# Data Privacy Act

*Deputy Commissioner Ivy D. Patdu* [*]
*Atty. Rasiele Rebekah DL. Rellosa* [**]

## I. Introduction

It is of popular view that the Data Privacy Act of 2012 was intended to support the Business Process Outsourcing (BPO) industry, complementing other incentives intended to attract foreign investment. The BPO industry, coined as the "Sunshine industry,"[1] is accepted as a significant contributor to the Philippine economy, demonstrating its capability to generate jobs and increase Gross Domestic Product. The law is touted as a measure to "boost confidence in both the country's booming Information Technology and Business Process Outsourcing (IT-BPO) industry and growing e-governance initiatives."[2] This should not, however, be taken to mean that the law exists principally for the BPO industry, because the collection, use, and storage of personal data of individuals is not confined to any particular industry. In fact, one of the biggest repository of personal data is the government, and the law accordingly provides specific obligations for government agencies.[3] The Data Privacy Act of the Philippines, as opposed to data protection laws in some jurisdictions, covers both public and private sector.

It bears emphasis that the Data Privacy Act should never be considered as catering primarily to interests of the business sector or government agencies because at its core is the obligation to protect the data privacy rights of individuals whose personal data are collected, used, stored, or otherwise processed.[4] The law itself orders that "any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed."[5] The individual or the data subject[6] should be acknowledged as the nucleus of the law, because more than being just legislation to support certain industries or promote innovation and economic growth, the Data Privacy Act is legislation for human rights.

---

[*] '02 M.D., University of the Philippines; '09 J.D. Ateneo de Manila University School of Law; The author is the Deputy Privacy Commissioner of the National Privacy Commission and is currently teaching Legal Medicine in the San Beda College of Law-Alabang. She worked with the National Telehealth Center and the Health Privacy Group of the Department of Health, assisting in the development of the Privacy Guidelines for the Philippine Health Information Exchange. Her previous works include Recommendations for Social Media Use in Hospitals and Health Care Facilities, 31 PJO-HNS 1 (2016); Health Information Privacy in the Philippines: Implications for Policy and Practice (Antonio, Patdu, Marcelo), Privacy in the Developing World—Philippines Monograph Series 04/2013.

[**] '10 B.S in Development Communication, Major in Educational Communication (Cum Laude), University of the Philippines LB; '14 J.D., Ateneo de Manila University School of Law; The author is currently working in the Privacy Policy Office of the National Privacy Commission.

[1] BPO Industry: Philippine's Sunshine Industry available at http://www.outbounders.tv/bpo-industry-philippines-sunshine-industry/ (last accessed Dec. 26, 2016).

[2] Press Release, *Data Privacy Act Approved, Press Freedom Protected* (June 9, 2012) available at http://www.senate.gov.ph/press_release/2012/0609_angara1.asp (last accessed Dec. 26, 2016).

[3] *See* for example Chapter VII of Republic Act No. 10173, An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission and for other Purposes [Data Privacy Act] §22-24 (Aug. 15, 2012.).

[4] Data Privacy Act, §3(j). *Processing* is defined broadly in the Data Privacy Act, referring to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

[5] Data Privacy Act, §38.

[6] Data Privacy Act §3(c)( *Data subject* refers to an individual whose personal information is processed.)

In the Declaration of Policy, the law provides —

> It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.[7]

This declaration emphasizes the duty of the State to uphold the right to privacy. While the section states "privacy, of communication", noting the only time that the word "privacy" is mentioned specifically in the Bill of Rights,[8] the aspect of privacy that is covered by the law is the right to *information privacy*. This aspect is built on the same principles that hold privacy as a right protected by the Constitution. The right to privacy is "the right to be let alone" and boldly claimed by U.S. Supreme Court Justice Louis Brandeis as "the most comprehensive of rights and the right most valued by civilized men."[9] He explained in this wise —

> The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. **They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.** To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[10]

The right to privacy is at the crucible of the Bill of Rights, supporting the right of persons to life, liberty and property, due process, the right of the people to be secure in their persons, houses, papers, and effects and the right against self-incrimination. Freedom of speech and of the press, freedom of religion, freedom of movement and freedom of association—the full enjoyment of these depends on freedom from unwarranted government intrusions, and a guarantee that individuals are entitled to a reasonable expectation of privacy in their personal lives. Upholding the right to privacy means acknowledging that an individual's dignity has value. As an aspect of privacy, "informational privacy"[11] must be viewed under the same lenses, and afforded the same protection. The right to information privacy refers to the right of individuals to control information about themselves, and to have the ability to determine what information about them is collected or disclosed, how their personal data is to be used and for what purpose.

