stratbase
ADRi
PUBLICATIONS

OCCASIONAL PAPER

MARCH 2019
ISSUE 12.3

CROSSING DATA PRIVACY LINES: IMPLEMENTING THE PHILIPPINES NATIONAL ID SYSTEM

OCCASIONAL PAPER MARCH 2019
02

CROSSING DATA PRIVACY LINES: IMPLEMENTING THE PHILIPPINES NATIONAL ID SYSTEM

Image Credit:geotab.com/blog/big-data-privacy/

NATIONAL ID SYSTEM

For a time, the Philippines had been one of only few countries in the world without a national ID system and thus, had not enjoyed the benefits savored in countries that have adopted it as India and Kenya, among others. A 2016 Asian Development Bank report described identification systems as a means for developing nations to fast-track the process of accelerating economic and social development.

DATA PRIVACY IN DIGITAL-ERA STATE GOVERNANCE

The prospects for greater innovation and improvement across all processes of government is immense in the digital age, reshaping the backbone and the landscape by which the public sector can address the needs and challenges of society. Described as evolving—even disruptive—technology is making its head way by drastically changing traditional government operations. There has never been a time of massive potential and opportunities not just for government but for all aspects of life. In what is seen to be the oncoming Fourth Industrial Revolution (Schwab 2016), technology is impacting economic, social, cultural, and human environments in scale, scope, and complexity as never before. The exponential rate of its movement with breakthroughs in biotechnology, nanotechnology, artificial intelligence, quantum computing, robotics, and the Internet of Things, among others, is changing many systems including governance (Schwab 2017).

It is heyday for government. The digital age brings in a way of doing things and infrastructure that speed up the delivery of services to citizens that vastly improve utilization of resources and access to governmental services, while also adding to transparency and greater accountability. In 2012, the United Nations e-government assessment anchored on integrated services of various public services through single sign-ons on portals, that enriched citizen experience, enabled back office integration across departments, and reinforced institutional arrangements (UN 55-72). Tremendous advancements have happened since then with governments continually pursuing reforms in key aspects of government to boost citizen participation, streamline processes, weed out duplication, and review policies to fit the digital age.

* THE VIEWS AND OPINIONS EXPRESSED IN THIS PAPER ARE THOSE OF THE AUTHOR AND DO NOT NECESSARILY REFLECT THOSE OF THE INSTITUTE.

Fueling the evolving digital society is data, said to be the “new oil” (The Guardian 2013) that every tech-driven endeavor cannot move without and the quality of which determines the value and usefulness of such endeavor. Data is to the information age as oil is to the industrial age. Authentic, complete, accurate, and reliable data produced and collected by the government enable the latter to improve policies and regulations, provide quality services, recognize rights and entitlements, eliminate corruption, raise accountability, build trust in public institutions, and be the backdrop against which government performance is regularly measured. In this sense, data has become a public good (Shah 2018) and the challenge now is how data can be better used in aid of quality governance. This is at the core of governing in the digital age.

Efficiently managing data is thus essential to effective governance, especially as citizen requirements and interactions with government generate information, and government making useful data available creates an informed populace that is better able to engage and contribute to nation-building. With data as a public good—a social good—and with its vast potential to aid governance, governments must thus seek strong data responsibility legislation that guides data owners and/or managers on their roles and obligations in collecting, managing, sharing, and protecting data and data stakeholders. Needing particular protection are personal data, the exposure of which is getting larger as the technology ecosystem is getting bigger in the private and public spheres. Personal data protection could therefore be a hurdle when seeking to fully engage people as participants in digital-era state governance. Proper stewardship of information and ensuring personal data security and protection have never been more critical.

Data privacy and protection laws of governments around the world have time and again been put to test in their discernment of what constitutes a violation and in their ability to deal with cases in their jurisdictions that at times transcended territorial boundaries. Even countries that are more sophisticated in its ways and have tighter rules on user data have not been spared, as highlighted in the case of former National Security Agency (NSA) contractor Edward Snowden who leaked highly classified information from the NSA in 2013, the British global political consultancy Cambridge Analytica security breach in March 2018 in which about 87 million Facebook users data were illegally collected through an online personality quiz in a bid to help candidate Donald Trump, and the ongoing accusations against Chinese company Huawei over national security issues in countries where the former provides its technology.

