BIG BROTHER CASTS HIS SHADOW?: PROPOSING A LEGAL PRIVACY FRAMEWORK FOR THE PHILIPPINE IDENTIFICATION SYSTEMS ACT*

*Emir-Deogene Villafuerte Mendoza***
*Monique Banta Ang****

> *"The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—the rain may enter—but the King of England cannot enter!"*[1]
>
> —William Pitt

I. INTRODUCTION

On 27 March 2016, the Philippines experienced a massive security breach concerning government-held data when personal and sensitive information of over 55 million registered Filipino voters were leaked following a breach on the database of the Commission on Elections (COMELEC). The database reportedly contained passport information, tax identification numbers, names of firearm owners and information about their firearms, e-mail addresses, among others.[2] A group that identified itself as "Anonymous Philippines" then defaced COMELEC's website, demanding that the poll body implement the security features of the vote-counting machines for the May 2016 elections. Subsequently, another group calling itself "LulzSec" leaked 340 gigabytes of the COMELEC database online. A

---

* *Cite as* Emir-Deogene Mendoza & Monique Ang, *Big Brother Casts His Shadow?: Proposing Legal Privacy Framework for the Philippine Identification Systems Act*, 93 PHIL. L.J. 446, [page cited] (2020).

** J.D., University of the Philippines College of Law, Class Valedictorian, *cum laude* (2019); B.A. Public Administration, *summa cum laude*, University of the Philippines (2015).

*** J.D., University of the Philippines College of Law (2019); B.S. Life Sciences, Ateneo de Manila University (2014).

[1] I William Pitt, *Speech, Mar. 1763, in* HISTORICAL SKETCHES OF STATESMEN WHO FLOURISHED IN THE TIME OF GEORGE III First Series (1845).

[2] Jessamine Pacis, *National Privacy Commission to issue findings on Comelec breach*, FOUNDATION FOR MEDIA ALTERNATIVES, Sept. 8, 2016, *at* https://www.fma.ph/2016/09/08/national-privacy-commission-to-issue-findings-on-comelec-breach/ (last visited Jan. 10, 2020).

global security software company named Trend Micro Inc. commented that the COMELEC leak "may turn out as the biggest government related data breach in history."[3]

At present, the Philippines is pilot-testing a new national Identification (ID) system, an undertaking which will allow the government to collect and access personal information of its citizens and resident voters. However, with the recent data breach, the capability of the government in securing the personal information of its citizens is in question.

Notably, this challenge is not unique to the Philippines. Privacy around the world has been gradually eroding for decades and the leaps and bounds in technology has only served to accelerate this process.[4] With the advent of the Internet, obtaining private information about an individual can be done within seconds.[5] Networked databases serve as a bank of personal profiles gathered from credit card data, browsing history, and virtually all information available online and found in public records. [6] Thus, the government now faces a challenge to find the balance between the constitutionally-protected right to privacy and the need to streamline government processes by employing a national ID system.

The government must heed the warning of George Orwell, in his novel *1984*, of a dystopia led by an all-knowing Big Brother which is fueled by constant surveillance. It must overcome the Big Brother label, rather than become the feared dictatorship powered by information technology and data banks. Admittedly, the potential for invasion of privacy is present with the introduction of a national ID system and other technical instruments. Hence, it is in the best interest of the public that these technologies be regulated and safeguards be held in place to protect the dignity and constitutionally protected rights of Filipinos against unreasonable searches and seizure, to be presumed innocent, to privacy, and to due process of the law. The national ID system law must also contain safeguards and limitations in order to avoid possible abuses by government authorities. This leads to the pivotal question of whether the national ID system law contains such measures.

---

[3] Jolo Malig, *Comelec hacking threatens security of voters: Trend Micro,* ABS-CBN NEWS (PHIL.)., Apr. 7, 2016, *at* https://news.abs-cbn.com/halalan2016/focus/04/07/16/comelec-hacking-threatens-security-of-voters-trend-micro.

[4] Rick S. Lear & Jefferson D. Reynolds, *Your Social Security Number or Your Life: Disclosure of Personal Identification Information by Military Personnel and the Compromise of Privacy and National Security*, 21 B.U. INT'L L.J. 1, 3 (2003).

[5] *Id.* at 5.

[6] *Id.* at 14.

Based on the foregoing, the objective of this paper is to analyze Republic Act (R.A.) No. 11055, the law establishing the Philippine Identification System. Part II provides a brief overview of select national identity card policies around the world. Part III discusses past efforts towards a national identification system in the Philippines. Parts IV and V contain a discussion and an analysis of the Philippine Identification System ("PhilSys"), respectively. In line with this analysis, a legal framework is proposed. The PhilSys Act itself must be amended to comply with the requirements of *Ople v. Torres.*[7] A tradeoff must be decided between the speed of developing through possibly dangerous technologies versus stable tried-and-tested technologies to protect privacy. Furthermore, the Data Privacy Act must govern the PhilSys, even if the enabling law of the latter is not express. This can be done simply by amending the implementing rules of the PhilSys Act to include all the rights of a data subject under the Data Privacy Act, consistent with the Supreme Court doctrine of harmonizing all existing laws on the same subject matter.

II. NATIONAL IDENTITY CARD POLICIES AROUND THE WORLD

Prior to the passage and effectivity of the PhilSys Act, the Philippines was one out of only nine countries in the world without a national ID system, as most countries have been issuing national identification cards to its citizens.[8] Asian countries that have implemented such a system include Singapore, China, and Malaysia.

In Singapore, citizens are issued national IDs for identification purposes. However, the country is developing a National Digital Identity ("NDI") system with the objective of integrating technology in economic and government services by 2020. The NDI aims to provide a more convenient and secure access to a wide range of government services, including filing of income taxes, paying parking fines, and securing permits for foreign domestic helpers. The government also aims to work with the private sector to extend the NDI to "value-added services," such as the signing and storage of digital agreements.[9]

---

[7] Ople v. Torres [hereinafter "Ople"], G.R. No. 127685, 293 SCRA 141, July 23, 1998.

[8] Loreben Tuquero, *Nothing to be afraid of? Other countries use their national IDs in countless ways*, RAPPLER, June 15, *at* https://www.rappler.com/newsbreak/iq/204657-national-id-functions-worldwide (last updated Aug. 6, 2018).

[9] *Id.*

Meanwhile, China's national ID card serves many purposes apart from identification. Chinese nationals may use their IDs to open bank accounts, purchase tickets for public transportation, and obtain driver's licenses. Moving forward, the Chinese government aims to digitize the ID and make it available on smartphones, thus doing away with the physical ID card. China is also creating a facial recognition system as a police enforcement measure as it would match a citizen's face with his or her ID photo from out of the 1.3 billion population of the country.[10]

The national ID card of Malaysia is known as "MyKad," and is used in government and private transactions. Their national ID system stores not only personal but also healthcare information, allowing for a more efficient access of information in medical emergencies and routine treatments. Interestingly, MyKad also serves as a form of payment by being a reloadable cash purse to pay for public transportation and other government services.[11]

Meanwhile, a few countries remain resistant to a national ID system. The government of the United Kingdom (U.K.) attempted to enact a national ID system by passing the Identity Cards Act of 2006, and subsequently creating the National Identity Scheme. Based on this scheme, a centralized National Identity Register would contain personal information and biometrics of its citizens. This was never fully implemented because after the election of a new set of leaders, the scheme was scrapped altogether. It was unclear what the information in the National Identity Register will be used for.[12] However, an important consideration in analyzing the failure of the system is the politics in the U.K. at that time. The system was instituted by a government which had become unpopular, and was replaced by its opposing party. Critics did not question the system itself but the information to be collected, as the government planned to obtain approximately 50 different pieces of information from each citizen. The cost of the ID card was also an issue with each citizen to be charged £60.00.[13]

---

[10] *Id.*

[11] *Id.*

[12] Aaron Martin, *National Identity Infrastructures: Lessons from the United Kingdom,* presented at the 10th International Conference on Human Choice and Computers Amsterdam, Netherlands, Sept. 2012, *available at* https://hal.inria.fr/hal-01525100/document (last visited Jan. 10, 2020); Andrew Martin & Ivan Martinovic, *Security and Privacy Impacts of a Unique Personal Identifier*, UNIVERSITY OF OXFORD CYBER STUDIES PROGRAMME WORKING PAPER SERIES (2016), *at* https://www.politics.ox.ac.uk/materials/publications/14987/workingpaperno4martinmartinovic.pdf. "The scheme proved highly unpopular with many sectors of the community because its objectives were not entirely clear to the population at large."