---

[7] Data Privacy Act §2.

[8] Phil. Const. art III, §3.

[9] Brandeis J, dissenting in *Olmstead v. United States*, 277 U.S. 438 (1928).

[10] *Id*. (Emphasis supplied)

[11] In Whalen v. Roe 429 U.S. 589 (1977), the U.S. Supreme Court expounded that cases characterized as protecting "privacy" involved two different kinds of interests, and that one of this is the individual interest in avoiding disclosure of personal matters.

Implicit also in the "Declaration of Policy"[12] of the Data Privacy Act is the recognition that even as the law protects the right to privacy, it also articulates that free flow of information should be ensured. This should allay fears that the Data Privacy Act could be used as a shield to curtail access to information or to impede innovation and research. The law assures that data protection is not an obstacle for people to obtain benefits from utilization of personal data. The policy statement directs support for open data initiatives, freedom of information and other forms of data sharing. At the same time, it emphasizes that the use of personal data comes with a responsibility. The rights of data subjects should, at all times, be a paramount consideration. Those who exercise control over personal data processing and all forms of data sharing should adhere to data privacy principles and implement appropriate organizational, physical and technical security measures for personal data protection.

The importance of the right to information privacy should be put into context. More than a hundred years ago, an engineer predicted that "man will see around the world. Persons and things of all kinds will be brought within focus of cameras connected electrically with screens at opposite ends of circuits, thousands of miles at a span."[13] This prediction was fulfilled in the last few decades, christened as the information or digital age, where technology has been revolutionizing the way things are done and where information has become readily available to more people.

The advancements in information and communication technology allowed people around the world to be connected, for all kinds of data to be collected and shared, and for volumes of data to be accumulated. It has often been mentioned that 90% of the world's data have been generated only in the last few years.[14] Information is valuable commodity, changing how everyday life is experienced. It is the new currency of power.[15] When Edward Snowden disclosed classified documents of the National Security Agency of the United States of America, the world was taken aback at the widespread surveillance being conducted by the U.S. Government, including surveillance activities directed against known allies.[16] Snowden's revelations renewed privacy concerns but likewise affirmed how information is a sought-after product.

Information is critical for decisions affecting national and economic security, foreign and domestic policies, and other legitimate interests of public authorities. In addition to these, governments also recognize how meaningful use of data coupled with innovation can improve public services and foster growth. Governments launch projects that take advantage of technology to be able to use data in making people's lives better.[17] In the same manner,

[12] Data Privacy Act §2.

[13] Tom Geoghegan, Ten 100-year predictions that came true, (Jan 11, 2012) available at http://www.bbc.com/news/magazine-16444966 (last accessed Dec. 16, 2016); Watkins' predictions, published in a 1900 issue of Ladies' Home Journal under the title "What May Happen in the Next Hundred Years.", available at http://www.techinsider.io/futurist-in-1900-makes-predictions-that-came-true-2015-10 (last accessed Dec. 16, 2016).

[14] SINTEF, Big Data, for better or worse: 90% of world's data generated over last two years (May 22, 2013) available at https://www.sciencedaily.com/releases/2013/05/130522085217.htm (last accessed Dec. 27, 2016).

[15] Sponsorship speech of Senator Edgardo Angara for S.B. 2965, An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Data Protection Commission and for other Purposes (Sept. 21, 2011) ("In this digital era, information is the currency of power – valuable, coveted, but at a very high risk.").

[16] BBC News, Edward Snowden: Leaks that exposed US spy programme (Jan.17, 2014), available at http://www.bbc.com/news/world-us-canada-23123964 (last accessed Dec. 29, 2016).

[17] *See, for example,* Estonia's e-government and e-residency programs, United Kingdom's Government Digital Services, and United States Digital services, Mexico's National Open Data Policy, Tunisia's Open Government Partnership.

the Philippine Congress currently seeks to expand the scope of authorized State surveillance activities,[18] to guarantee freedom of information access,[19] and to institutionalize open data initiatives.[20]

The generation of data is not an exclusive activity of governments. When Facebook acquired WhatsApp, the public was assured that there will be no data sharing between the companies, but the companies have since then backpedaled.[21] A change in privacy policy now required new users of WhatsApp to consent to the data sharing between the companies to avail of the messaging service. The private sector has long been capitalizing on data collection and use of people's information to advance their economic and commercial interests. Private companies invest on big data and analytics.[22] Data sets about people can be sold and bought. Individuals are being profiled based on their online activities, or on data collected about them offline, often with consent.