The Philippine Government, too, has its data privacy laws under challenge and scrutiny. The next statements will look into how the Philippine government’s understanding and thrusts in that area have moved forward and how this government can fail or succeed. It will be against the backdrop of the Philippines national identification system that was signed into law in August last year, and in light of major data breaches such as the *Comeleaks* in 2016 that exposed over 70 million voters’ registration data and the massive passport data mishandling at the Department of Foreign Affairs this year, and these against the enforcement of Republic Act No. 10173 (Data Privacy Act of 2012) that is said to follow internationally accepted data protection and privacy standards.

IMPLEMENTING THE PHILIPPINE NATIONAL ID SYSTEM

The Philippine government is at the center of a large-scale digital metamorphosis. It is looking to better decisions and faster services, as well as greater inclusion with the signing into law of the country’s first national ID system (R.A. No. 11055) at a budget of PhP25 billion. It took the country awhile to finally set up an identification system of such scale, but with the Data Privacy Act of 2012 in place and with a determined presidency, the government is emboldened to realize this legislative agenda to scale up an identification system and set it for implementation.

For a time, the Philippines had been one of only few countries in the world without a national ID system and thus, had not enjoyed the benefits savored in countries that have adopted it as India and Kenya, among others. A 2016 Asian Development Bank report described identification systems as a means for developing nations to fast-track the process of accelerating economic and social development. More than merely planning and integrating government services, providing the same to the people, and addressing the issues of social and financial inclusion and governance, ID systems help protect each citizen’s fundamental rights, allowing citizens to vote, move across borders, and access opportunities, among others. Such systems also “provide transparency in governance, curb leakages in government spending, generate valuable insights for government policies, and ensure that every citizen is counted in every governance process (ADB 1-7).”

The 2015 Brookings financial inclusion report and scorecard (Villasenor et al 2015) put the Philippines in 15th place and commended the country for having effectively provided access to

Image Credit: employerlinc.com/2018/05/biometric-privacy-laws-pose-new-challenges-risks-for-employers

a wide range of financial services for all Filipinos, with micro-loans surging 333 percent since 2002. Bangko Sentral ng Pilipinas' own financial inclusion report for the same year, though, showed that only 31.3 percent of Filipino adults had a formal bank account and only four out of ten indicated that they saved money. More optimism was seen for subsequent years should the country set up an ID system that would open doors to more inclusion especially for the unemployed and informal sectors. Adding to the impetus for a national ID system was a report that 14 percent of Filipinos were denied government and other financial services due to a lack of proper identification documents (ABS-CBN 2018).

Looking far ahead, the Philippines is put in a backdrop of global competition, not just for establishing an edge but perhaps also for survival. Already the world, for one, is looking at which cities will contribute most to global growth. A study by Oxford Economics, a leading independent global economic consultancy that identified future trends and market opportunities in the world's largest 750 cities (representing 57% of global gross domestic product and expected to contribute 61% by the year 2030), taking into account population size, age, and income per capita, showed Asia with top 10 of those cities along with New York City in contributing the most to global economic growth by 2030. While the Philippines had not surfaced among this list of top countries, the country can very well gain insight and impetus from the phenomenon happening in its neighborhood (Britton 2017).

The digital ID system is presented as a crucial enabler for financial inclusion with its potential to address the age-old problem of lack of verifiable IDs, which turns away small-value transactors from economic and other opportunities (BSP 2017). The digital age of speed and unprecedented processing power in an enabling environment had reduced the financial exclusion of adults across Asia and the Pacific to about 1 billion.

The national ID system centralizes all personal information of every Filipino citizen and resident alien and generates a Philippine ID (PhilID) and PhilSys Number (PSN) that will be used to authenticate one's identity in all government and private sector transactions, including application to schools, application for passport, driver's license, tax-related transactions, voter's registration, and bank transactions. Besides being a ticket to financial inclusion and ease of doing business in the country, the national ID also opens up access to government services especially for the poor and marginalized, thereby making public service delivery more efficient while also reducing bureaucratic red tape and corruption, and preventing fraudulent claims. It is even hoped to reduce poverty by removing political influence on the distribution of goods and opportunities. There is the belief, as it is, that the root of poverty in the Philippines is also largely political (Timberman 2018).

