UNDER THE WATCHFUL EYE

The Philippines' proposed national ID system, the anti-terror bill, and the global project to keep an eye on everyone

A SPECIAL REPORT FROM FOCUS ON THE GLOBAL SOUTH
20 APRIL 2005

EXECUTIVE SUMMARY

The national ID system is not about simplifying government transactions. Its true intent is to construct a massive, centralized database of dossiers on all Filipinos accessible not only to local authorities but also to the US and other governments. Along with the proposed anti-terror law, this database will be a dangerous instrument of control and repression: It will make it easier for the government to keep an eye on political dissidents, opposition members, activists – or whoever will be designated as "terrorists" by those who have the power to define the term. But it also poses danger even to non-political individuals and ordinary citizens because the database could be used for profiling via "data-mining": the process of electronically calculating the level of risk posed by individuals in the hope of singling out "potential terrorists" based solely on information in people's dossiers. It is a process that is intrinsically prone to discrimination and error.

The local push for a national ID system is not isolated and should be seen in a bigger context. It is part of on-going attempts to construct a global infrastructure for mass registration and surveillance. The construction of this infrastructure is marked by the following: the push for national identification systems around the world and the adoption of a global identification system, the creation of an infrastructure for tracking movement and for monitoring communications and transactions, the networking of national and international as well as public and private databases; and the global expansion of data-mining practices.

With the anti-terror law rolling back legal safeguards against state abuse, this global registration and surveillance infrastructure will lead to the detention or restriction of movement of many innocent civilians, the curtailment of political opposition, and the erosion of human rights and civil liberties. And yet, for these real dangers, there is no guarantee that the national ID system will make Filipinos feel safer. ■

Proposals for a National ID System (NIS) have been revived by the Philippine government following recent bombings in several urban areas in the country. How this system will finally be implemented is still unclear and there have been differing suggestions on what it aims to accomplish. President Gloria Macapagal-Arroyo has categorically stated that it is one of the "key elements" in the fight against terrorism.[1] Still, there are efforts to cast the proposal as nothing more than a way to facilitate government transactions, to "speed up business,[2]" or, as Press Secretary Ignacio Bunye puts it, to make wallets less bulky.[3} Senator Panfilo Lacson laments, in the explanatory note accompanying his NIS bill, how difficult it is for people to remember different government numbers and how the revision of this numbers "compound one's misery.[4]" Justified this way, the NIS proposal is just an innocent plan to make Filipinos' lives easier, a harmless scheme that could only be opposed by those who, according to Interior Secretary Angelo Reyes, have something to hide.[5}

A proposal's packaging, however, does not necessarily reveal its true intent. While the operational details of the NIS still have to be finalized, we can try to find out whether the proposal is as innocuous as it is portrayed in three ways: First, by examining how the proposal fits in with other related developments around the world; second, by looking at how similar systems are being used or are intended to be used in different countries around the world; third, by scrutinizing how the system is actually planned to be implemented.[6}

PART OF SOMETHING BIGGER

After the 9-11 attacks in the United States in 2001, a rolling wave of anti-terror legislation and other measures were enacted across the globe. The US was the first to pass its own version, the USA PATRIOT Act. Backed by the United Nations Security Council and armed with its economic, political, and military power, the US demanded that other countries follow its lead and pass laws modeled after its own.

Swayed by the stick and carrots wielded by the US or, in many cases, taking advantage of the opportunities for advancing their own agenda, many governments promptly complied. The United Kingdom, for example, passed its Anti-Terrorism, Crime and Security Act, while the European Union, Canada, and many other countries revised existing laws or adopted their own set of measures. Other governments entrenched their internal security laws. Malaysia's controversial Internal Security Act has found a new justification and has even expanded. Indonesia also has a new anti-terrorism law; while in Thailand, an anti-terrorism executive degree was passed.[7}

Most of these anti-terror measures invariably have provisions legalizing warrantless arrests and indefinite detentions, loosening of rules governing wiretapping, surveillance, and monitoring of personal communication and transactions, freezing of assets, etc. – all without state officials having to prove that they have reasonable grounds to do so. In some cases, they include provisions that sanction secret searches, secret arrests and secret trials – in the sense that an individual is not allowed to report to anyone that he or she has been searched, arrested or has been undergoing trial – as well as the use of secret evidence – in the sense that the evidence does not have to be shown to the accused, giving her or him no chance to question its source and validity.