It should come as no surprise that both government and private sector engage in initiatives that deal with personal data processing. Information is the driving force for change and those unable to adapt to the information age would be left behind. The challenge is to reap the benefits from the availability of information while ensuring that use of personal data will not negatively impact the rights and freedoms of those individuals about whom personal data is processed. Prioritizing data privacy and personal data protection is not only timely, but necessary. The changing times lead the Court to say that —

> The concept of privacy has, through time, greatly evolved, with technological advancements having an influential part therein. This evolution was briefly recounted in former Chief Justice Reynato S. Puno's speech, The Common Right to Privacy, where he explained the three strands of the right to privacy, viz: (1) locational or situational privacy; (2) informational privacy; and (3) decisional privacy. [23]

Due to the advances in technology, the challenges in upholding the right to information privacy has likewise become greater. Personal data protection is no longer just about manual records being kept in filing systems secured by lock and key. The right to information privacy now involves cybersecurity and cyber resilience, including protecting personal data against

---

[18] *See, for example,* An Act Expanding the Scope and Coverage of RA 4200, Otherwise known as An Act to Prohibit and Penalize Wiretapping and Other Related Violations of the Privacy of Communication and for other Purposes, SB 1210, 17th Congress, First Regular Session, (Oct. 19, 2016).

[19] *See, for example,* An Act Implementing the People's Right to Information and the Constitutional Policies of Full Public Disclosure and Honesty in the Public Service and for other purposes, SB 1208, 17th Congress First Regular Session (Oct. 19, 2016).

[20] *See, for example,* An Act Institutionalizing the Establishment of the Philippine Big Data Center, SB 688, 17th Congress, First Regular Session, (Aug. 11, 2016); An Act Requiring the Registration of Subscriber Identity Module (SIM) Cards in Mobile Phones SB 1219, 17th Congress First Regular Session (Oct. 20, 2016).

[21] BBC News, Facebook accused over WhatsApp takeover (Dec. 20, 2016), available at http://www.bbc.com/news/business-38380395 (last accessed Dec. 29, 2016).

[22] Louis Columbus, Forbes, 51% Of Enterprises Intend To Invest More In Big Data (May 22, 2016) http://www.forbes.com/sites/louiscolumbus/2016/05/22/51-of-enterprises-intend-to-invest-more-in-big-data/#527737d3ad04 (last accessed Dec. 29, 2016).

[23] Vivares v. St. Theresa's College, G.R. No. 202666, September 29, 2014 citing Chief Justice Reynato S. Puno's speech, *The Common Right to Privacy*, delivered before the Forum on The Writ of Habeas Data and Human Rights, sponsored by the National Union of Peoples' Lawyers on March 12, 2008 at the Innotech Seminar Hall, Commonwealth Ave., Quezon City. (http://sc.judiciary.gov.ph/speech/03-12-08-speech.pdf. Last Accessed, January 24, 2013).

malwares, ransomwares and other cyberattacks. To consider, however, that data privacy is only about cybersecurity would be a myopic view. Strengthening systems requires adhering to data privacy principles,[24] and implementing privacy, both by design and by default,[25] in data processing systems.

In the Philippines, admittedly, there remains the need to embrace a culture of privacy, built on acceptance of information privacy as a fundamental human right. While the Data Privacy Act became law in 2012, it was not until March of 2016 that the National Privacy Commission, an independent body mandated to implement and administer the law, was constituted.[26] As of August 2014, over one hundred (100) countries worldwide have developed their own data protection regulations.[27] As compared to many other countries, personal data protection in the Philippines is still at its infancy. In August, 2016, in a report titled "Data Danger Zones", the Philippines is ranked as No. 143 out of over 170 nations evaluated on the ability "to keep digital information safe, private and secure."[28] Improving this ranking requires a confluence of factors, including an enabling socio-political environment that would allow the National Privacy Commission to function independently in the performance of its regulatory and enforcement functions, and the presence of multi-sectoral cooperation and coordination from both government and private sector, strengthened by the collective commitment to comply with the Data Privacy Act.

## II. Right to Information Privacy

The US Supreme Court acknowledged the right to privacy as an important right in *Griswold v. Connecticut*, explaining that the penumbras of the Bill of Rights guaranteed zones of privacy.[29] In the Philippines, the opportunity to make a similar declaration came when the right to privacy was raised before the Philippine Supreme Court in *Morfe v. Mutuc.*[30] In this case, the Court was called to decide on whether the periodical submission by a government officer or employee of his Statement of Assets and Liabilities was unconstitutional for being

[24] Data Privacy Act, §11. The general privacy principles under the Data Privacy Act of 2012 requires adherence to the principles of transparency, legitimate purpose and proportionality.