While there had been attempts in past administrations to secure a national ID system to facilitate access to social welfare, healthcare, financial, and other services, these had been met with strong opposition, legal challenges, budget issues, and weak public support, among others. Resistance had been so strong that the government in past administrations gave in instead to data redundancy as these allowed different government agencies to issue separate identification numbers to individuals, requiring them to provide data multiple times.

Considered a "foundational ID," the national ID is expected to supersede all 14 previous separate government ID systems, including the Unified Multi-purpose ID (UMID) which used to be the most interconnected ID as it integrated ID numbers from the Social Security System (SSS), Government Service Insurance System (GSIS), Philippine Health Insurance Corporation (Philheath), and the Home Development Mutual Fund (Pag-ibig). It may be noted that the UMID covers only around 20 percent of the 101 million Philippine population. Despite having been finally signed into law by President Rodrigo Duterte in August 2018, the Philippine Identification System Act that put in place this national ID remains disconcerted by strong resistance from certain sectors despite the innumerable benefits raised.

Those against the national ID system cite the possibilities of abuses of power that such a robust database of personal information might initiate, including various forms of discrimination, state oppression, and surveillance. Proponents' and adversaries' opposing views on the system abound. A paper published by technology and rights advocacy group Foundation for Media Alternatives (FMA 2018), for example, expounded on both sides, while hopeful that the country's first comprehensive data protection law (R.A. No. 10173 or the Data Privacy Act of 2012) as well as every citizen's vigilance of potential abuses will hold the dangers of the system's implementation at bay. Whether opponents or adversaries, it is apparent that the issue of trust in government and in digital space hang in the balance and will be critical in determining success or failure in the system's implementation.

Now that the national identification system is set, how can it succeed? A critical populace can spell the opposite, but if only to ensure that the billions of taxpayers' money will find its way to significant benefits for all, the proper stewardship of information lies among the key aspects, along with consideration of some tenets and suggestions to add to the wisdom of law and policy structures already put in place to make sure that these privacy laws follow the developments of the times.

Personal data is private and sacred. The right to privacy is imbedded in the Constitution and is held sacred for its vast implications on human dignity and freedom, among others. Such freedom is taken away from individuals in data breaches when certain important decisions impacting them are made without their awareness or participation, hence, denying these individuals control over their lives. When people feel their personal information are held hostage by an entity as the state and put at risk for discrimination or suspicion, they will feel impeded in their exercise of the freedom to express themselves or to associate whether in social or political activities. Furthermore, this privacy, this anonymity, is thus important as it ensures that people treat each other as free people and equals despite differences and incompatibilities in their identities, beliefs, affiliations, interests, etc. This sense of freedom and equality are elements for democratic politics that structure and limit competition for power (Lever 109). Truly, the risk of a data breach is deeply personal especially given that the data one provides the government can live in perpetuity, not erased following what should be ephemeral transactions for goods or services.

A person's inputs into the data requirements of the national ID system (including biometric information as fingerprints, iris scan and photograph, among others) and every information added from thereon with every transaction using one's assigned ID number (enrolling in school, purchasing a plane ticket, or making a claim with a government agency), pile into an ever-growing data mound and a record history that gradually creates a profile of experiences and preferences, soon becoming an intimate portrait of the individual. While there is merit to the importance of having an audit trail or history in every individual's record to maintain the integrity of the information contained, as well as for transparency on how every individual's information is being processed, the buildup is such that this can enable another, this time an entity which is the government holding such details, to gain not just information on the person but also insights from the record on that person's beliefs,

Image Credit: cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html

outlook, and character at an exponential rate. A narrative based on the individual's information may also even be possibly formed or manipulated to build a profile fitting the objective, which could be malicious, of whoever has those information on hand.