HARMONIZING TERROR LAWS AND SECURITY FUNCTIONS

In sum, most anti-terror laws have allowed states to do almost everything they want with people they suspect of whatever they have designated to be acts of "terrorism," while at the same time preventing these individuals from defending themselves or proving their innocence. Individuals can hide nothing from the government even as the government is allowed to hide virtually everything from them. Under the anti-terror laws, "suspected" terrorists are presumed guilty unless proven innocent and the burden of proof is on the individual, not on the state.

Alongside this growing coherence among different countries' laws is the increasing coordination among various countries' law enforcement and intelligence agencies. Shortly after the February 14 Makati bombings, for example, a team of Australian anti-terror agents arrived in the country to join local investigators. Various US agencies are also expanding their reach and deepening their ties with their counterparts around the world. The US Department of Homeland Security, for example, has an office in the EU capital of Brussels. In Kuala Lumpur, the US has established the Southeast Asia Regional Counter-Terrorism Center to train local police and intelligence authorities in the region.

Thus, not only are states adopting similar – if not identical – laws, they're also linking their security functions and operations at a global scale. The result of both trends has been the emergence of a global "anti-terror" regime that has resulted in a global erosion of human rights and civil liberties. Laws and measures that have been enshrined in most societies after decades – if not centuries – of efforts to protect citizens from the abuse of state power have been rolled back in just three years.

The proposal for the NIS and the anti-terror bills (ATB) should be seen in this bigger global context – not as isolated local initiatives that suddenly appeared in a vacuum. Though it is not yet clear how the Philippines' own anti-terror law will look like after or if ever it comes out of the legislative mill, it is expected to hew very closely to the template described above. Despite claims to the contrary by some proponents, the proposal is inseparable from the government's anti-terror campaign. While others have disavowed its "anti-terror" aims, President Arroyo herself has explicitly said that the proposal is intended to be integral to the government's anti-terror bill, a measure which she has vowed to push for in order to "to add more teeth in the fight against terror" and "to strengthen our internal security laws.[8]" Secretary Reyes claims that the proposal will hinder "would-be" terrorists from carrying out their plans.[9] Senator Lacson says that it is because of "terrorism" that the NIS should be implemented without delay.[10]

ENTERING THE MATRIX

But how would the NIS and the ATB catch "terrorists"? And how would human rights be compromised?

The MATRIX may have the answers. The Multistate Anti-Terrorism Information Exchange (MATRIX) project is a massive database that contains millions of personal information, including physical features, ethnicity, current and past addresses, phone numbers, criminal history, real estate information, photographs of neighbors and business partners, car model, credit history, marriage and divorce records, etc. The actual list of data compiled is kept secret so nobody knows for sure – except those who maintain and access the database – what else the MATRIX keeps. Sixteen states in the US had pilot-tested the program but due to public protests, only five states are still currently using it. And though it is operated in only these five states, the MATRIX's database includes information culled from many other states' databases. Maintained by a private company, Seisint Inc., the MATRIX is partly funded by the US Department of Justice, controlled by the US Department of Homeland Security, and accessible to local and federal government officials.[11]

What was the MATRIX for? Using all the information available, Seisint formulated a "terrorism quotient" to seek out "potential terrorists" among the individuals whose records were in the database. The company set up a "terrorist index" which included factors that could either increase or decrease the probability of an individual being a "terrorist." Included in this index were age, gender, ethnicity, credit history, "investigational data," information in drivers' licenses, connections to "dirty addresses," etc.

This practice is called "data mining": the computerized analysis of extensive electronic databases containing a vast amount of information on private individuals to identify patterns of behavior that supposedly indicate "terrorist" activity. This in turn is used for "profiling" or assigning of levels of risk to individuals.

Based on the supercomputer's calculations, a total of 120,000 individuals were found to have a "High Terrorist Factor" score. Their names were given to the Federal Bureau of Investigation, the Secret Service, and other police agencies. Dozens were arrested but until now, their identities remain secret. It is also not known what the evidence were for arresting them, whether they were convicted or charged with any crime at all, or whether they are still in detention.[12]

TOWARDS A PINOY MATRIX

While that may sound like a science-fiction plot, the MATRIX is real: its existence is neither denied nor classified. Judging from the avowed motives and some of the publicized operational details of the proposed NIS, there is good reason to suspect that the MATRIX provides the model for what the government intends to do with all the information it wants to get it hands on. The justices of the Supreme Court suspected as much when they outlawed former President Fidel Ramos' earlier order to implement an NIS, saying that it could give the government "the power to compile a devastating dossier against unsuspecting citizens."