[25] *See* Implementing Rules and regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [IRR] (August 24, 2016), §26(b), which expounds on the concept of "privacy by design" and "privacy by default." It provides in part:

> 1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
> 2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.

[26] The first Privacy Commissioner and Chairman of the National Privacy Commission is Raymund Enriquez Liboro. He is assisted by two Deputy Privacy Commissioners: Ivy D. Patdu for Policy and Planning, and Damian Domingo O. Mapa for Data Processing Systems.

[27] Data Protection, available at https://www.privacyinternational.org/node/44 (last accessed Dec. 26, 2016)

[28] CFO Innovation Asia Staff, "Only four Asian nations safe for data storage" (Aug. 12, 2016) available at http://www.telecomasia.net/content/only-four-asian-nations-safe-data-storage (last accessed Dec. 26, 2016) ("Combining independent data from the United Nations, World Economic Forum, Transparency International and several other leading privacy groups, the report titled "Data Danger Zones" ranks over 170 nations on their abilities to keep digital information safe, private and secure."); The report "Data Danger Zones" in pdf is available at https://www.artmotion.eu/wp-content/uploads/2016/07/DataDangerZones.pdf (last accessed Dec. 26, 2016). It must be noted that the report looked into what it considers key factors for data privacy: political instability, corruption, risk of natural disasters, quality of infrastructure, risk of internal conflicts, and risk of terrorism. This suggests that the report considers socio-political factors as critical factors in establishing data protection framework.

[29] Griswold v. Connecticut. 381 U.S. 479 (1965).

[30] Morfe v. Mutuc, G.R. No. L-20387, January 31, 1968.

violative of due process and the right against self-incrimination. The Court, considering the case as one of first impression, declared that "The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection."[31]

In ruling against the constitutional challenge, the Court also established that the right to privacy is not absolute:

> Even with due recognition of such a view, it cannot be said that the challenged statutory provision calls for disclosure of information which infringes on the right of a person to privacy. It cannot be denied that the rational relationship such a requirement possesses with the objective of a valid statute goes very far in precluding assent to an objection of such character. This is not to say that a public officer, by virtue of a position he holds, is bereft of constitutional protection; it is only to emphasize that in subjecting him to such a further compulsory revelation of his assets and liabilities, including the statement of the amounts and sources of income, the amounts of personal and family expenses, and the amount of income taxes paid for the next preceding calendar year, there is no unconstitutional intrusion into what otherwise would be a private sphere. [32]

Justice Ynares-Santiago, speaking through her dissent in *KMU, et al., v. The Director General, NEDA, et al., and Bayan Muna Representatives et al., v. Ermita, et al.*,[33] classified the right to privacy as an inalienable right of an individual to be let alone.[34] She also discussed the attributes of informational privacy, but again cautions that the right is not absolute:

**The basic attribute of an effective right to informational privacy is the individual's ability to control the flow of information concerning or describing him, which however must be overbalanced by legitimate public concerns.** To deprive an individual of his power to control or determine whom to share information of his personal details would deny him of his right to his own personhood. For the essence of the constitutional right to informational privacy goes to the very heart of a person's individuality, a sphere as exclusive and as personal to an individual which the state has no right to intrude without any legitimate public concern.[35]

One of the earliest legislation relevant to the right to information privacy was Republic Act No. 4200, An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the privacy of Communication, and for other purposes, otherwise known as the Anti-Wiretapping Law, which prohibits unauthorized tapping of any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept or record any communication or spoken word.[36] While prohibiting the recording of private communication, the law exempts from the prohibition wiretapping done by law enforcement in relation to surveillance activities for certain crimes when authorized by written order of the Court.[37] Under the Constitution, the

[31] *Id.*

[32] *Id.*

[33] Dissenting Opinion of Justice Consuelo Ynares-Santiago in G.R No 167798 Kilusang Mayo Uno, et al., v. The Director General, National Economic Development Authority, et al., and G.R No. 167930 Bayan Muna Representatives Satur C. Ocampo, et al., v. Eduardo Ermita, et al. (19 April 2006) (emphasis supplied.).

[34] *Id.*

[35] *Id.*

[36] Republic Act No. 4200, An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for other purposes, (Anti-Wiretapping Law) (1965).