With this exponential risk despite the espoused exponential benefit, a few thoughts are surfaced. First, there should be limits in the collection of personal data, and there should be no hoarding of data. Criteria of inclusion should start with what data are necessary to carry on the objective, not a collect-all-data-now approach for purposes or value still unknown. This is spot-on risk avoidance in that the question of whether the data asked are necessary in the first place reduces the possibility of unnecessary but sensitive data from going into the system. Cautious as all should be, this minimization of data, this collection of the least amount of personal information on need-only basis is the way to go. Data regulators, controllers, and managers should look into the challenges and lessons encountered in other countries in implementing their national ID systems and in enforcing their data privacy laws. India's Aadhaar, the world's largest biometric ID system and the one on which the Philippines' ID system is being modelled after, was allegedly breached by rogue agents selling access (meant for government officials) to its central database for just a few hundred rupees, compromising over 130 million IDs of its over a billion ID holders. While following Aadhaar's trail for best practices, the country is best to pay attention also to the lessons and realizations in implementation.

While India grapples with the incident, closed networks for highly vulnerable data could also be looked into as an option, although such action could work against the full potential of big data. Some countries have actually started on this effort of hardening their internet systems, so a collaborative global discussion of this intervention is imminent.

And as there is no such thing as perfect digital security on the internet, the country must scrutinize other models as the European Union's General Data Protection Regulation (GDPR), checking how advanced nations draw the line to effectively shield sensitive data while managing necessary personal information. The new EU regulation is getting organizations upbeat in reassessing and beefing up their data privacy and data security governance strategies given the growing sophistication of cybercrimes. The Philippines must look into its own data security governance strategy that most of all should prioritize the data subjects' rights, conduct regular risk assessments, and adjust policies and procedures to accommodate new threats to security as soon as these are identified. Data controllers should also be upbeat on best practices across the globe given the wide-ranging, intercontinental nature and capabilities of cybercrimes.

High penalties as deterrents to crimes may also be considered, noting how advanced models like GDPR comes with high fines for noncompliance to dissuade would-be cyber criminals. Awareness of best practices and penalties, among others, will force regulators and even mere users to develop a culture of discernment and good practices.

Consultation is key. Citizen and stakeholder engagement in developing laws and regulations is a primary feature of democracy and good governance. In democracies, citizens are entitled to participate in government—in formulating, executing, and judging matters of public policy, and would even have a role in the quality of democracy (Michels 2011). Consultation is an opportunity to participate, and in this exercise, greater accountability is built on all sides, whether government, people, and/or other stakeholders. The digital age, given its tremendous capacity, should all the more be able to support democratic engagements, manifesting people's freedom to voice their opinions and coordinate efforts. Government should harness technology to connect better and be closer to its citizens and stakeholders for sound public policy. Its role adjusts with the evolving times in bridging the public to these technologies.

Despite the rhetoric, the national ID system, a data-intensive system that it is, has been the subject of public outcry for lack of consultation. Data privacy and human rights groups complained of rushed approval of the law's implementing rules and regulations. With what was considered token consultations with the public, the groups begrudged the too little opportunity to be heard on critical issues that needed to be raised, including those on handling of biometric exceptions, introducer-based registration, issues with function creep or seeding and shadow databases that allows offline authentication but may open up the system to greater risks, handling of authentication failures, deactivation of the ID number or the cancellation of the ID, and application in purely digital transactions, among others (GMA 2018).

The national ID system, controversial as the concept had been regarded since its inception, had enjoyed popular support just before it was signed into law. A Social Weather Stations (SWS) survey conducted in June 2018 showed that three in every five Filipinos believed that such a system will be helpful to them (SWS 2018). The SWS survey also showed that 61percent of Filipinos had trust that the government will protect information that will be fed into the system. This survey on the national ID, said the SWS, was non-commissioned and released as a public service.

The government can take advantage of this initial popularity with the public to carry on this undertaking. There is room for adjustments as the project moves along to ensure that the provisions of the privacy law are met and the risks are avoided. Poor consultations moving forward can backfire and can impact on the success of this major undertaking.

Citizens' opt in to the national ID system is not a yes to state control or surveillance. Based on the same SWS survey results, 49 percent of those surveyed believed that the government will not use the national ID against its oppositionists or detractors. While only 13 percent expressed little trust in this regard, 39 percent were undecided.