[13] Gemalto, *National ID cards: 2016-2019 facts and trends*, GEMALTO WEBSITE, *at* https://www.gemalto.com/govt/identity/2016-national-id-card-trends (last visited Jan. 9, 2020).

The United States (U.S.) of America is another country that has not implemented a national ID system at the federal level. However, IDs are issued by states and territories. The Real ID Act of 2005[14] sets forth minimum requirements for state ID cards and driver's licenses to be accepted by the government for official purposes. The Real ID Act was passed after the 11 September 2001 attacks, which prompted the government to tighten security measures.[15] It has been observed as pushing the U.S. one step closer to a national identification card that requires personal information to be stored in a central database.[16]

In addition, the US Social Security Number has seen an overload of uses, being both a personal identifier and an authentication "secret" (despite not being intended for the purpose).[17] The risks of such use have been discussed in the literature.[18]

---

[14] 119 Stat. 302.

[15] Jessica Dickler, *New ID rules at the airport are pushed back to 2020*, CNBC, Jan. 10, 2018, *at* https://www.cnbc.com/2018/01/10/new-id-rules-at-the-airport-pushed-back-to-2020.html; Debra Milberg, *The National Identification Debate: Real ID and Voter Identification*, 3 ISJLP 443, 449 (2007). "Proponents of REAL ID argue that by adopting the Act, Congress is simply implementing the recommendations of the 9/11 Commission. These proponents claim that the Act was created in response to recommendations made by the 9/11 Commission in an effort to make it more difficult for terrorists and undocumented immigrants to obtain legitimate identification documents and to travel freely around the country."

[16] Milberg, *supra* note 15, at 444, 471.

[17] Martin & Martinovic, *supra* note 12.

[18] Elizabeth Friedheim, *The National ID Card: Privacy Threat or Protection*, 21 J. MARSHALL L. REV. 831, 843-45 (1988). "Fourth, the SSN identifier now ties individual people to a huge number of data banks in federal archives… Fifth, federal use of the national identifier would be problem enough; but this extensive federal use has turned the SSN into a common identifier even in private data banks. Employers, money lenders, agencies that receive federal funds or dispense them and all report to the federal government using the SSN… Sixth, these various data banks exist in an era of rapidly growing computer technology and relatively weak legal controls on the free exchange of information."; at 848 "The SSN is a promiscuous personal identifier which has been having intercourse with every data bank within reach and which has infected all Americans with an incurable invasion of privacy. Americans all have informational herpes."; Lear & Reynolds, *supra* note 4, at 27-8. "The development of the social security number as a national identification number for both military and commercial purposes has created both a privacy and national security nightmare. The statement is especially true for service members effectively required to provide their social security number to enemy forces while a POW."

III. PAST EFFORTS TOWARDS A NATIONAL IDENTIFICATION SYSTEM IN THE PHILIPPINES

A. Presidential Decree No. 278

In 1973, citing national security issues, President Ferdinand Marcos signed Presidential Decree (P.D.) No. 278, which mandated the creation of a "national reference card system." The Decree cited the pressing need for the government to establish a system of positive identification of all Filipino citizens and foreign nationals in the Philippines—one essential to ensuring national security and affording convenience in the transaction of official business with government and private offices and agencies. Among the objectives of such system would be the replacement of all existing identification systems currently prescribed by government agencies to afford convenience to the general public.[19] All Filipino citizens and foreign nationals living in the Philippines were to be assigned a Reference Number for identification; they were also to be issued a National Reference Card.[20] It took President Marcos seven years to create a national identification system committee to implement P.D. 278.[21] However, for undisclosed reasons, the Decree was never fully implemented.[22]

B. Administrative Order No. 308

In 1996, President Fidel Ramos issued Administrative Order (A.O.) No. 308 to establish a "National Computerized Identification Reference System." The *whereas* clauses of the order cited a need to provide Filipino citizens and foreign residents the facility to conveniently transact business with basic service and social security providers and other government instrumentalities, which will require a computerized system to properly and efficiently identify persons seeking basic services on social security and reduce, if not totally eradicate, fraudulent transactions and misrepresentations.[23]

However, in *Ople*,[24] the eponymous senator filed a petition with the Supreme Court, questioning the constitutionality of the order. The Court ultimately granted his petition and invalidated A.O. No. 308.

---

[19] Pres. Dec. No. 278 (1973), pmbl.

[20] *Id.* at items 1 and 2.

[21] Exec. Order No. 630 (1980).

[22] Andre Ria B. Buzeta-Acero, *Towards a National ID System: An Examination of Kilusang Mayo Uno, et al. v. the Director General and Executive Order No. 420*, 51 ATENEO L.J. 149, 152 (2006).

[23] Adm. Order No. 308 (1996).

[24] *Ople*, 293 SCRA 141.

First, the Court ruled that a national ID system may be instituted only by Congress and may not be covered by an administrative order, as it does not merely implement the Administrative Code of 1987. It in effect established a National Computerized Identification Reference System, and as such, it deals with a subject that requires a legislative act.[25]

Second, even assuming legislation was not necessary, the Court ruled that A.O. No. 308 violated the constitutional right to privacy. In the words of the Court, the broadness, vagueness, and overbreadth of A.O. No. 308 "will put our people's right to privacy in clear and present danger."[26] A.O. No. 308 failed to specify what specific biological characteristics and what particular biometrics technology would be used to identify people who will seek its coverage.[27] Furthermore, the indefiniteness of A.O. No. 308 allowed government authorities to store and retrieve information for a purpose other than the identification of the individual through his or her Population Reference Number.[28] A.O. No. 308 likewise failed to detail how the information gathered would be handled, particularly who would control and access the data, under what circumstances, and for what purpose.[29]

---

[25] *Id.* at 152.

[26] *Id.* at 158.

[27] *Id.* at 160. "In the last few decades, technology has progressed at a galloping rate. Some science fiction are now science facts. Today, biometrics is no longer limited to the use of fingerprint to identify an individual. It is a new science that uses various technologies in encoding any and all biological characteristics of an individual for identification. It is noteworthy that A.O. No. 308 does not state what specific biological characteristics and what particular biometrics technology shall be used to identify people who will seek its coverage. Considering the banquet of options available to the implementors of A.O. No. 308, the fear that it threatens the right to privacy of our people is not groundless."

[28] *Id.* at 161. "The potential for misuse of the data to be gathered under A.O. No. 308 cannot be underplayed as the dissenters do. Pursuant to said administrative order, an individual must present his PRN everytime he deals with a government agency to avail of basic services and security. His transactions with the government agency will necessarily be recorded-- whether it be in the computer or in the documentary file of the agency. The individual's file may include his transactions for loan availments, income tax returns, statement of assets and liabilities, reimbursements for medication, hospitalization, etc. The more frequent the use of the PRN, the better the chance of building a huge and formidable information base through the electronic linkage of the files. The data may be gathered for gainful and useful government purposes; but the existence of this vast reservoir of personal information constitutes a covert invitation to misuse, a temptation that may be too great for some of our authorities to resist" (footnotes omitted).

[29] *Id.* at 162. "The lack of proper safeguards in this regard of A.O. No. 308 may interfere with the individual's liberty of abode and travel by enabling authorities to track down his movement; it may also enable unscrupulous persons to access confidential information and circumvent the right against self-incrimination; it may pave the way for 'fishing expeditions' by government authorities and evade the right against unreasonable searches and seizures" (footnote omitted).

Thus, according to *Ople*, a national ID system law must comply with the following requisites:

1. The national ID system law must state what specific biological characteristics and what particular biometrics technology shall be used to identify people who will seek its coverage.

2. The national ID system law must definitely state its purpose in order to avoid potential for misuse.

3. The national ID system law must state in clear and categorical terms how the information gathered shall be handled. It must provide who shall control and access the data, under what circumstances and for what purpose.

The Court explained that these factors are essential to safeguard the privacy of citizens and guarantee the integrity of the information contained in such a system.[30]

C. Executive Order No. 420

In 2005, President Gloria Macapagal Arroyo issued Executive Order (E.O.) No. 420[31] in order to streamline and harmonize the identification systems of all government agencies and government-owned and controlled corporations (GOCCs). Under the Unified Identification System, government agencies will collect the following data: name, home address, sex, picture, signature, date of birth, place of birth, marital status, names of parents, height, weight, two index finger marks and two thumbmarks, any prominent distinguishing features like moles and others, and Tax Identification Number (TIN).[32]

The constitutionality of E.O. No. 420 was eventually questioned in *Kilusang Mayo Uno v. Director-General*.[33] In that case, the petitioners claimed that *first*, E.O. No. 420 is a usurpation of legislative functions; and *second*, it

---

[30] *Id.*

[31] The full title of the Executive Order is "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."