[37] Anti-Wiretapping Law, §3.

privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.[38] The right to information privacy is not limited to private communications. It covers the protection of personal data and the right of individuals to control information about themselves, without regard to whether the information was generated in the context of a private communication

In the Philippines, various laws provide for information privacy, either by protecting privacy in general or criminalizing privacy violations.[39] In 2008, the Supreme Court issued the Rule on the Writ of Habeas Data.[40] The writ of habeas data is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.[41]

While the Rule on the Writ of Habeas Data affirms the need to protect information privacy, it is a summary remedy. It has been invoked in several cases where there is an apparent violation of the right to information privacy, but the affected data subjects often do not get relief for failure to show that the privacy violation affects the right to life, liberty or security.[42] In *Lee v. Ilagan*, the Court emphasized:

> As the rules and existing jurisprudence on the matter evoke, alleging and eventually proving the nexus between one's privacy right to the cogent rights to life, liberty or security are crucial in *habeas data* cases, so much so that a failure on either account certainly renders a *habeas data* petition dismissible, as in this case.[43]

The right to information privacy is a fundamental human right. The violation of the right to information privacy, by and of itself, however, will be insufficient to support the petition for habeas data. The Court consistently requires a clear showing of how the privacy violation

---

[38] Phil. Const. art III, §3.

[39] *See, for example,* An Act Revising the Penal Code and Other Penal Laws [Revised Penal Code], Act No. 3815, arts. 228-230, 290-292 (1932); An Act to Exempt the Publisher, Editor or Reporter of any publication for revealing the Source of Published news or information obtained in Confidence, Republic Act No. 53 (Oct. 5, 1946), amended by R.A. No. 1477 (1956); An Act to Ordain and Institute the Civil Code of the Philippines, [New Civil Code] Republic Act No. 386, arts. 19-21, 26, 32, 723 (June 18, 1949); An Act Prohibiting Disclosure of or Inquiry into Deposits with any banking institution and providing penalty therefor, Republic Act No. 1405, (1955); An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purpose [Anti-wiretapping law], R.A. No. 4200 §§ 1-2(1965); An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and Other Purposes, "Electronic Commerce Act of 2000", Republic Act No. 8792, §§31-33 (June 14, 2000). Prevention and Control of HIV/AIDS in the Philippines, Instituting a Nationwide HIV/AIDS Information and Educational Program, Establishing a Comprehensive HIV/AIDS Monitoring System, Strengthening the Philippine National Aids Council, and for Other Purposes, "Philippine AIDS Prevention and Control Act of 1998", Republic Act No. 8504, (February 13, 1998); An Act Instituting the Comprehensive Dangerous Drugs Act of 2002, Repealing Republic Act No. 6425, Otherwise Known as the Dangerous Drugs Act of 1972, as Amended, Providing Funds Therefor, and for Other Purposes, "Comprehensive Dangerous Drugs Act of 2002", Republic Act No. 9165, (June 7, 2002); An Act Defining Violence Against Women and Their Children, Providing for Protective Measures for Victims, Prescribing Penalties Therefore, and for Other Purposes, "Anti-Violence Against Women and Their Children Act of 2004", Republic Act No. 9262, (March 8, 2004); The Child and Youth Welfare Code, Presidential Decree No. 603, Title VIII Chapter 1 art. 166 (1974).

[40] A.M. No. 08-1-16-SC, Rule on the Writ of Habeas Data (Jan. 22, 2008).

[41] Rule on Writ of habeas Data, §1.

[42] *See* for example Tapuz v. del Rosario, G.R. No. 182484, June 17, 2008; Castillo v. Cruz, G.R. No. 182165, November 25, 2009; Roxas v. Macapagal-Arroyo, G.R. No. 189155. September 7, 2010; Vivares v. St. Theresa's College, G.R. No. 202666. September 29, 2014; Lee v. Ilagan, G.R. No. 203254. October 8, 2014.

[43] Lee v. Ilagan, G.R. No. 203254, October 8, 2014.

affects the right to life, liberty and property. In those cases, where the information privacy violation fails to meet the jurisdictional requirements of the writ of habeas data, the person about whom personal data is processed is not left without a remedy. In 2012, through R.A. No. 10173 or the Data Privacy Act of 2012, the right to information privacy was specifically upheld in law, mandating protection of personal data and crystallizing the rights of data subjects or individuals about whom personal data is processed. Under the Act, data subjects have the right to complain before the National Privacy Commission on violations of their information privacy or cases of personal data breach.