As said, upholding privacy supports democratic politics and limits power of one or a few by enabling people to see and treat each other as equals despite differences in beliefs, interests and identities. With the system's robust information of individuals and the questions on the law's implementing rules and regulations (after not having been subjected enough to consultations), there could be a fine line that separates proper use of information and an encroachment or a violation of privacy, such that the whole system could be misconstrued and can actually be a comprehensive surveillance system. Indeed, there can be many ways that one's record history can be used against him or her, and one does not necessarily have to be guilty of anything. The system's record history (R.A. No. 11055) can, over considerable time, develop into a centralized file that will give a detailed history of an individual's activities, tracking each transaction one makes. This may pave the way for "dataveillance" (a recent term coming from this secret tracking through data) or a comprehensive surveillance system.

The existence of the Data Privacy Act of 2012 reinforces the state's "commitment" to having a legal recourse in the event of violation of one's privacy. Interestingly, the country's Human Security Act of 2007 (a major anti-terrorism law that enables surveillance) is mandated to comply with the Privacy Act. The law imposes penalties of fines or imprisonment for any person who illegally discloses information from the system or uses it for unauthorized purposes. There is a challenge, however, to implement the law on breaches in surveillance by the very confidential nature of the act.

Image Credit: rappler.com/nation/212957-groups-urge-philippine-statistics-authority-delay-national-identification-system-irr-approva

While state surveillance is not defined under Philippine law, it is commonly understood as the close monitoring of activity, behavior, information, and communications of an individual by the state. In some instances, it can also be conducted on groups or populations. Surveillance can be carried out through wiretapping, bugging, physical monitoring, dataveillance as would be in this case, and some other more sophisticated means. One cannot know the extent of government surveillance in the country because of the secret nature of the act itself.

Treating people and their data as tools for certain other people's purposes is morally wrong. When a person or persons are denied influence over matters that may have serious implications on their lives, liberty, social standing, and their prospects, and they have no recourse for comment, appeal, or compensation by the secret nature of the act (of surveillance), the power involved is fundamentally undemocratic, even if not absolute. Even when a state may use surveillance to achieve what could be noble ends, this clandestine monitoring runs against the core democratic idea that people are entitled to govern themselves freely and as equals, and there could be no equals when there is a secret watchful eye for ends that are not known or have not been approved by citizens or their representatives. State surveillance leaves people vulnerable to misinterpretation of their actions as well as to the misuse of state power, and over time builds an atmosphere in which the state is perceived as threatening and people are reduced to being powerless and defenseless individuals.

People, in this case, should be entitled to raise and discuss with government the latter's policy on surveillance, in the same way that citizens discuss policies on justice, education, employment, and welfare, among others, inasmuch as government surveillance can be detrimental to individual lives and liberties. And where there is a violation of rights, people must be able to find whether or not government has indeed acted in covert ways, in which case the remedies should cover also that nature of government action (Newell 216-219). Add to this would be adherence to proportionality, retention periods, and implementation of better security measures to prevent data misuse.

Government officials and personnel must continually reinvent themselves. The country's Data Privacy Act is intended to be "a 21st century law for 21st century concerns and crimes," seeking to be world-class and designed to be comprehensive. This means that government officials and personnel must measure up to this new, fast-changing environment for which they must regularly reinvent themselves to contribute to an ever improving governance policy on data security and data privacy that is attuned to the times. To do so, the government should seek well-selected personnel who will be periodically trained not just to manage the technical and administrative requirements of the system but to also effectively collaborate with business, civil society, other stakeholders, and global regulators.

The ability of public authorities and government systems to move with the evolving environment through fast decision-making and effective policy-making will determine success and survival of the undertaking. With the entire bureaucracy in tow, government must be as modern, tech-savvy, and innovative while pursuing the public good.

CONCLUSION

Klaus Schwab, in describing how to manage what he called the fourth industrial revolution that emerges from this digital phenomenon, said that, "Neither technology nor the disruption that comes with it is an exogenous force over which humans have no control…" and suggests that people should grasp the opportunity and exercise the power to shape "a future that reflects our common objectives and values." In the end, he said, it all comes down to people and values. The digital revolution is yet to draw the best in the human race in terms of creativity, empathy, and stewardship, to lead to a new collective and moral consciousness based on a shared sense of destiny (Schwab 2016).

Along that line, government must thus resolve to establish a shared view among the people of how technology should affect lives and shape economic, social, cultural, and human environments. But within itself, it must also reflect on how it can project leadership by closing in on the best scenarios by which citizens can gain greater confidence given their knowledge of what happens when their data is given and have greater control over how their data is retained and shared not only within government environments but also outside where personal data may flow out (as the GDPR for instance is giving EU citizens and consumers greater control with any institution that collects data from them). Proactively, government can provide better clarity and codify how agencies, whether inside or outside government, should gather, use, and dispose of personal data.