[32] Exec. Order No. 420, § 3.

[33] Kilusang Mayo Uno v. Director-General [hereinafter "Kilusang Mayo Uno"], G.R. No. 167798, April 19, 2006.

infringes on the citizen's right to privacy. The Supreme Court ultimately upheld the constitutionality of said order.

The Court ruled that E.O. No. 420 applies only to government agencies that already have the power to maintain ID systems and issue ID cards. The Court explained that legislation is required for the creation of a government-maintained ID card system in the following cases:

> First, when the implementation of an ID card system requires a special appropriation because there is no existing appropriation for such purpose. Second, when the ID card system is compulsory on all branches of government, including the independent constitutional commissions, as well as compulsory on all citizens whether they have a use for the ID card or not. Third, when the ID card system requires the collection and recording of personal data beyond what is routinely or usually required for such purpose, such that the citizen's right to privacy is infringed.[34]

According to the Court, legislation is not required to carry out E.O. No. 420. *First*, it does not require any special appropriation. *Second*, E.O. No. 420 is neither compulsory on all branches of government, nor is it compulsory on all citizens. *Third*, E.O. No. 420 requires a very narrow and focused collection and recording of personal data, while safeguarding the confidentiality of such data. In fact, the data collected and recorded under E.O. No. 420 is far less than the data collected and recorded under the ID systems existing prior to E.O. No. 420. Therefore, E.O. No. 420 does not in fact establish a national ID card system.[35]

Finally, the Court ruled that E.O. No. 420 does not infringe on the right to privacy. The said order does not bar the adoption of ID systems by government entities; it only applies to government entities that maintain ID systems. E.O. No. 420 even provides safeguards to protect the confidentiality of the data collected.[36] Section 6 of E.O. No. 420 provides:

> The Director-General, National Economic and Development Authority, and the pertinent agencies shall adopt such safeguard as may be necessary and adequate to ensure that the right to privacy of an individual takes precedence over efficient public service delivery. Such safeguards shall, as a minimum, include the following:

---

[34] *Id.*
[35] *Id.*
[36] *Id.*

a. The data to be recorded and stored, which shall be used only for purposes of establishing the identity of a person, shall be limited to those specified in Section 3 of this Executive Order;

b. In no case shall the collection or compilation of other data in violation of a person's right to privacy shall be allowed or tolerated under this order;

c. Stringent systems of access control to data in the identification system shall be instituted;

d. Data collected and stored for this purpose shall be kept and treated as strictly confidential and a personal or written authorization of the Owner shall be required for access and disclosure of data;

e. The identification card to be issued shall be protected by advanced security features and cryptographic technology; and

f. A written request by the Owner of the identification card shall be required for any correction or revision of relevant data, or under such conditions as the participating agency issuing the identification card shall prescribe.[37]

D. Summary: *Ople* vis-à-vis *Kilusang Mayo Uno*

The main difference between the cases of *Ople*[38] and *Kilusang Mayo Uno*[39] is that, in the latter, the executive order in question applies only to government entities that already maintain ID systems and issue ID cards pursuant to their regular functions under existing laws. It does not grant such government entities any power that they do not already possess. In contrast, the assailed executive issuance in *Ople* aimed to create a national ID system that did not exist prior to the enactment of said issuance. Thus, there was a need for new legislation.

However, despite the Court's ruling in *Kilusang Mayo Uno*, the implementation of E.O. No. 420 did not quell the public's uproar. As noted by Buzeta-Acero, the Supreme Court failed to rule on the civil rights issues

---

[37] Exec. Order No. 420 (2005).

[38] Ople v. Torres, G.R. No. 127685, 293 SCRA 141, July 23, 1998.

[39] *Kilusang Mayo Uno*, G.R. No. 167798.

and the many repercussions of having an integrated national identification system, and limited its discussion to the procedural validity of the creation of the executive order.[40]

IV. THE PHILIPPINE IDENTIFICATION SYSTEM

Following multiple attempts at a national ID system by past administrations, R.A. No. 11055 or the "Philippine Identification System Act" finally created the country's single national identification system known as the Philippine Identification System ("PhilSys"). The stated objectives of the Act are: (1) "to provide a valid proof of identity for all citizens and resident aliens as a means of simplifying public and private transactions"; and (2) to be a "social and economic platform which shall serve as the link in the promotion of seamless service delivery, enhancing administrative governance, reducing corruption, strengthening financial inclusion, and promoting ease of doing business."[41] Pilot testing of the system began on September 2, 2019. The full roll out is expected on July 2020 for Filipinos living in the country, while overseas Filipino workers may begin registering by 2021.[42]

A. Legislative History

1. House Bill No. 6221 (Filipino Identification System)

The House of Representatives version of the national ID system law, House Bill No. 6221, proposed the establishment of the Filipino Identification System ("FilSys") requiring Filipino citizens living in the Philippines or abroad, who are at least 18 years old, to obtain a FilSys ID which would contain essential information about the citizen's identity. A Common Reference Number ("CRN") or a unique and permanent identification number would be issued to a citizen registered under the FilSys.[43]

The FilSys ID was proposed to contain at least 35 pieces of information. Ten data entries would appear on the card itself, while 19 data entries would be on the smart chip embedded in the card, and 35 entries

---

[40] Buzeta-Acero, *supra* note 22, at 150 (2006).

[41] Rep. Act No. 11055, § 3.

[42] Ralf Rivas, *All Filipinos can enroll for national ID by mid-2020*, RAPPLER, Sept. 2, 2019, *at* https://www.rappler.com/nation/239141-psa-says-filipinos-can-enroll-for-national-id-2020

[43] H. No. 6221, 17th Cong. 2nd Sess., § 4 ¶ g (2017).

would be kept in a Filipino Citizen Registry, an electronic database, by the Philippine Statistics Authority (PSA).[44]

2. Senate Bill No. 1738 (Philippine Identification System)

In contrast, the Senate version of the bill does not expressly mandate citizens to register and acquire such identification. But similar to the House version, the Senate bill integrates the various government-issued IDs into an official identification system.[45]

3. Bicameral Conference Committee

The bicameral conference committee agreed to adopt the Senate version of the bill after minor changes were made.[46]

B. Key Features

The PhilSys is the government's central identification platform for all citizens and resident aliens of the Philippines. An individual's record in the PhilSys shall be considered an official and sufficient proof of identity.[47] The PhilSys has three key components: the PhilSys Number ("PSN"), Philippine Identification ("PhilID"), and PhilSys Registry. The PSN is a randomly generated, unique, and permanent identification number for every citizen or resident alien upon birth or registration by the PSA.[48]

The PhilID is a non-transferable card that shall preferably be issued to all citizens or resident aliens registered under the PhilSys, subject to the guidelines to be issued by the PSA.[49] The PhilID shall be the physical medium issued to convey essential information about the person's identity, containing on its face the PSN, full name, sex, blood type, marital status (optional), place of birth, a front facing photograph, date of birth, and address of the individual in whose favor it was issued. All information appearing in the PhilID should match the registered information in the PhilSys. The PhilID shall include a QR Code which contains fingerprint information and other security features

---

[44] § 7.

[45] S. No. 1738, §§ 2, 3 (2018).

[46] CNN Philippines Staff, *Senate, House panels approve nat'l ID system bill*, CNN PHIL., May 24, 2018, *at* https://cnnphilippines.com/news/2018/05/24/senate-house-bicameral-conference-national-ID-system.html

[47] Rep. Act No. 11055, § 6.

[48] § 7, ¶ a.

[49] § 7, ¶ c.

to safeguard data privacy and security, and prevent proliferation of fraudulent or falsified identification cards. The PSA in consideration of advances in technology, utility, security, and confidentiality may, subject to appropriate guidelines that shall be issued on the matter, provide citizens or resident aliens with mobile PhilID.[50]

Finally, the PhilSys Registry contains the PSN and registered records and information of all persons registered in the PhilSys. The information on the PhilSys Registry shall be classified in a manner that allows safeguards for data privacy and security, access controls, and change management.[51]

The information to be collected and stored under the PhilSys are demographic data—full name, sex, date of birth, place of birth, blood type, address, Filipino or resident alien, marital status (optional), mobile number (optional), and email address (optional)—and biometric information—a front facing photograph, full set of fingerprints, and iris scan.[52]

One (1) year after the effectivity of the PhilSys Act, every citizen or resident alien shall register personally with the following registration centers that have the necessary facilities to capture the information required to be contained in the Registry:

1. PSA Regional and Provincial Offices;
2. Local Civil Registry Offices (LCROs);
3. Government Service Insurance System (GSIS);
4. Social Security System (SSS);
5. Philippine Health Insurance Corporation (PhilHealth);
6. Home Development Mutual Fund (HDMF);
7. Commission on Elections (COMELEC);
8. Philippine Postal Corporation (PHLPost); and
9. Other government agencies and GOCCs as may be assigned by the PSA. [53]

---

[50] § 7, ¶ c(1).
[51] § 7, ¶ b.
[52] § 8.
[53] § 9.

