack identification should also be looked into.

CONCLUSION

Clearly, a proposed ID system has its share of advantages as well as disadvantages. However, as the paper has shown, it is not a panacea to the ills that hound the country. Efforts to curb criminality should still be focused on huge budgetary investments in the training, values education and capacity-building of the police. This should be complemented by resolving the perennial problems in the other pillars of the justice system.

Administrative efficiency or success in decreasing incidence of tax evasion and red tape on the other hand, can only be achieved if the government makes significant strides in instituting in the bureaucracy the central tenets of good governance: transparency, predictability, participation and accountability.

The staggering cost is also a major concern not just for developing countries such as the Philippines but also for rich ones such as the United States and the United Kingdom. A more realistic cost estimate is imperative if the government is bent on making the ID system work. It must be based on the system specification, the information and the level of technology of the proposed ID system.

Ultimately, the viability of an ID system rests on a question that has hounded mankind since the time it founded the institution of government as the basis of social order: To what extent should a citizen allow the government to interfere with private affairs in exchange for his security?

References:

Reports and Analyses

Cato Institute. Cato Policy Analysis No. 237 September 7, 1995. "A National ID System: Big Brother's Solution to Illegal Immigration" by John J. Miller and Stephen Moore.

Congressional Research Service (CRS) Report for Congress. "Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues" by Daniel Morgan and William Krouse, Resources, Science and Industry Division and Domestic Social Policy Division. February 7, 2005.

Government of the Philippines, World Bank and Asian Development Bank. 2003. "Philippines: Improving Government Performance: Discipline, Efficiency and Equity in Managing Public Resources."

French, Angela. "Real ID: Big Brother Could Cost Big Money," Citizens Against Government Watch (CAGW). October 17, 2005.

London School of Economics and Political Science. The Identity Project. An Assessment of the UK Identity Cards Bill and Its Implications. Interim Report. London, March 2005.

National Computer Center. "Information and Communication Technology (ICT) Resources Survey 2002-2003," June 30, 2003.

Privacy International Interim Report. Mistaken Identity; Exploring the Relationship Between National Identity Cards and the Prevention of Terrorism, April 2004

Wang, Tova Andrea. (undated). The Century Foundation Homeland Security Project. The Debate Over a National Identification Card.

Journal

Office of the Special Envoy for Transnational Crimes (OSETC) Digest. "The National ID System." January-March 2005.

Unpublished Work

Australian Privacy Foundation. A New 'Australian Card': The Costs Outweigh the Benefits: An Open Letter to Coalition MPs. (July 28, 2005)

Baviera, J. and Mendoza, A, Jr. Expanding and Enhancing the Usage of the Tax Identification Number (TIN). December 18, 2002

Statutes

Executive Order No. 420. Requiring All Government Agencies and Government-Owned and-Controlled Corporations to Streamline and Harmonize their Identification (ID) Systems, and Authorizing for Such Purpose the Director-General, National Economic and Development Authority to Implement the Same and For Other Purposes.

Executive Order No. 420. Implementing Rules and Regulations.

Presidential Decree No. 278. Instituting a National Reference Card System and Creating Therefor the National Registration Coordinating Committee.

Administrative Order No. 308. Adoption of a National Computerized Identification Reference System.

Web - Based Articles

Card Technology, 2001. "Going Global with National I.D." <http://www.wired.com/news/conflict/0.2106,47073,00.html>

Demos. "Statement in Opposition to a National Voter Identification Card." <http://www.demos.org/pate337.cfm>

Jones, Jennifer, 2001. "White House Nixes Controversial National I.D. Notion." Infoworld. <http://www.infoworld.com/articles/hn/xml/01/09/27/010927hnnatid.html>

Scheeres, Julia, 2001. "ID Cards Are de Rigueur Worldwide," wired news. <http://www.wired.com/news/conflict/0,2100,47073,00.html>

This paper was principally prepared by Dir. Jean Encinas-Franco of the Governance Sector under the supervision of the SEPO Director General.

The views and opinions expressed herein are those of the SEPO and do not necessarily reflect those of the Senate, of its leadership, or of its individual members.