The Data Privacy Act of 2012 upholds the right to information privacy while supporting free flow of information. The law imposes obligations on those involved in the processing of personal data to safeguard the information being collected, used, or stored. The end in view is that the confidentiality, integrity and availability of these personal data are protected, and that the concerned individuals will not be unduly prejudiced as a result of the processing. Personal data should be protected because its unauthorized or unlawful collection, use or disclosure could lead to the commission of crimes against individuals about whom data is processed, or could cause them other forms of injury and damage.

Unauthorized access to personal data can be used to perpetuate identity fraud and to commit other crimes. Information that may be used to enable identity fraud include financial documents, usernames, passwords and other login data, biometric data, information in identification documents or licenses, and other unique identifiers like Philhealth, SSS, GSIS, and TIN number. Earlier this year, media reported how a public school teacher allegedly became the victim of identity fraud after posting his Identification Card issued by the Professional Regulation Commission in social media.[44]

In 2008, a video clip of what is now known as the "Cebu Canister Scandal" was uploaded on YouTube.com, showing hospital staff jeering and laughing after the successful extraction of a metal spray bottle canister from a patient's rectum.[45] Hospital staff declaring "Baby out", the extracted canister being sprayed, and the video spreading from cell phone to cell phone constitute utter disregard for the patient's privacy. The face of the patient was not shown in the video, but later when interviewed by media, the patient said that everyone eventually found out about his identity.[46] The patient was angry at the invasion of his privacy. When he consented to the operation, he did not fathom that the successful operation also meant that his private affairs will be exhibited to the public, or that people would make assumptions about his life, subjecting him to ridicule or judgment. This case exemplifies how the unwarranted disclosure of personal data could cause injury to a data subject. A violation of privacy is essentially an affront to human dignity.

In upholding the right to information privacy, people should be made aware of the value of their personal data. Daniel Solove, an expert in privacy law, wrote about why privacy

[44] GMA News Online, Public School teacher in debt because of Identity Theft (Feb. 26, 2016), available at http://www.gmanetwork.com/news/story/556952/news/metro/public-school-teacher-in-debt-because-of-identity-theft (last accessed Dec. 29, 2016).

[45] *See discussion* in Antonio, Patdu and Marcelo, *Health Information Privacy in the Philippines: Implications for Policy and Practice* Privacy in the Developing World—Philippines Monograph Series 04/2013 (2013).

[46] GMA News Online, Cebu surgery scandal: Findings anger victim of abuse (April 19, 2008) available at http://www.gmanetwork.com/news/story/90323/news/regions/cebu-surgery-scandal-findings-anger-victim-of-abuse#sthash.oVftqS33.dpuf (last accessed Dec. 27, 2016).

should matter. He said, in part, that:

> Privacy is a limit on government power, as well as the power of private sector companies. The more someone knows about us, the more power they can have over us. Personal data is used to make very important decisions in our lives. Personal data can be used to affect our reputations; and it can be used to influence our decisions and shape our behavior. It can be used as a tool to exercise control over us. And in the wrong hands, personal data can be used to cause us great harm.
>
> xxx
>
> Personal data is essential to so many decisions made about us, from whether we get a loan, a license or a job to our personal and professional reputations. Personal data is used to determine whether we are investigated by the government, or searched at the airport, or denied the ability to fly. Indeed, personal data affects nearly everything, including what messages and content we see on the Internet. Without having knowledge of what data is being used, how it is being used, the ability to correct and amend it, we are virtually helpless in today's world. Moreover, we are helpless without the ability to have a say in how our data is used or the ability to object and have legitimate grievances be heard when data uses can harm us. One of the hallmarks of freedom is having autonomy and control over our lives, and we can't have that if so many important decisions about us are being made in secret without our awareness or participation.[47]

Personal data is being processed in volumes, often using automated processes for further use. In availing of services, entering into financial transactions, applying to school or for a job, and many other activities, personal data is being collected and stored. The Philippines, despite its notorious problem with internet connectivity, continue to be among the world's top users of social media sites.[48] These social media sites entice users because they provide a free platform for a host of online activities, while actually collecting the personal data of its subscribers. The government through its various agencies process personal data of individuals who provide information to obtain health and social welfare benefits, to get pension or law enforcement clearance, to apply for licenses, to register as voters, and in general to avail of public services. Without safeguards, there will be no limits to how private and public sector collect and use personal data.

The volume of data about individuals being processed on a daily basis and the corresponding risks to data subjects arising from unlawful or unauthorized access, as well as the possibility of using profiling and other automated processes to make decisions affecting people's lives, makes it imperative that those who process personal data be accountable for the protection of data subjects.