In the case of Filipino citizens residing abroad, the registration shall be made in the nearest Philippine Embassy or Philippine Foreign Service post, or other registration centers that may be designated by the Department of Foreign Affairs (DFA) in coordination with the PSA.[54]

Under the law, *citizen* refers to a Filipino citizen, as defined in the Constitution, [55] including those with dual or multiple citizenships in accordance with R.A. No. 9225, otherwise known as the "Citizenship Retention and Re-acquisition Act of 2003." [56] *Resident alien* refers to an individual who is not a citizen of the Philippines, but has established residence in the Philippines for an aggregate period of more than 180 days.[57]

C. Support

Supporters claim that the institution of a national ID system will bring about a multitude of benefits. *First*, a national ID system is a necessary tool to improve efficiency in the delivery of government services. *Second*, it may promote financial and social inclusion as previously undocumented individuals may obtain official identification that will give them access to employment opportunities and banking services, among other benefits.[58] *Third*, this system may help prevent crime, terrorism, and fraud. Senator Panfilo Lacson, sponsor of the bill, and former Philippine National Police chief, said the system is a valuable tool in aiding law enforcers as it could help them deter criminality and terrorism by facilitating the processes of apprehension and prosecution.[59] *Finally*, it may aid in ensuring public safety, as citizens can be easily tracked in the event an emergency arises.[60]

---

[54] § 9.

[55] CONST. art. IV, § 1.

[56] Rep. Act No. 11055, § 3, ¶ e.

[57] § 3, ¶ n.

[58] Foundation for Media Alternatives, The National ID Debate: Is the Philippines Ready? (2018), *available at* https://www.fma.ph/wp-content/uploads/2018/02/Briefing-National-ID-3.pdf (last visited Jan. 8, 2020).

[59] Camille Elemia, *Filipinos to have national IDs soon after Senate, House pass bill*, RAPPLER, Mar. 19, 2018, *at* https://www.rappler.com/nation/198503-national-id-system-philippines-implementation-after-senate-house-bill

[60] *See supra* note 58.

D. Opposition

Conversely, those against the national ID system claim that it opens the door to abuse by paving the way for discrimination, state oppression, and surveillance.[61]

During the third reading of the House version of the PhilSys Act, a number of congressmen expressed their misgivings. Anakpawis party-list Representative Ariel Casilao, in explaining his vote against the National ID system, stated that the government seems to be establishing a police state, as what in truth and fact is being established is a system of mass surveillance.[62] Meanwhile, Gabriela party-list Representative Emmi De Jesus objected to the provision which permits the collection of other information determined by participating government agencies in this manner:

> Is this not overly broad to cover everything about the national ID holder while openly breaching the person's right to privacy? This is alarming, especially in the context of the non-stop extrajudicial killings among peasants, political activists, indigenous peoples, and even the current controversial murder of poor Filipinos in the name of the war on drugs. An unlimited expanse of personal data placed in the hands of a regime that relies heavily on dictatorship and fascist methods can only mean intensified surveillance and state profiling, which might even lead to more killings.[63]

Kabataan party-list Representative Sarah Elago expressed a similar sentiment and warned that the establishment of a National ID System could lead to the deterioration of democracy:

> Amid a backdrop of rising impunity and extrajudicial killings, the use of a National ID System to go after government critics and legitimate dissenters is not far-fetched and as such, with its

---

[61] Cesar Garcia, *Past attempts at a national ID system: A battleground of privacy, executive power*, RAPPLER, June 7, 2018, *at* https://www.rappler.com/newsbreak/iq/204341-past-efforts-national-id-system-philippines, *citing* Foundation for Media Alternatives, *supra* note 58.

[62] Congress of the Philippines, Congressional Record - Plenary Proceedings of the 17th Congress, Second Regular Session. Vol. 2, No. 21, at 14 (Sept. 8, 2017), *available at* http://congress.gov.ph/legisdocs/congrec/17th/2nd/17C2RS-VOL2REC21-20170908.pdf

[63] *Id.* at 15.

> unwarranted invasion of our privacy, it will just become an instrument of political persecution and will lead to the further erosion of our Philippine democracy.[64]

Does the PhilSys Act contain measures to address these concerns?

V. ANALYSIS

A. Does the PhilSys Act Comply with *Ople*?

As earlier discussed, the Court, in *Ople*,[65] laid down the following requisites:

1. The national ID system law must state what specific biological characteristics and what particular biometrics technology shall be used to identify people who will seek its coverage.

2. The national ID system law must definitely state its purpose in order to avoid potential for misuse.

3. The national ID system law must state in clear and categorical terms how the information gathered shall be handled. It must provide who shall control and access the data, under what circumstances and for what purpose.

1. Biological Characteristics and Biometric Technology

The PhilSys Act fails the first test. *First*, Section 8(b)(4) contains a catch-all provision, allowing the collection and storage under the PhilSys of, "if necessary, other identifiable features of an individual as may be determined in the implementing rules and regulations (IRR)." While the enumeration in the IRR of data to be collected does not exceed those required under the Act, Section 8(b)(4) empowers the PSA, by merely amending the IRR, to collect additional data in the future.[66] The PhilSys Act provides no standard to guide the PSA in determining what identifiable features would be collected. Even

---

[64] *Id.* at 16.

[65] G.R. No. 127685, 293 SCRA 141(1998).

[66] Both Rep. Act No. 11055, § 8(b) and the Rep. Act No. 11055 Rules & Regs., Rule II, § 7(B) mention as biometric information to be collected: (1) Front Facing Photograph; (2) Full set of fingerprints; (3) Iris scan.

the word "necessary" is not sufficient, since any reason cited by the government can fit the term.

This aspect of the Act fails to meet the sufficient standard test, which requires adequate guidelines or stations in the law to map out the boundaries of the delegate's authority and prevent the delegation from running riot.[67] Thus, the danger that the PhilSys will contain all information to identify a person is not simply an illusion.

This catch-all provision of the PhilSys Act is no different from the vagueness of A.O. No. 308, which was assailed in *Ople*.[68]

Second, the PhilSys Act omits any mention of the particular biometrics technology that would be used to identify people. The PhilSys Act mandates the PSA to issue guidelines and undertake measures to ensure secure, reliable, and efficient authentication of PhilSys records upon the request of authorized government and private entities. Pursuant thereto, the State shall provide for the installation of state-of-the-art biometric machines in all relevant agencies for authentication of data and identity holders.[69] Nothing in the Act prevents the PSA from adopting new and more effective technology, including those for registration, authentication, and data security, taking into consideration the declared principles and objectives of the Act.[70]

It is the IRR that states the technology to be used to identify the individual. For online authentication, the following information will be used to validate the identity of the registered person: (1) PSN and biometric information; (2) PSN and demographic information; and (3) PSN, biometric, and demographic information.

The requesting entity shall choose the suitable mode(s) of authentication, which may involve the use of multiple factors such as, but not limited to, demographic information, biometric information, one-time password ("OTP"), and PhilID, for a particular service or transaction per its requirement. The PSA shall provide guidelines on authentication assurance levels based on international standards and best practices. In exceptional cases to be determined by the PSA, where the PSN cannot be provided, the biometric and demographic information may be used to authenticate the registered person's identity.

---

[67] Eastern Shipping Lines v. Phil. Overseas Emp't Adm., 248 Phil. 762, 772 (1988).
[68] Ople v. Torres, G.R. No. 127685, 293 SCRA 141, July 23, 1998.
[69] Rep. Act No. 11055, § 15, ¶ 1.
[70] § 15, ¶ 3.

For offline authentication, the presentation of the PhillD and the matching of the data stored in the QR code will be used to validate the identity of the registered person for transactions and services, as mentioned under the PhilSys Act. The PhilSys may return a *Yes/No* response or demographic data including photographs, depending on the use case.[71]

Thus, the choice of single or multiple factors depends exclusively on the requesting entity and not to the PSA. The latter does not even have the power to approve, revoke, or review the choice of the requesting entity. The list of options is also not exhaustive. Thus, a requesting entity may choose a password or PIN despite the well-known problems of password theft or guessing. Stronger schemes require a smart card or other token, together with a card reader deployed in every authentication context.[72]

2. Definitely-stated Purposes

The PhilSys Act protects against unlawful disclosure of information or records, subject to certain exceptions.[73] The Act imposes criminal penalties on any person who utilizes the PhilID or PSN in an unlawful manner, or uses the same to commit any fraudulent act, or for other unlawful purpose/s.[74]

However, the Act also fails the second test. Neither the PhilSys Act nor the IRR expressly limit the authorized uses for personal information under the PhilSys to those stated in the PhilSys Act. While Section 18 states that nothing in the Act shall be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law,[75] the Act and the IRR do not even identify the instances where existing law allows the sharing or transfer of any personal data.