Insofar as government is expected to design and implement policies that enhance the country's vitality and welfare, it is imperative for it to also actively engage non-state actors in healthy consultation and discourse on matters that affect the public that they represent, to address national thrusts and concerns in a holistic way, and to lessen resistance with greater consonance among all. These discussions should even lead towards a better view of the state's policy on state security and surveillance, for one, to ease suspicion or discomfort and uncertainty that make people withdraw rather than engage with government.

The business sector and civil society, on the other hand, must join hands with government in instilling data privacy, security, and protection as necessary parts in business strategy and nation-building.

The business sector needs to reflect on adjustments that are called for in its online business model—that includes how the sector collects and uses data—to address customers' growing concerns and apprehensions, in this way recovering the trust and loyalty now increasingly lost due to unscrupulous practices and misuse of data in business operations. Proactively, too, given the sector's access to resources, it can pursue models of more robust security and privacy protection that create or bring back trust and loyalty of customers and share with government and the bigger society for mutual benefits.

Civil society, whether or not with government, but most especially with government, should pursue its agenda for social change inasmuch as technology has permeated personal lives. As the aggregate of non-governmental organizations and institutions that seek to represent the interests and will of citizens, and aim to provide checks and balances in democracies' increase, the country should benefit from civil society's capacity for participatory engagement, its ability to influence government and hold it accountable, and the extent by which it is able to promote the "common good" and protect the welfare of people especially the weak and disenfranchised with unmitigated access to private data. It can employ any or all of the strategies that it does best—raising political and judicial awareness of related issues, bringing down the discourse to sensitize the local folks, ratcheting up the pressure to resolve critical concerns by organizing forums or using social media, lobbying, sending petitions to national and international bodies, proposing new laws or amending existing laws, and contesting critical issues in the courts to establish clear positions. Civil society can also provide the platform with which to better connect beyond local boundaries and join hands with the global community.

With government, business, and civil society collaboration, a continuing effort to refine implementing rules and regulations of the data privacy law, as of other laws, can remain dynamic and relevant to the times.

As pertaining to the Philippines national identity system, its potential as a development tool can only materialize if its stakeholders will apply this same vigilance and action towards leading the system into maturity and stability to enable it to support the development process, as has been the experience with the identity systems of other countries (ADB 1-7).

With such a shared view of the future, to say that technology will lead to the erosion of privacy would therefore be misleading, as this can only occur when people surrender to the course instead of building vigilance and action against man-made violations to data subjects' rights.

REFERENCES

ABS-CBN News. “National ID system can ‘open up’ more opportunities to all: Pernia.” ABS-CBN News, https://news.abs-cbn.com/business/03/16/18/national-id-system-can-open-up-more-opportunities-to-all-pernia, March 16, 2018. Accessed February 20, 2019.

Asian Development Bank. “Identity for Development for Asia and the Pacific,” Asian Development Bank, Philippines, 2016, pages 1-7.

Bangko Sentral ng Pilipinas. 2017 Financial Inclusion Survey: Moving Towards Digital Financial Inclusion. Bangko Sentral ng Pilipinas, www.bsp.gov.ph/downloads/Publications/2017/2017FISToplineReport.pdf.

Britton, Mark. “Global Cities: The Changing Urban Hierarchy.” Oxford Economics, December 2017, www.oxfordeconomics.com/cities/report, https://d1iydh3qrygeij.cloudfront.net/Media/Default/content-pieces/Global%20Cities%202017.pdf.

Foundation for Media Alternatives. The National ID Debate: Is the Philippines Ready? www.fma.ph/resources/resources-on-privacy/national-id-system/. Accessed 2-4 Feb. 2019.

GMA Network News. “Why the rush to implement the national ID system?” www.gmanetwork.com/news/opinion/content/669691/why-the-rush-to-implement-the-national-id-system/story/, October 1, 2018. Accessed February 5, 2019.