This time, however, we're talking not just of a local but a global database of dossiers accessible not only to Filipino officials but to other governments as well. It is important to stress that what's crucial to the national ID system is not just the physical card itself but the vast amount of information stored in or linked to each card. Under the plan, all Filipinos are supposed to be given a single "reference number" at birth. And as Defense Secretary Avelino Cruz has said, "With one number for each individual, it is easier to check their files from a computer.[13]"

The NIS has three significant features: First is its compulsory nature. Senator Lacson's bill explicitly states that those who will fail to secure an ID will be imprisoned while those who refuse to recognize the card as the "only official identification" of the bearer will be fined. If the NIS is simply about "facilitating government transactions," as is claimed, then there is no compelling reason why it has to be mandatory. People do not have to be punished if, contrary to Bunye's preferences, they would rather that their wallets remain bulky. The compulsory nature of the NIS is predicted to be one of the most contentious aspects of the proposal and its proponents are likely to consider it as the one non-negotiable clause in the bill.

Second is the consolidation of all the information on individuals currently kept by different government agencies such as the National Statistics Office, the Government Service Insurance System, the Social Security System, the Bureau of Internal Revenue, the Land Transportation Office, the Commission on Elections, etc. For Bunye, "The ideal step is to have one synchronized system.[14]" Lacson's bill calls for the creation of a National Registration Coordinating Commission to oversee the fusion of their databases. Senate President Frank Drilon's proposal to just combine all the agencies' databases – without having to legislate an ID system – will have the same effect.[15] Under both Lacson's and Drilon's proposals, people who have records with the cited agencies would have no say on whether they want their records in a particular agency to be merged with their records in the other agencies.

Third is the deliberate ambiguity on precisely what information will be contained in each card and, more importantly, in the database where the reference numbers and the corresponding data are stored. Among the information to be kept under Lacson's bill include the name, address, blood type, next-of-kin, and other "sensitive and confidential data." Reyes said the ID will contain only the bearer's personal information such as her or his full name, birth date, height, weight, and, in his words, other "distinguishing features." For his part, Cruz wants criminal records included. It is important to note that the set of data accessible to the owner of each ID does not necessarily have to be identical to what can be accessed by those who will maintain the central database. The "sensitive and confidential data" which Lacson's bill mentions for example is confidential only to the bearer but obviously not to the government.

What other information will be included and from where will they be taken? Under the emerging "anti-terror" regime discussed above, we can expect the government to invoke security reasons to keep this information to itself. But as with the MATRIX model, we can expect the government to gather as much information on individuals as possible and to link the database with other databases, not just locally but internationally as well. Not only will we not know what sort of "sensitive" information is being collected on us, we may also not know who exactly will be prying over our dossiers.

Whether enforced by law, by an administrative order, or by local ordinances, the three features discussed above are expected to be the cornerstones of an overt – or possibly a *de facto* – national ID system. They are essential to constructing an effective centralized dossier for storing information on suspected "terrorists" or for ferreting "potential terrorists" in a population. The NIS will have to be compulsory because it does not make much sense to have a database with only the records of those who volunteered information. People will have to be forced to register or else. The bigger the percentage of people in a population whose records are included in the database, the wider the net for catching "potential terrorists." The more information there is for each record and the wider the array of information gathered, the more "accurate" data mining is hoped to be. In sum, the more people and the more information there are, the more reliable our local MATRIX will be to whoever will have control over it.

A GLOBAL MATRIX?

But who holds the key to the MATRIX? In this case, it may not just be the likes of Angelo Reyes or Panfilo Lacson.

There is reason to believe that the Philippines' NIS is intended to be part of an ambitious global registration and surveillance infrastructure that aims to ensure that virtually everyone on earth is registered and that all of our movement, communication, and transactions are monitored, recorded, and stored in databases that are networked with each other and that are accessible to various governments. Again, this may sound like an outlandish conspiracy theory but in fact, the requirements of this global registration and surveillance infrastructure are already being put in place.