---

[71] Rep. Act No. 11055 Rules & Regs., Rule II, § 12.

[72] Martin & Martinovic, *supra* note 12. "Authentication may come from the ID itself, together with a password or PIN, for example. But the problems of password theft and guessing are well-known today, making such authentication unsuitable for high-grade transactions."

[73] Rep. Act No. 11055, § 17. Discussed *infra* regarding the Data Privacy Act requisite of consent by the data subject.

[74] § 19,¶ 2.

[75] § 18,¶ 2.

Thus, the same observation of the Court in *Ople* applies to the PhilSys Act:

> A.O. No. 308 should also raise our antennas for a further look will show that it does not state whether encoding of data is limited to biological information alone for identification purposes. In fact, the Solicitor General claims that the adoption of the Identification Reference System will contribute to the "generation of population data for development planning." This is an admission that the PRN will not be used solely for identification but for the generation of other data with remote relation to the avowed purposes of A.O. No. 308.[76]

In fact, the PhilSys Act expressly allows the PSA to use all data it collates under the PhilSys to generate aggregate data or statistical summaries without reference to or identification of any specific individual.[77]

Without legislative scrutiny, the PSA may expand the uses of the PSN and the PhilID simply by amending the IRR. This situation has already happened with identification numbers initially intended only for a specific purpose: the Social Security number in the United States[78] and the Tax File Number in Australia.[79] Computerized data systems have always been adopted for purposes other than their originally intended use.[80] Although it is not

---

[76] *Ople*, 293 SCRA at 160.

[77] Rep. Act No. 11055, § 18,¶ 2.

[78] *See* John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 996 (1984). "The increasing use by many agencies of the social security number, originally intended to be used solely in administering the social security system, made cross-indexing among various systems relatively easy. The merger of these apparently separate personal record systems has therefore become possible without the creation of physically centralized records." *See also* Lear & Reynolds, *supra* note 4, at 1.

[79] *See* Roger Clarke, *The Resistible Rise of the National Personal Data System*, 5 SOFTWARE L.J. 29, 43 (1992). "The only organisation authorised [sic] to use the TFN in relation to taxation matters was the Australian Taxation Office (ATO), although employers, investment bodies, superannuation funds and tax agents were required to collect, store, and report it to the ATO. However, there were several ways- in which the TFN scheme was automatically much broader than had been understood by the public, and by many of the people who were involved in the discussions preceding Parliamentary approval"; at 44 "The scope of taxation law was, therefore, readily expandable both by administrative action of the Government (i.e., without the purview of Parliament), and by the inclusion in a new Government Bill of a simple machinery provision unlikely to attract careful scrutiny by Parliament."

[80] Shattuck, *supra* note 78, at 1000; *See also* Friedheim, *supra* note 18, at 843 (1988). "[T]he SSN identifier now ties individual people to a huge number of data banks in federal archives. Originally, the SSN identified people for the Social Security Administration.", at 844 "[T]his extensive federal use has turned the SSN into a common identifier even in private data banks."

mandatory *de jure*, the use of the PhilID may cover all aspects of life, thus making its possession *de facto* mandatory. Rights and benefits can be denied to people simply because they do not have PhilIDs.[81] The PhilSys may become a vehicle to enhance control of individuals' lives by public and private agencies.[82]

Notably, the PhilSys replaces all other government-issued IDs. One of the objectives of the PhilSys Act is to eliminate the need to present other forms of identification when transacting with the government and the private sector.[83] The PhilID shall serve as *the* official government-issued identification document of cardholders in dealing with all national government agencies, local government units (LGUs), GOCCs, government financial institutions (GFIs), and all private sector entities.[84]

In *Ople*,[85] the Court observed that despite the argument of the dissenters that A.O. No. 308 confers no right, imposes no duty, affords no protection, and creates no office, under such regulation, "a citizen cannot transact business with government agencies delivering basic services to the people without the contemplated identification card. No citizen will refuse to get this identification card for no one can avoid dealing with the government. It is thus clear as daylight that without the ID, a citizen will have difficulty exercising his rights and enjoying his privileges."[86] The lack of a provision expressly limiting the uses of the PhilSys to those stated in the PhilSys Act has this same effect.

---

[81] *See* Clarke, *supra* note 79, at 45. "Specifically, the sanction was that taxation would be deducted from wages or interest income at the highest marginal rate (about fifty cents on the dollar). However, in December 1989, only one year after the original legislation had been passed, amendments to the Social Services Act made the quotation of the TFN a precondition to the payment of unemployment and sickness benefits."

[82] Shattuck, *supra* note 78, at 992-3. "The card, backed by a national databank of personal information concerning all persons lawfully in the United States, would constitute a secure national identification system that could block the employment of illegal aliens. The proposal has sparked controversy because the identification system could become a vehicle for the violation of civil rights if used by the police to conduct wide-ranging searches and investigations or by other government agencies to keep track of private, law-abiding citizens," "Nonetheless, these high technology systems are also being used at an increasing rate by large public and private agencies to enhance their control of the lives of individuals."

[83] Rep. Act No. 11055, § 3(1).

[84] Rep. Act No. 11055, § 7(c)(2); Rep. Act No. 11055 Rules & Regs., Rule II, § 6(C)(2) adds "State Universities and Colleges."

[85] Ople v. Torres, G.R. No. 127685, 293 SCRA 141, July 23, 1998.

[86] Martin & Martinovic, *supra* note 12. "Is use of the ID scheme compulsory for every citizen and in every circumstance? If so, this maximises the utility of the scheme, but possibly compromises the privacy of the individual and thus may invoke resistance (more so in some countries than others."

True, under the PhilSys Act, proof of identity shall not necessarily be construed as proof of eligibility to avail of certain benefits and services which shall be determined based on applicable rules and regulations of the government authorities or agencies concerned.[87] But what constitutes proof of identity to begin with? If the PhilSys replaces all other government IDs, then only the PhilID or PSN can serve as proof of identity. If an individual has neither, then he or she has no proof of identity. If there is no proof of identity, the question of eligibility for certain benefits or services cannot even be entertained.

Nothing in the PhilSys Act and its IRR stops computer-matching, or the use of unrelated computer tapes of massive numbers of personal files to conduct government or corporate investigations. Computer-matching erodes the constitutional rights against unreasonable searches and seizure, to be presumed innocent, to privacy, and to due process of law.[88] If the PhilID becomes the only proper identification, then loss of the card would leave anyone stopped by the police vulnerable to an extensive personal search.[89] The Constitution, as presently interpreted, would also allow the government to use information found during such a search in a criminal prosecution against the search victim.[90]

The PhilSys Act requires all government agencies, including GOCCs, to incorporate in their identification systems and databases the PSN of covered individuals, which shall be the standard number for such individuals across all agencies of the government.[91] Notably, the PhilSys Act and the IRR do not expressly prohibit the maintenance of one database containing not only PhilSys information, but also all transactions of an individual across both government agencies and the private sector.[92] Thus, this standard number allows building a database of both personal information and of transactions with an individual across all government agencies and even private entities. This facilitates, in turn, the forming of a profile of an individual based on their

---

[87] Rep. Act No. 11055, § 14.

[88] Shattuck, *supra* note 78, at 1002-4.

[89] Friedheim, *supra* note 18, *citing* Terry v. Ohio, 392 U.S. 1 (1968) and WAYNE LAFAVE, 3 SEARCH AND SEIZURE §§ 9.1-9.6 (1978 & Supp. 1985). Details the development of the Terry search with numerous citations. The Philippine Supreme Court has adopted *Terry* since its ruling in Manalili v. Ct. of Appeals, 345 Phil. 632, 636 (1997).

[90] Friedheim, *supra* note 18, 841.

[91] Rep. Act No. 11055, §7, (a).

[92] *See also* Martin & Martinovic, *supra* note 12. "Moreover, the ID card system keeps aspects of an individual's data independent from other actors' data. Citizens associated with their employers can transact and sign documents commercially using a personal identity."

transactions with the government. The database may also be coupled with GPS or RFID technology to track individuals.[93] Nothing in the PhilSys Act and the IRR expressly state that surveillance is an unauthorized use of the PhilSys.