## III. Data Privacy Act

The Data Privacy Act of 2012 was signed into law on August 15, 2012.[49] Its

[47] Daniel Solove, PRIVACY + SECURITY BLOG, News, Developments, and Insights, 10 Reasons Why Privacy Matters (Jan. 20, 2014) available at https://www.teachprivacy.com/10-reasons-privacy-matters/ (last accessed Dec. 27, 2016). Solove also wrote a paper on Why Privacy Matters Even if you have 'nothing to hide', The Chronicle of Higher Education (May 15, 2011).

[48] While the numbers vary from anywhere between 25% to 95%, surveys indicate that utilization of social networking sites in the Philippines is high compared to other countries not only in the Asia-Pacific region but also globally, earning for the country the moniker —The Social Networking Capital of the World. Social Networking Capital of the World available at http://www.nicojr.com/2011/05/the-philippines-is-the-social-networking-capital-of-the-world/ (last accessed Dec. 27, 2016).

[49] The bill that eventually became R.A. No. 10173 or the Data Privacy Act of 2012 was principally sponsored by Senator

Implementing Rules and Regulations took effect on September 9, 2016.[50] The principles enshrined in the Data Privacy Act were based on the European Parliament and Council's Directive 95/46/EC (DPD)[51] and the Asia Pacific Economic Cooperation (APEC) Privacy Framework.[52] The Data Privacy Act was also influenced by the reform initiatives on the DPD, which later led to the adoption of the General Data Protection Regulation (GDPR) on April 27, 2016.[53] In fact, many of the new provisions introduced by the GDPR had already been earlier incorporated to the Data Privacy Act, such as the right to portability[54] or breach notification.[55]

The Data Privacy Act ("Act") created the National Privacy Commission, which was given the mandate to administer and implement the provisions of the Act, and to monitor and ensure compliance of the country with international standards set for data protection.[56] This means that in addition to the provisions of the Act, due consideration should be given to accepted international principles and standards for personal data protection. The guiding policy is to safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development.[57]

*Personal Data*

The Act applies to to the processing of personal data by any natural or juridical person, in the government or private sector. As can be gleaned from its title, the purpose of the Act is for the protection of "individual personal information," referring to personal data of a natural person. This means that information about corporations or juridical persons are beyond the scope of the Act. Information not deemed "personal data" are likewise excluded from the application of the law.

Personal data refers to any information that could be used to identify an individual. If on the basis of a given information or set of information, the identity of a natural person can be known, then the information is personal data. Examples of personal data include the name or photograph of a person, his or her fingerprint, and identification cards and numbers. Anonymous information or aggregated data can no longer be used to identify a natural person,

Edgardo J. Angara: An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Data Protection Commission and for other Purposes, SB 2965, 15th Congress Second Regular Session (Sep. 14, 2011). S.B. No. 2965 was approved in substitution of other bills introduced by Senators Miriam Defensor Santiago (S.B. No. 1908, S.B. No. 2236) and Antonio Trillanes (S.B. No. 355), and H.B. No. No. 4115 introduced by Reps Roman Romulo, et al.

[50] Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [IRR] (Aug. 24, 2016).

[51] European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Oct. 24, 1995, available at: http://www.refworld.org/docid/3ddcc1c74.html (last accessed 29 December 2016).

[52] Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2005), available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (last accessed on 16 December 2016).

[53] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[54] Data Privacy Act, §19.

[55] Data Privacy Act, §20(f).

[56] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and for Other Purposes, Republic Act No. 10173, chap II §7 (2012)

[57] IRR, §2.

and is thus no longer considered as personal data. Statistical data by itself is aggregate data, which will not lead to the identity of any particular individual.

It must be noted that the IRR of the Act uses the term "personal data" when referring to all types of information relating to individuals, regardless of the sensitivity or privileged nature of the information, and shall refer to the following collectively:

> a. "Personal information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
> b. "Sensitive personal information" refers to personal information:
>  1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
>  2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
>  3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
>  4. Specifically established by an executive order or an act of Congress to be kept classified.
> c. "Privileged information" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.[58]

The classification is important because under the Act there are specific provisions that apply only to personal information, as distinguished from sensitive personal or privileged information.[59] Sensitive personal and privileged information as a general rule should not be processed except if with consent of the data subject, or when specifically authorized by law. [60] This is because the sensitivity of the personal data also means that unlawful or unauthorized processing would be more prejudicial or lead to greater harm to the data subjects.