An international network of human rights and civil liberties groups – including the International Civil Liberties Monitoring Group, the American Civil Liberties Union, and the UK-based research and investigative journalism center Statewatch, among others – have identified the following indicators to prove that this infrastructure is indeed being constructed:

■ The global push for national identification systems

It is not only the Philippines which is currently considering adopting a national ID system. Similar proposals are also being floated in the US, in the UK and in other countries. It is not true, as Reyes claims that the US already has a national ID system in place. And while it's true that a number of other countries have long had some kind of a national ID system, as claimed by the government, what fails to be mentionioned is that the implementation of these systems were accompanied by strict privacy and date protection laws that limit access to databases and prevent the unauthorized consolidation of information.[16] What's new are the recent efforts to relax these restrictions. In many countries such as the US and the UK, proposals for national ID systems are deeply unpopular because they're associated with repressive police states. Authorities are instead hoping to skirt around public opinion by putting in place a *de facto* ID system without people's consent.

■ The creation of a global identification system

One way to achieve universal registration is through the global adoption of biometric passports. A biometric passport is one which stores an individual's fingerprint, photograph, and/or iris information in a chip that can be read and verified electronically. Governments have been discussing the introduction of biometric passports as a universal standard for years but this was deferred due to national and regional laws protecting privacy and civil liberties. After the 9-11 attacks however, the US pushed for this standard and in 2004, the International Civil Aviation Organization (ICAO) required all countries to implement it.

Significantly, the ICAO not only required immigration authorities to issue and inspect biometric passports, it also allowed states to use biometric passports for other purposes. They can set up and maintain central databases of all travellers' biometric information, store other information aside from fingerprints and iris data in the passports' chips, and use the passports as keys to a network of state and private databases.

Information in the biometric passport are to be stored in "contact-less integrated circuits," similar to Radio Frequency Identification Chips which allow for identification at a distance. Such a technology will allow governments to identify everyone at political meetings, demonstrations, or other political gatherings. It will also enable them to possibly set up a network of automated readers on roads or satellites in order to track our every step.

■ The creation of an infrastructure for globally tracking movement

The biometric passports or national ID cards with "contact-less integrated circuits" are expected to be required not just for international travel but for domestic travel using different means of transportation as well. If this happens, all bus stations or airports will turn into a vast network of internal checkpoints for monitoring and controlling movement.

A related development is the drive towards accessing and sharing passenger name record (PNR) information or all the information on passengers kept in air travel reservation systems. This includes passengers' addresses as well as the address where they will be staying abroad, who they will be staying with, travel itinerary, credit card information, meal preference, medical information, etc. The US now requires all foreign airlines to provide PNR information to its customs service and other agencies, to give them direct access to the airlines' computer systems, and to make data available to US agencies for all foreign flights – not just for those destined to the US.

■ The creation of an infrastructure for the global surveillance of electronic communications

Since 1948, the US, UK, Canada Australia and New Zealand have been implementing a program to monitor the world's communication systems in order to spy on other governments and to share information on each others' citizens. Called ECHELON, this program allows governments to intercept e-mails, faxes, telexes, and phone calls and enables them to analyze millions of messages and conversations daily. Now all this surveillance will increase dramatically with the adoption of the *Convention on Cybercrime* by the US and 29 other countries in November 2001. Under this treaty, internet, phone, and other communication companies are obliged to provide security agencies with direct access to messages in their systems, including information about who the messages were sent to, when they were sent, as well as the history of web pages visited by their costumers. Companies are likewise forbidden from revealing whose and what records they divulged.

■ The creation of an infrastructure for the global surveillance of financial transactions

After 9-11, there has been a raft of new anti-money laundering laws adopted by various countries to track and control financial transactions around the world. These laws compel banks and businesses not only to build the capacity to conduct surveillance on their database systems but also to actively compile information on their costumers that they would not otherwise bother to collect, report certain transactions to the government, and keep an eye on customers that are on watch lists. Under the USA Patriot Act, for example, all businesses, shop owners, contractors, real estate agents, banks, etc are required to file a "Suspicious Activity" report for transactions above a certain amount.

■ Growing access to private sector databases and growing involvement of the public sector in surveillance

As evidenced by the role of airlines, telecommunication companies, internet providers, banks and other financial institutions in the developments discussed above, the private sector is increasingly being tapped to play an integral role in this global registration and surveillance infrastructure. Under the Patriot Act, the FBI has the power to access any record stored by US-based companies and their subsidiaries – regardless of whether the information belongs to US citizens or not. Aside from compelling these companies to gather information and provide them to the government, private sector firms are also increasingly being given the financial incentive to compile information on their own.