The PSA may, by administrative regulation, allow the use of the PSN or PhilID as digital signatures for documents. However, in the case of a severe privacy attack, the PSN or PhilID may be abused in that a digital signature procured for the purpose of authentication could later be used to falsify an individual's consent.[94]

Another cause of concern is Section 13, which may also be construed as a catch-all provision:

> The PhilID shall be honored and accepted, subject to authentication, *in all transactions requiring proof or verification of citizens or resident aliens' identity*, such as, but not limited to:
>
> (a) Application for eligibility and access to social welfare and benefits granted by the government;
>
> (b) Application for services and benefits offered by GSIS, SSS, PhilHealth, HDMF, and other government agencies;
>
> (c) Applications for passports and driver's license;
>
> (d) Tax-related transactions;
>
> (e) Registration and voting identification purposes;
>
> (f) Admission to any government hospital, health center or similar institution;
>
> (g) All other government transactions;
>
> (h) Application for admission in schools, colleges, learning institutions and universities, whether public or private;
>
> (i) Application and transaction for employment purpose;

---

[93] Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475 (2013).

[94] Martin & Martinovic, *supra* note 12. "[I]t is wise to separate the cryptography used for authentication from the cryptography used for signing. Otherwise, in a severe attack, the former could be used to achieve the latter without the citizen's consent."

> (j) Opening of bank accounts and other transactions with banks and other financial institutions;
> (k) Verification of cardholder's criminal records and clearances;
>
> (l) *Such other transactions, uses or purposes, as may be defined in the IRR.*
>
> The PSN and biometrics of an individual, as authenticated through the PhilSys, shall be honored and accepted, notwithstanding the absence or non-presentation of a PhilID.[95]

The IRR is just as all-encompassing, providing for: "other transactions requiring proof of identity."[96]

A national ID system with unlimited purposes has the unfortunate effect of stifling democracy. As early as 1970, Ralph Nader warned that data banks are a subtle kind of blackmail because their existence inhibits people and prevents them from speaking out and blowing the whistle against the system.[97]

3. How Information Shall Be Handled

Lastly, the PhilSys Act fails the third test. The IRR simply states that the PSA shall designate a separate Data Protection Officer for the PhilSys; that the PSA shall ensure that applicants are adequately informed upon registration in the PhilSys on how their data will be used, and how they can access their registered information and record history; and that all applicable rights of the registered person shall be upheld.[98] The IRR does not state the manner by which applicants are to be informed, nor is the term "adequately informed" defined. Neither does the IRR define the applicable rights of the registered person. Are the rights of a data subject under the Data Privacy Act applicable? This matter is further discussed below.

Even if applicants are informed, they can never be completely informed, because the circumstances and the purposes for which their personal information is to be used are open-ended, as discussed in the second test.

---

[95] Rep. Act No. 11055, §13(*l*). (Emphasis supplied.)

[96] Rep. Act No. 11055 Rules & Regs., Rule III, § 13(m).

[97] Lacey Fosburgh, *Nader Fears Computer Will Turn Us Into Slaves*, NEW YORK TIMES, Sept. 2, 1970, at 18, *available at* https://www.nytimes.com/1970/09/02/archives/nader-fears-computer-will-turn-us-into-slaves.html

[98] Rep. Act No. 11055 Rules & Regs., Rule V, § 22.

4. Summary

The PhilSys Act fails all three requisites set by the Court in *Ople*. Although it is a legislative measure, it is no different content-wise from A.O. No. 308, which was struck down by the Court in that case.[99]

B. Does the PhilSys Act Contain Data Privacy Protections Consistent with the Data Privacy Act?

The law on data privacy in the Philippines is R.A. No. 10173 or the "Data Privacy Act of 2012" (DPA). Under such Act, the processing of personal information shall be allowed, "subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality."[100]

There are two ways in which the provisions of the DPA apply to the PhilSys established under the PhilSys Act. *First*, the DPA applies automatically. *Second*, the DPA provisions are contained in the PhilSys Act.

1. Does the Data Privacy Act Apply Automatically?

It may seem that the DPA applies automatically to the PhilSys. *First*, the repealing clause of the PhilSys Act expressly excludes the DPA from its coverage.[101] *Second*, the Supreme Court adheres to the doctrine that the legislature should be presumed to have known the existing laws on the subject and not have enacted conflicting statutes. Hence, all doubts must be resolved against any implied repeal, and all efforts should be exerted in order to harmonize and give effect to all laws on the subject.[102] *Third*, the IRR of the PhilSys Act states that all applicable rights of the registered person shall be upheld.[103]

---

[99] *Ople*, 293 SCRA 141.

[100] Rep. Act No. 10173, § 11.

[101] § 25. "All laws, except Republic Act No. 10173, decrees, orders, rules, and regulations, which are inconsistent with the provisions of this Act, are hereby repealed or modified accordingly."

[102] *In re* Matter of Application for the Issuance of a Writ of Habeas Corpus Richard Brian Thornton for and in Behalf of the Minor Child Sequeira Jennifer Delle Francisco Thornton, 436 SCRA 551, G.R. No. 154598, August 16, 2004.

[103] Rep. Act No. 11055 Rules & Regs., Rule V, § 22.

However, it is more likely that the DPA does not apply automatically to the PhilSys. *First*, both the PhilSys Act and the IRR are silent regarding the applicability of the DPA to the PhilSys, even if only suppletory. The IRR does not even state what the applicable rights of the registered person that would be upheld are.[104] While the PhilSys Act did not repeal the DPA, the former does not expressly state that the latter applies to the PhilSys. *Second*, the DPA itself exempts from its scope information necessary in order to carry out the functions of public authority.[105] *Lastly*, the IRR of the PhilSys Act lumps together the terms "personal information" and "sensitive personal information,"[106] suggesting that they are to be treated in the same manner. In contrast, under the DPA, the processing of personal information is permitted only if not otherwise prohibited by law, and when at least one of the conditions enumerated in the DPA exists.[107] Meanwhile, the processing of sensitive personal information is generally prohibited, subject to certain exceptions.[108]

2. Does the PhilSys Act Contain the Same Safeguards as the Data Privacy Act?

The fact that the DPA does not automatically apply to the PhilSys does not prevent Congress from including the same protections under the former to the latter's governing law. However, it appears from the PhilSys Act that Congress did not do so.

i. Requisite of Consent

To reiterate, under the DPA, the processing of personal information is permitted only if not otherwise prohibited by law and when at least one of the conditions enumerated in the DPA exists. One of these conditions is when

---

[104] *Id.*

[105] Rep. Act No. 10173, § 4(e). "Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA)."

[106] Rep. Act No. 11055 Rules & Regs., Rule I, § 4(h). "[...] For purposes of this Act, personal information includes sensitive personal information, as defined under the Data Privacy Act of 2012."

[107] Rep. Act No. 10173, §12.

[108] § 13.

the data subject has given his or her consent.[109] On the other hand, the processing of sensitive personal information is generally prohibited, except when the data subject has given his or her consent.[110] Processing under the DPA includes collection and recording of information.[111]

Meanwhile, the PhilSys Act is silent regarding the requisite of consent of any individual before the collection and recording of his or her personal information in the PhilSys. The PhilSys Act speaks of consent only in two instances: *first*, as a prerequisite to authentication;[112] and *second*, as an exception to unlawful disclosure. [113] In these instances, an individual's personal information is already present in the PhilSys. Notably, the PhilSys Act requires the PSA to ensure that individuals are adequately informed upon, and not before, registration for the PhilSys.[114]

The fact that an individual's consent is not required before the submission of his or her personal information in the PhilSys is supported by the provision in the IRR which states:

> *Persons incapacitated to give consent under Article 1327 of the Civil Code (minors, insane or demented persons and deaf-mutes who do not know how to write)* shall be accompanied by their parent/s or legal guardian/s who must be of legal age *during registration.* In default or absence of any parent of legal age, the person exercising substitute parental authority as provided in Article 216 of the Family Code shall accompany the minor during registration.[115]

---

[109] § 12.

[110] § 13.

[111] § 3(j).

[112] Rep. Act No. 11055, § 12(3). "Any requesting entity shall obtain the consent of an individual before collecting his or her identity information for the purposes of authentication. It shall inform the individual submitting his or her identity information the following details, namely: (a) the nature of the information that may be shared upon authentication, and (b) the uses to which the information received during authentication may be put by the requesting entity: Provided, That the information requested shall only be used for the purpose for which it was requested."

[113] §17. "No person may disclose, collect, record, convey, disseminate, publish, or use any information of registered persons with the PhilSys, give access thereto or give copies thereof to third parties or entities, including law enforcement agencies, national security agencies, or units of the Armed Forces of the Philippines (AFP), except in the following circumstances: (a) When the registered person has given his or her consent, specific to the purpose prior to the processing."