Lever, Annabelle. “Democracy, Privacy and Security.” Privacy, Security and Accountability: Ethics, Law and Policy, edited by Adam D. Moore, Rowman & Littlefield International, Ltd., London, 2016, p. 109.

Michels, Ank. “Innovations in democratic governance: how does citizen participation contribute to a better democracy?” https://journals.sagepub.com/doi/10.1177/0020852311399851, First Published June 13, 2011.

Newell, Bryce Clayton. “Mass Surveillance, Privacy and Freedom.” Privacy, Security and Accountability: Ethics, Law and Policy. Edited by Adam D. Moore, Rowman & Littlefield International, Ltd., London, 2016, pp. 216-219.

Republic Act No. 11055 or the Philippine Identification System Act. www.officialgazette.gov.ph/2018/08/06/republic-act-no-11055/. Accessed February 2-6, 2019. This Republic Act was signed into law on August 6, 2018, and its Implementing Rules and Regulations approved by the PhilSys Policy and Coordination Council on October 5, 2018.

Republic Act No. 11055. www.officialgazette.gov.ph/downloads/2018/08aug/20180806-RA-11055-RRD.pdf, page 3. Record history, in the national ID law, refers to details of authentication requests made whenever a government-issued identification card is used in any transaction by a registered individual.

Schwab, Klaus. The Fourth Industrial Revolution: what it means, how to respond. 14 January 2016, www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

Schwab, Klaus. The Fourth Industrial Revolution. Penguin Random House, USA, 2017. Originally published by the World Economic Forum in Geneva, Switzerland, 2016. The term, “Fourth Industrial Revolution,” was coined by Schwab, the Founder and Executive Chairman of the World Economic Forum. In this book of the same name, he distinguished this unfolding era from the first to the third revolutions.

Shah, Sonal and William D. Eggers. “The Government CDO: Turning public data to the public good.” www2.deloitte.com/insights/us/en/industry/public-sector/chief-data-officer-government-playbook/government-cdo-turning-public-data-to-the-public-good.html, October 12, 2018. Accessed February 18, 2019.

Social Weather Stations. “Second Quarter 2018 Social Weather Survey: 73% of Pinoys support the National ID system.” Social Weather Stations. www.sws.org.ph/swsmain/artcldisppage/?artcsyscode=ART-20180807214354, August 7, 2018.

The Guardian. Tech giants may be huge, but nothing matches big data. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data, August 23, 2013. Accessed February 16, 2019. The term “new oil” for data is widely credited to Clive Humby, UK Mathematician and architect of Tesco’s Clubcard, 2006.

Timberman, David G. “Persistent poverty and elite-dominated policymaking.” Routledge Handbook of the Contemporary Philippines. Edited by Mark R. Thompson and Eric Vincent C. Batalla. London, 2018.

United Nations. “Taking a Whole-of-Government Approach.” The United Nations e-Government Survey 2012: e-Government for the People. Department of Economic and Social Affairs, United Nations, New York, 2012, pages 55-72. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2012-Survey/unpan048065.pdf.

Villasenor, John D., Darrell M. West, and Robin J. Lewis. The 2015 Brookings Financial and Digital Inclusion Project Report: Measuring Progress on Financial Access and Usage. Center for Technology Innovation at Brookings, Washington, D.C., August 26, 2015. Also in www.brookings.edu/wp-content/uploads/2016/06/fdip2015.pdf. Accessed 6-10 Feb. 2019. The Brookings Institution is a policy think-tank in the USA founded in 1916 as the Institute for Government Research.

12.3
VOLUME

ABOUT

Allen B. Surla

is a former Director for Information Technology at De La Salle University. His work prior to the academe included establishing the first cyber technopark in the Philippines. At present, he is a senior faculty member of DLSU's Political Science Department and Assistant Dean for External Affairs and Lasallian Mission of the College of Liberal Arts. He does consultancy work for both local and international organizations, with particular focus on ICT and local governance.

STRATBASE ADR INSTITUTE

is an independent international and strategic research organization with the principal goal of addressing the issues affecting the Philippines and East Asia

9F 6780 Ayala Avenue, Makati City
Philippines 1200

V 8921751
F 8921754

www.stratbase.ph

Image Credit: biometricupdate.com/201805/tanzania-leverages-increased-knowledge-and-skill-to-move-toward-universal-biometric-identity