The US government, for example, has obtained information from domestic and foreign databases by directly purchasing them from such private data aggregators as Acxiom, Abacus, and LexisNexis.[17] Hundreds of millions of Latin Americans' private records are now in the hands of US security agents after they were bought from the US company ChoicePoint.[18] Other companies don't even have to be offered money; they are giving the information voluntarily without informing their costumers and asking for their permission. In May 2004, the biggest airline companies in the US such as American, United, and Northwest, admitted to handing over millions of records to the FBI.[19] Other examples abound.

■ The consolidation of national and international databases

Alongside the extensive and aggressive collection of information worldwide is the unprecedented consolidation of this collected information globally. We're seeing a comprehensive network of interconnected and inter-operable local and national, public and private databases accessible to various government security agents around the world. For example, the US and the Europol recently signed an agreement that will allow US agencies to access the Europol database with all its information on individuals' racial backgrounds, political opinions, religious beliefs, and even their sex life.[20] The increasing collaboration among different governments' security agencies obviously also entails the sharing of information among them.

■ The expansion of "data mining"

The MATRIX is just one example of a data-mining project that uses the mountains of information that is currently being compiled on individuals. The Total Information Awareness program developed by the US' Defense Advanced Research Projects Agency, for example, aimed to mine what US Defense officials described as "the transaction space" to find "signatures" of terrorist activity. The project has since been officially called off but has effectively been revived under different names. For example, the Central Intelligence Agency (CIA) reportedly has a data-mining program which has been described by a CIA official as "so powerful it's scary.[21]"

Another data-mining project with a concrete application is the Computer Assisted Passenger Prescreening System or CAPPS II. Using the passenger name records (PNR) described earlier, the system seeks to classify travelers as having "green," "amber," or "red" risk profiles. "Green" travelers will be allowed to board their flights, "amber" ones could be interrogated, while "red" ones will not be allowed to fly and may even be detained. The Canadian government is also reportedly installing a similar program inter-operable with that of the US.[22] Meanwhile, German police units have been inputting data collected on men with Islamic backgrounds into a "Central Foreigners Register" for information "trawling" or "dragnet control.[23]"

Taken together, all of the seemingly isolated and little-reported developments above point to the construction of a global infrastructure intended not just for ordinary police work but for the mass surveillance and control of populations by the United States, our national government, and other governments as well. The proposed anti-terror bills and the national ID system are part of efforts to more deeply integrate us into this global infrastructure. All the personal records that will be consolidated in one central national database, as well as those that have been or will be collected on us will be linked to a global network of databases and made accessible not just to our own government but to the US and other governments as well. They will then be used to classify us and measure our "risk potential."

Under this global infrastructure, we are all treated as suspects – with some, such as Muslims or activists deemed to be more suspicious than others. We are all "potential terrorists" now and it is up to us to prove otherwise. Under the global "anti-terror" regime, however, with its secret arrests, secret evidence and secret trials, we may not even be given the chance to prove our innocence. And unlike before, when people for the most part only had to worry about the likes of Reyes or Lacson poring over our dossiers, now we also face the prospect of US Defense Secretary Donald Rumsfeld freely going over our files and having the power to secretly arrest us wherever we may be.

THE USUAL SUSPECTS

This infrastructure will victimize not just those with "something to hide" – or who may have all the right reasons to hide something from the likes of Reyes and Lacson – but virtually everyone. The danger comes from two sources:

First is the deliberate attempt by a government to tag as "terrorist" those whose objectives counter that of the state and the interests it represents. As has been pointed out by human rights groups around the world, one of the most fundamental problems with the "war on terror" and the accompanying wave of anti-terror legislation is that governments have been granted unquestionable power to decide who's a "terrorist" and who's not according to their own criteria and their own interests. The New York-based Lawyers Committee for Human Rights (LCHR) sums up the impact of anti-terror legislation when it said, in a report, "In a growing number of cases, legal safeguards are now observed only so far as they are consistent with the chosen ends of power." There are no universal and objective guidelines for determining who's a "terrorist" and who's a "freedom fighter." Neither have there been democratic processes for designating the labels. The EU list of "terrorists," for example, simply lifted many of the organizations in the US list, and was railroaded through Parliament without debate.[24]

The US list itself includes a number of groups which could be considered national liberation movements and groups resisting repressive regimes. During the apartheid era, former South African president Nelson Mandela was considered as a "terrorist." Most recently, the Iraqis resisting the occupation of their country, a legal right enshrined in the Geneva Conventions, have been labeled by the United States as "terrorists" – a view unquestioningly repeated by the mainstream media.