[114] § 18(1).

[115] Rep. Act No. 11055 Rules & Regs., § 8(a). (Emphasis supplied.)

Therefore, the impression is that a person must submit his personal information to the PhilSys, whether or not he wants to. This conclusion is supported by the discussion earlier that the purposes of the PhilSys are not definitely stated. Thus, if people want to avail of any right or benefit under existing laws, they have no choice but to register under the PhilSys and get PhilIDs.

ii. Right to Be Informed

The DPA states that the data subject shall have the right to be informed of whether personal information pertaining to him or her was, is, or will be processed, and to be furnished certain information before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity.[116]

The PhilSys Act does not contain any provision requiring that the individual concerned be informed of the processing of personal information pertaining to him or her. The right to be informed of such is vital, because the purposes of personal information under the PhilSys are not definitely stated, as defined earlier.

The PhilSys Act itself provides information on the description of the personal information to be entered into the system,[117] and the purposes for which they are being or are to be processed, even if not definitely stated,[118] before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. After all, ignorance of the law excuses no one from compliance therewith.[119] The PhilSys Act states that the PSA shall ensure that individuals are adequately informed upon registration for PhilSys on how their data will be used.[120]

However, the PhilSys Act does not provide information on scope and method of the personal information processing, the recipients or classes of recipients to whom they are or may be disclosed, methods utilized for automated access, if the same is allowed by the data subject and the extent to which such access is authorized, the identity and contact details of the personal information controller or its representative, the period for which the information will be stored, the existence of their rights (i.e. to access,

---

116 Rep. Act No. 10173, §16(a),(b).
117 Rep. Act No. 11055, § 8.
118 Discussed *supra*.
119 CIVIL CODE, art. 3.
120 Rep. Act No. 11055, § 18(1).

correction as well as the right to lodge a complaint before the National Privacy Commission), which are all required by the DPA.[121]

iii. Right to Access

The DPA assures the data subject reasonable access to, upon demand, the following information:

1. Contents of his or her personal information that were processed;

2. Sources from which personal information were obtained;

3. Names and addresses of recipients of the personal information;

4. Manner by which such data were processed;

5. Reasons for the disclosure of the personal information to recipients;

6. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

7. Date when his or her personal information concerning the data subject were last accessed and modified; and

8. The designation, or name or identity and address of the personal information controller.[122]

The PhilSys Act states that the PSA shall ensure that individuals are adequately informed upon registration for PhilSys on how they can access their registered information and record history.[123] The record history consists of the following:

1. Date of filing of the application for registration and the particulars thereof;

2. Date of filing of every application for modification and the particulars thereof;

---

[121] Rep. Act No. 10173, § 16(b).
[122] § 16(c).
[123] Rep. Act No. 11055, § 18(1).

3. Modification of entry made, the date such modification was made, and the document/s or other proof submitted in support thereof;

4. Reason for the omission of any entry;

5. Dates of issuance, reissuance, and cancellation of the PhilID, and including the reasons therefor;

6. Details of authentication requests processed by the Philippine Statistics Authority (PSA), including the date the request was made and processed, the requesting entity, and the response provided by PhilSys;

7. Disclosure, conveyance, dissemination, publication and use of information by third parties; and

8. Other relevant information regarding the registration, modification, and authentication of personal information of a citizen or resident alien under the PhilSys Act.[124]

However, the PhilSys Act does not assure access to the information above. Unlike the DPA, which states that the data subject shall have access to the listed information upon demand, the PhilSys Act does not give a timeframe with which the PSA must provide to the individual concerned such information. The IRR states that registered persons may request, not demand, the PSA to provide access to their own registered information and record history, subject to the guidelines and regulations to be issued by the PSA, without even detailing what these guidelines and regulations are.[125]

iv. Right to Dispute Inaccuracy or Error

The DPA states that the data subject shall be entitled to dispute the inaccuracy or error in the personal information given and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable.[126]

The PhilSys Act not only grants the right but requires citizens or resident aliens to update their registration information in the manner to be specified by the PSA.[127] However, unlike the DPA, the PhilSys Act does not

---

[124] § 5(i).
[125] Rep. Act No. 11055 Rules & Regs., Rule V, § 21(5).
[126] Rep. Act No. 10173, § 16(d).
[127] Rep. Act No. 11055, § 11.

require the personal information controller to ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof. Nor does the PhilSys Act require that the third parties who have previously received such processed personal information be informed of its inaccuracy and its rectification upon reasonable request of the data subject.[128]

v. Other Rights of a Data Subject

The PhilSys Act is silent as regards the following rights ensured by the DPA:

1. Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information;[129]

2. Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information;[130]

3. Where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format,

---

[128] Rep. Act No. 10173, § 16(d). *See also* Martin & Martinovic, *supra* note 12. "Concretely, the Estonian Personal Data Protection Act, the Public Information Act, and the Electronic Communication Act assist in protecting individuals' constitutional rights, which in this context include the right to obtain information about the activities of public authorities; the right to inviolability of private and family life in the use of personal data; and the right to access data gathered in regard to oneself. Together with the national ID system, this legal framework allows Estonians to trace who accesses their data, when, and for what purposes. For example, it is possible to see which doctors have accessed one's personal data, or if policemen access data illegitimately (e.g., for personal reasons)."

[129] Rep. Act No. 10173, § 16(e).

[130] § 16(f).

which is commonly used and allows for further use by the data subject.[131]

4. To lodge a complaint before the Commission.[132]

Notably, the PhilSys Act does not provide whether an individual has the right to have his personal information deleted from the PhilSys. Nor does it require the deletion of personal information of an individual who has died, of a citizen who loses Philippine citizenship, or a resident alien who has ceased to reside in the Philippines. The IRR only speaks of deactivation of the PSN.[133] Thus, the PhilSys contains, perhaps perpetually, details of an individual.

The PhilSys Act also does not provide for the deletion of personal information to be replaced after updating or recapturing such information. Thus, an individual's information in the PhilSys may contain his previous addresses and biometrics.

In addition, the IRR requires that for children below five years old, their PSN shall be linked to that of their parent or guardian.[134] However, the IRR does not state how long the link shall last.

Since the purposes of the PhilSys are not definitely-stated, all this information may allow the PSA or any government agency to build a profile of any individual, together with his or her familial relationships and transactions.

vi. Security

The PhilSys Act mandates the PSA, with the technical assistance of the Department of Information and Communications Technology, to implement reasonable and appropriate organizational, technical, and physical security measures to ensure that the information gathered for the PhilSys, including information stored in the PhilSys Registry, is protected from unauthorized access, use, disclosure, and against accidental or intentional loss, destruction, or damage.[135] This provision is a repetition of the DPA.[136] However, the PhilSys fails to include the other provisions in Chapter V to VII

---

[131] § 18.
[132] § 16(b)(8).
[133] Rep. Act No. 11055 Rules & Regs., § 9(A)(2)(6).
[134] § 8(A)(6).
[135] Rep. Act No. 11055, § 18(1).
[136] Rep. Act No. 10173, § 20(a).

of the DPA on the security of personal information, accountability for transfer of personal information, and security of sensitive personal information in government. On this last point, the IRR of the PhilSys Act lumps together personal information and sensitive personal information.[137]

vii. Summary

In its entirety, not only does the DPA not automatically apply to the PhilSys, the PhilSys law also does not contain many of the guarantees required by the DPA.

C. Does the PhilSys Act Address Other Concerns in the Literature?

A concern in existing literature is the ability to extract personal information from the national ID number. Hence, there is a preference for a unique randomly-generated number over a name or a number based on date of birth, even if the latter is easy to remember.[138] Unique identifiers also ensure that where records are linked, this is done accurately.[139]

The PhilSys Act provides that the PSN is a randomly generated, unique, and permanent identification number that will be assigned by the PSA to every citizen or resident alien upon birth or registration.[140] The IRR adds that the PSN shall not be pre-determined or pre-assigned to any individual. Neither shall any individual be allowed to choose his or her PSN or have more than one PSN.[141] Thus, a third party would not be able to easily guess or reconstruct the PSN from limited information about the holder, such as his date of birth.

---

[137] Rep. Act No. 11055 Rules & Regs., Rule I, § 4(h).

[138] Martin & Martinovic, *supra* note 12. "Conversely, the inclusion of the date of birth within the ID has proved problematic for reasons of privacy, because it tends to make it desirable to move the ID from the 'non-secret' to the 'secret' category. If there is little randomness (entropy) within the ID, a third party can easily guess or reconstruct the ID from limited information about the holder; hence the ID is effectively in the 'published' category."