The definition of the anti-terror laws that have been adopted are so vague that governments could easily tag the label on the political opposition, trade union movements, and other activists. For example, terrorism is defined under the EU anti-terror law as "committing or threatening to cause extensive damage to a government or public facility, transport system, infrastructure facility, or private property likely to result in major economic loss when committed with intent to compel the organization to perform or abstain from any act or seriously destabilize or destroy the fundamental political, constitutional, economic or social structure or a country or international organization." With this definition, people who engage in strikes or join mass protests against the World Trade Organization could easily be labeled as "terrorist.[25]" Indeed, immigrants wishing to enter Europe are now required by law to give backgrounds of their trade union involvement.[26] The Canadian Security Intelligence Service (CSIS) has already identified certain sections of the anti-globalization movement as security concerns. But as the former director the CSIS admitted, definitions of "terrorism" could "easily include behavior that doesn't remotely resemble terrorism.[27]"

The problem is, once the "terrorist" label is affixed to an individual, it sticks. Anti-terror laws do not give individuals or groups any due process for contesting governments' designation. With the national ID system, expect your "terrorist quotient" to go up under-data mining once your participation in a strike or in a mass demonstration is recorded in your dossier. Worse, you won't even know what other things you do could ratchet up your score since the government will not be obliged to disclose what factors are included in its "terrorist index." When state agents do decide to get you, thanks to the chips tracking your every move, they'll know exactly where you are. Hand in hand, the NIS and the anti-terror law will be very effective tools for repression.

FREE HOLIDAYS IN CUBA

But it's not only the activists, the trade unionists, or other political groups that need to be concerned. The second source of danger inherent in the global infrastructure of surveillance is plain error. Everyone is in danger and simple statistics prove that this warning is not being alarmist.

Suppose that at least a billion people are included in a global database that is data-mined to identify "potential terrorists." If even just 0.1% of them are calculated to have a "high terrorist potential" and assuming that the technology is fool-proof, with a margin of error of only 5%, that would still be 50,000 people wrongfully accused. Assessing the possible impact of the CAPPS II program, the Association of Corporate Travel Executives calculated that even if only 2% of passengers were designated "red" travelers, that would mean up to 8 million passengers barred from flying or detained every year.[28] Even the US Government Accountability Office had reported that CAPPS II was not shown to be effective in identifying possible "terrorists." David D. Jensen at the University of Massachusetts, one of the researchers for the TIA project, admitted that their envisioned data-mining process could result in "high numbers of false positives...[29]"

The biometric technology used for passports and ID cards itself is prone to error. US government tests have shown that scanners cannot recognize individuals 5% of the time or matches the bearer of the card to someone else 1% of the time. The percentage of error rises to 15% as photographs become dated. If there were one billion biometric passport holders, that would mean 150 million people mistaken for someone else. Even if the technology achieves a 99.99% accuracy rate, that would still be one million people wrongfully recognized.[30]

The distribution of error, however, is not equal and the error itself is not entirely innocent. With ethnicity or religion likely to be factored in in the algorithm, Muslims, people with Muslim-sounding name, or people with a Middle-Eastern profile are expected to be singled out. Even without data-mining, Muslim communities in the Philippines have routinely been scoured for "terrorist" suspects and scores of innocent civilians have been arrested and detained. Once the NIS is in place and data-mining is practiced, these groups' vulnerability could only be heightened because racial and ethnic profiling is intrinsic to any mass surveillance project. According to a recent research by the Institute of Race Relations in Britain, Blacks and Asians were four times more likely to be stopped and searched under the UK's anti-terror laws. Others, including those from the Middle East, are seven times more likely to be stopped.[31]

If the errors resulted only in minor inconvenience, they could be shrugged off. But for the 700 foreign nationals who were shipped off as "terrorist" suspects in Guantamano Bay in Cuba alone, the error has meant indefinite detention, denial of access to lawyers and relatives, and torture. For Maher Arar, a Canadian citizen from Syria who was taken aside at the New York airport, it meant being sent to Syria by US officials, being detained and tortured in prison, and staying in a cell just a bit wider than his torso and just two inches longer than his height for almost a year. The Syrians eventually released him, saying they had no evidence against him and that they held him only to please the United States.[32]

REAL COSTS, IMAGINARY BENEFITS

Adopting the anti-terror bill and the NIS would mean embracing these dangers. And yet, despite the high price to be paid and the potential threats ahead, there is no guarantee that they will really make Filipinos more secure. "There is no guarantee that it will eliminate terrorism," Congressman Prospero Nograles, one of the NIS' proponents in Congress recently admitted in a TV interview.[33] Indeed, government officials are often at a loss when pressed to explain how exactly an ID system could possibly have stopped the latest bombing in Makati.

Concerns about human rights and civil liberties, as well as the lack of any proof that the NIS will indeed stamp out "terrorism," help explain why its proponents are attempting to package the proposal in another garb. If the government and the proponents of the measure really just want to make people's lives easier or if it wants to dispel accusations that they merely want to keep an eye on the population, then the following steps should be accepted without any conditions:

■ Any national ID system should not be made compulsory in law or in fact.

There should be no penalties for people who refuse to acquire IDs. People should not be jailed if they prefer to keep their wallets bulky. At the same time, no measures should be taken to institutionalize a *de facto* compulsory ID system in which people are not formally required to have IDs but are left with no other choice but to secure them. No ID should be the "only official identification," as Lacson wants. In no way should a person's failure to show the ID be used to deprive him or her of free movement, government services, or employment. There should be no registration at birth; the decision whether to get an ID should be given only to adults.

■ The data to be collected should be protected.

Before any national ID system could be legislated, the passage of a Data Protection Law should be considered a prerequisite. This law will list concrete steps to prevent abuse of data, assign responsibility for its protection, and prescribe penalties for violations. In the face of the US' and other governments' efforts to contravene similar statutes through regulations and standards set by unaccountable supranational bodies, this law should contain a provision explicitly declaring that none of its provisions could be overridden by international agreements or international organizations.

■ The data to be collected should be limited.

The data to be stored in each ID as well as in the central back-end database should be restricted to those that have already been freely given to other government agencies. The complete set of data linked to each ID should be fully disclosed to the bearers. No other "confidential" or add-on data should be included. There should be no information whatsoever on people's religion, political affiliation, or any other category which may be used as a basis for profiling, discrimination, or persecution.

■ The data should not be disclosed to third parties.

The database should not be linked to any other database, whether public or private, in the Philippines or abroad. It should not be tied with any databases compiling information on people's phone calls, internet browsing, travel, or financial transactions. It should not be made available to the local law enforcement agencies as well as to the FBI, the CIA, or other government's agencies. It should not be voluntarily given nor sold to private data aggregators.

■ The data should only used for the purposes for which they were collected.

The data should not be used for data-mining or profiling. No one may be categorized as a "risk potential" based on the information contained in the ID. The data should also not be used to track movement: people should not be required to show IDs while traveling around the country such that one's movement from point A to point B would be recorded.

■ There should be adequate legal protections against abuse and sufficient mechanisms to ensure data security.

Stringent measures to protect the integrity of the data should be clearly spelled out. Severe penalties should be imposed on anyone illegally accessing or disclosing information in the database as well as to those using them for data-mining purposes or for surveillance.

It is highly doubtful whether proponents of the NIS will agree to the above safeguards since each of them undermine the very purpose for which the system will be established. But it would still be worthwhile checking the above provisions against the operational details of any NIS proposal. Whether or not they will be put in place will reveal whether it is in fact the proposal and its proponents that have something to hide.

Supporters of the NIS are likely to argue that in the fight against "terrorism," human rights and civil liberties would have to be sacrificed for greater security. Given the absence of any assurance that the NIS will indeed lead to catching "terrorists" and given the certainty that the proposal will definitely trample on the rights of innocent civilians and legitimate dissenters, it is worth asking whether we are not trading away real security for imaginary safety. ■

NOTES:

[1] Lira Dalangin-Fernandez, "Arroyo backs national ID system," Philippine Daily Inquirer, 18 February 2005

[2] Rizal Raoul Reyes, "Philippine Social Security chairman: 'National ID will speed up business,'" Today, 2 November 2004

[3] Gil C. Cabacungan Jr, Christine Avendano, Edison Tandoc Jr, "Bunye dispels fears of national ID system," Philippine Daily Inquirer, 21 February 2005

[4] Senator Panfilo Lacson, Explanatory Note to Senate Bill No. 833, "An Act Instituting a National Reference Card System and creating therefore the National Registration Coordinating Commission."