[139] *Id.* "Unique identifiers enhance transparency in a different sense; they help to ensure that where records are linked, this is done accurately, whereas in matches involving the use of a name, the linking will necessarily be imprecise, raising the possibility that the wrong record will be accessed by accident."

[140] Rep. Act No. 11055, § 7(a).

[141] Rep. Act No Rules & Regs. 11055, Rule II, § 6(A).

D. Proposing a Legal Privacy Framework for the PhilSys

Whether the Philippines should adopt a national ID system is a moot question with the passage and effectivity of the PhilSys Act. Pilot test registration has already begun, with the mass roll-out scheduled for mid-2020. The PSA intends to enroll all Filipinos and resident aliens to the PhilSys by the end of 2022.

The least that the government can do is to ensure that the PhilSys adheres to the people's right to privacy. The DPA implements this constitutionally-guaranteed right. Thus, the provisions of the DPA should be expressly made applicable to the PhilSys. Congress need not amend the PhilSys Act to achieve this. The PSA may simply amend the IRR of the PhilSys Act to conform to the provisions of the DPA, to ensure swift protection. Of course, Congress may likewise choose to amend the law itself.

The amendment should not simply state that the DPA applies to the PhilSys, such an amendment must also tailor-fit the provisions of the DPA to the peculiarities of the PhilSys Act. Therefore, the IRR must be amended to include the following, concerning the individual citizen or resident alien:

1. The individual concerned must consent to the inclusion of his or her personal information to the PhilSys. His or her consent must come before such inclusion, and must be informed. He shall have the right to be informed whether personal information pertaining to him or her shall be, are being or have been processed and to be furnished certain information before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity.
2. The individual must be provided information on scope and method of the personal information processing, the recipients or classes of recipients to whom they are or may be disclosed, methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, the identity and contact details of the personal information controller or its representative, the period for which the information will be stored; and the existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the National Privacy Commission.

3. The individual must have reasonable access upon demand, not just request, to his or her personal information and record history. The guidelines should be clear and easy to follow. Although the inclusion of record history in the PhilSys has been criticized as it would open the door for surveillance,[142] the DPA requires that the data subject be granted access to such record history. Thus, the individual and only the individual should have access to his or her record history and only his or her own, and not of other persons.
4. The personal information controller must ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof. Third parties who have previously received such processed personal information must also be informed of its inaccuracy and its rectification upon reasonable request of the data subject.
5. The individual must have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.
6. The individual must be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information;
7. Where personal information is processed by electronic means and in a structured and commonly used format, the individual must have the right to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the individual;
8. The individual must have the right to lodge a complaint before the Commission.
9. The individual's personal information must be deleted from the PhilSys upon notice of his or her death.

---

[142] Jodesz Gavilan, *'Record history' casts cloud of doubt on proposed national ID system*, RAPPLER, June 12, 2018, *at* https://www.rappler.com/newsbreak/in-depth/204229-record-history-proposed-national-id-system-philippines (last updated Aug. 6, 2018).

10. The PhilSys must adhere to the other provisions on Chapter V to VII of the DPA, on the security of personal information, accountability for transfer of personal information, and security of sensitive personal information in government.

The amendment must also include the following security safeguards, which shall apply not only to the PSA but to any entity—government or private—handling the PhilSys or personal information from such system:

1. The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.[143]
2. The determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the National Privacy Commission may issue from time to time, the measures implemented must include:
   2.1. Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
   2.2. A security policy with respect to the processing of personal information;
   2.3. A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
   2.4. Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.[144]
3. The personal information controller must further ensure that third parties processing personal information on its behalf

[143] Rep. Act No. 10173, § 20(b).
[144] § 20(c).

shall implement the security measures required by this provision.[145]

4. The employees, agents or representatives of the personal information controller involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.[146]
5. The personal information controller shall promptly notify the National Privacy Commission and affected individual when personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (but such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[147]
6. The personal information controller is responsible for personal information under its control or custody, including information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.
   6.1.1. The personal information controller is accountable for complying with these requirements and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.
   6.1.2. The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with the DPA. The identity

[145] § 20(d).
[146] § 20(e).
[147] § 20(f).

of the individual(s) so designated shall be made known to any data subject upon request.[148]

7. All personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.[149]
8. Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.[150]
    8.1. Unless otherwise provided in guidelines to be issued by the Commission, personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:[151]
        8.1.1. In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;[152]
        8.1.2. If a request is approved, the head of the agency shall limit the access to not more than 1,000 records at a time; and[153]
        8.1.3. Any technology used to store, transport or access personal information for purposes of off-

[148] § 21.
[149] § 22.
[150] § 23(a).
[151] § 23(b).
[152] § 23(b)(1).
[153] § 23(b)(2).

site access approved shall be secured by the use of the most secure encryption standard recognized by the Commission.[154]

9. In entering into any contract that may involve accessing or requiring personal information, the personal information controller shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with the DPA and to comply with the other provisions of the DPA, in the same manner as agencies and government employees comply with such requirements.[155]

The protections of the DPA are not enough. The PhilSys is not just any regular database but a database of all citizens and resident aliens in the Philippines. The PhilSys is a national ID system, and thus, it must comply with the requisites laid down by the Supreme Court in *Ople*.[156]

The PhilSys Act must delete the catch-all provision on "if necessary, other identifiable features of an individual as may be determined in the implementing rules and regulations (IRR)."[157] The PhilSys Act does not cite any real need for biometric information other than a front facing photograph, a full set of fingerprints, and an iris scan already stated in the law.[158]

Congress must amend the PhilSys Act to expressly state that the purposes of the PhilSys are limited to those stated in such Act. The PhilSys Act must also enumerate the instances under existing laws when sharing or transfer of personal information is allowed. These changes will ensure that the purposes of the PhilSys are definitely stated and will keep the system from expanding and running riot behind the back of citizens and resident aliens.

The PhilSys Act must expressly state how the PSA shall handle and secure the PhilSys by, at the very least, embracing the security provisions embodied in the DPA. The PSA must also explain to the public the security features to which the PhilSys is subject to, without giving too much information which would lead to unauthorized access. The PSA must ensure the protection of personal information that does not belong to the requesting

---

154 § 23(b)(3).
155 § 24.
156 *Ople*, 293 SCRA 141.
157 Rep. Act No. 11055, § 8(b)(4).
158 § 8(b)(1), (2), (3).

individual. Further, the choice of authentication methods should be limited to the PSA and not to the requesting entity, or must at least require PSA approval.

It is desirable that the technologies for security and authentication be expressly stated in the PhilSys Act. However, technologies evolve faster compared to changes in the law. A counter-argument is that the Act should expressly state stable, tried-and-tested technologies to assure the privacy of personal information contained in the PhilSys. Such technologies should be preferred over emerging but untested technologies. Ultimately, a tradeoff between privacy and efficiency must be made in any amendment to the law.

VI. CONCLUSION

The Philippines has crossed the Rubicon with the adoption of the PhilSys Act, setting in motion the decades-long dream for a national identification system. The aims of such a system are laudable.

However, the road to hell is paved with good intentions. The PhilSys Act and its implementing rules and regulations do not comply with sufficient privacy guarantees laid down by the Supreme Court in jurisprudence and those contained in the DPA. These safeguards uphold the data privacy principles of transparency, legitimacy of purpose, and proportionality. The fact that the PhilSys is a national ID system is no reason to do away with these measures. Otherwise, the enormity of personal information to be contained in the PhilSys coupled with lack of limitations is bound to turn the government into Big Brother, sooner or later.

A legal framework that embraces both is a first step towards avoiding a data breach similar to what happened with the COMELEC's voters' database in 2016. However, a legal framework can only go so far. An attitudinal shift towards upholding such framework is required. The government cannot allow another leak to happen, especially from a system as encompassing as the PhilSys. The government must also restrain itself from going beyond the objectives of the PhilSys Act, and must resist temptations to expand the system to cover any conceivable purpose.

Thus, the legal framework must encourage a culture of privacy, not just in the government to whom personal information would be entrusted or in the private sector which may have access to the PhilSys for the purpose of authentication, but also among citizens who hopefully become alert about sharing their personal information and monitoring how such are used.

Otherwise, the constitutionally-guaranteed right to privacy would be all for naught. Absent vigilance, the national ID system may become the lynchpin of a police state, just like East Germany and Romania of the past, and China and North Korea of today.

As Ralph Nader said in 1970, which remains relevant half a century later, "The key democratic principle of man's control over his life is being abused. And unless we do something about it, we're suddenly going to wake up and realize we're a nation of slaves."[159]

- o0o -

[159] Fosburgh, *supra* note 97.