[5] Joel Francis Guinto, "DILG chief pushes national ID system against terrorism," Philippine Daily Inquirer, 18 February 2005

[6] For more information, see the report of the International Campaign to Stop Global Registration and Surveillance and the International Civil Liberties Monitoring Group report, Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms, and Democracy, Ottawa, 17 February 2004

[7] Yap Swee Seng, "Impacts on the South: The Case of Malaysia" in Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms, and Democracy, p. 56; See also the Summary Report of the Asian Consultation on the "Impact of Terrorism and Anti-Terrorism Measures in Asia," organized by the Asian Forum for Human Rights and Development (FORUM ASIA) and SUARAM, posted on http://www.forumasia.org/activities/thematic/tctmhr/index.shtml

[8] Dalangin-Fernandez, "Arroyo backs national ID system"

[9] Alexander Villafania, "Politicians back a national ID system," Philippine Daily Inquirer, 18 February 2005

[10] Senator Panfilo Lacson, Explanatory Note to Senate Bill No. 833

[11] Madeleine Baran, "Welcome to the Matrix," The New Standard, July 8, 04; David Cole, "Uncle Sam is Watching You," New York Review of Books, 18 November 2004

[12] Baran, "Welcome to the Matrix"

[13] "Inclusion of criminal records in national ID mulled," Philippine Daily Inquirer, 5 March 05

[14] Dalangin-Fernandez, "Arroyo backs national ID system"

[15] Alexander F Villafania, "Drilon: Why not just integrate existing IDs?" Philippine Daily Inquirer, 23 February 2005

[16] House of Commons Canada, A National Identity Card for Canada?, Interim Report of the Standing Committee on Citizenship and Immigration, October 2004, pp. 16-23, www.parl.gc.ca/Infocom/Documents/37/2/parlbus/commbus/house/reports/cimmrp06-e.htm [November 24, 2004]

[17] Kim Zetter, "Big Business becoming Big Brother," Wired.com, 9 August 2004

[18] Jim Krane, "Information bank reaches into Latin America: US buys access to personal data," Daily News (Los Angeles), 20 April 2003

[19] John Schwartz and Micheline Maynard, "FBI got Records on Air Travelers," New York Times, 1 May 2003

[20] Statewatch, "Proposed exchange of personal data between Europol and USA evades US data protection rights and protections," Statewatch News online, November 2002, http://www.statewatch.org/news/2002/nov/12eurousa.htm

[21] American Civil Liberties Union, "The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Contruction of a Surveillance Society," written by Jay Stanley (New York: ACLU, 2004)

[22] Tonda MacCharles, "Air Travellers face screening; Canadian program aims at terrorist 'risk scoring' system; Information would be shared with US, documents show," Toronto Star, 17 January 2004

[23] Statewatch, "Germany: Police 'trawling' for suspect foreigners," Statewatch bulletin, Vol. 12, No. 1 (Jan-Feb 2002)

[24] Anti-Terrorism and the Security Agenda: Impacts on Rights, Freedoms, and Democracy, p. 12

[25] Marjorie Cohn, "Spain, EU, and US: War on Terror or War on Liberties," Jurist, 17 March 04

[26] Carol Nahra, "Anti-Terrorism Moves will Take a Toll on Europe's Civil Liberties, Say Rights Groups," OneWorld, 12 February 2002

[27] Reid Morden, "Spies, not Soothsayers: Canadian Intelligence after 9-11," CSIS Commentary, No. 85, 26 November 2003.

[28] Tim Harper, "US ditches travel surveillance plan," Toronto Star, 16 July 2004.

[29] Michael Sniffen, "Controversial Terror Research Lives On," Associated Press, 23 February 2004

[30] Government of the United States, "Face Recognition for Identity Confirmation - Inspection of Travel Documents," FAL/12- WP/63 10/3/04, Presented to Twelfth Meeting of the Facilitation Division of the International Civil Aviation Organization, March 22-April 2, 2004, Cairo, Egypt

[31] Arun Kundnani, "Analysis: the war on terror leads to racial profiling," Independent Race and Refugee News Network, http://www.irr.org.uk/index.html, 7 July 2004

[32] Dana Priest, "Top Justice Aide Approved Sending Suspect to Syria," Washington Post, 19 November 2003

[33] Interview, ABS-CBN News Channel, March 10, 05

HERBERT DOCENA is a research associate with Focus on the Global South, a policy research and advocacy center. He can be reached at herbert@focusweb.org

FOCUS ON THE GLOBAL SOUTH
Unit 209 Burgundy Place Katipunan Avenue
Loyola Heights Quezon City
1108 Philippines
Tel. Nos: 433-0899, 433-3387
www.focusweb.org