Personal data, regardless of classification, allows one individual to be distinguished from another, or otherwise identified. This means that the Identification of a person can be reasonably or directly ascertained from the information. It is still personal data even if the information by and of itself would not make the data subject identifiable, but when put together with other reasonably available information would allow identification. Reasonableness, for this purpose, will be evaluated based on the probability, difficulty and potential of identification, including required time, cost and skill.

The Act applies to the processing of personal data, performed through automated means or manual processing, if the personal data are contained or are intended to be contained in a filing system. "Processing" refers to any operation or any set of operations performed

---

[58] Data Privacy Act, §3(h)(l)(k).

[59] *See for example* Data Privacy Act, §12 which applies to *personal information* as distinguished from *sensitive personal information*, and §13which applies to sensitive personal and privileged information. *See also* Data Privacy Act, Chap. VIII on Penalties, defining several crimes on the basis of whether the information is personal information or sensitive personal information. See Data Privacy Act, §11, which applies to personal, sensitive personal and privileged information collectively.

[60] Data Privacy Act, §13; IRR, §22.

upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[61] The Act will apply whether the personal data being processed is only a single record or an entire database with volumes of data, and whether contained in paper or electronic files.

*Personal Information Controller and Personal Information Processor*

As a general rule, the Act imposes obligations on any natural or juridical person involved in the processing of personal data, whether in the government or private sector. These would be the "personal information controllers" or "personal information processors."

The "Personal information controller" refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf.[62] This refers to the corporation itself or the government agency, acting through its board or officials. It may refer to an individual, when the individual is the sole owner and decision-maker of an enterprise involved in personal data processing. The term does not refer to the employee in charge of computer systems, those who encode data, or the head of the IT department. The personal information controller exercises control over the processing of personal data. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.[63]

For illustration, consider, for example, a hospital that processes personal data of its patients. It does so through its employees or consultants, such as the nurses or physicians. It may also do so through an IT employee that manages the electronic records in the hospital. In this case, the hospital is the personal information controller, not the nurses, physicians or IT personnel, because the latter process personal data only in behalf of the hospital.

In contrast, when a doctor has his or her own private clinic, and he or she keeps the medical records of his or her patients, then the doctor, as an individual, would be the personal information controller. The one who ultimately decides or who has the responsibility to decide what, how or why personal data is processed is the personal information controller.

Consider now, as another example, a hospital that enters into a contract with a company providing electronic medical record services, or other hospital information management system. The hospital, in effect, instructs the provider to process personal data of its patients. The hospital retains control over the processing because the EMR provider does not have the authority to use the personal data of the patients for any purpose under than pursuant to the agreement with the hospital. The hospital remains the personal information controller, while the EMR provider is the personal information processor.

The "Personal information processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.[64] If a personal information processor uses the personal data for a purpose other than pursuant to the instructions of the personal

[61] Data Privacy Act, §3(j); IRR, §3(o).

[62] Data Privacy Act, §3(h); IRR, §3(m).

[63] IRR, §3(m).

[64] Data Privacy Act, §3(i); IRR, §3(n).

information controller, then the personal information processor, by its actions, also become the personal information controller. Going back to the earlier example, if the EMR provider stores and discloses the electronic medical records to a pharmaceutical company it is affiliated with, then the EMR provider is acting as a personal information controller. This means, the EMR provider is also obligated to comply with the obligations of a personal information controller under the Data Privacy Act. Thus, if the disclosure to another company is without consent of the patient, the EMR provider's further processing of the medical records may constitute a crime.

It must be pointed out that a natural person who processes personal data in connection with his or her personal, family, or household affairs, by express provision of law, is not to be considered a personal information controller. [65] Thus, when an individual keeps a directory of names, addresses and phone numbers for purely personal purposes, the individual is not a personal information controller. When the directory of contacts is being used for example as a client list, or for a professional or commercial activity, then the individual will be considered a personal information controller. Being a personal information controller means the individual would have to comply with the obligations imposed on the personal information controller under the Data Privacy Act.

*Scope of Data Privacy Act*

The Act applies to the processing of personal data, in and outside of the Philippines when the data subject is a citizen or resident of the Philippines, or when the processing of personal data is being done in the Philippines.[66] When the processing is done outside the Philippines, and personal data relates to a citizen and resident of another country, Philippine laws would apply when the processing is being done by a person or entity with links to the Philippines, such as when the natural or juridical person involved in the processing of personal data is found or established in the Philippines.[67] For these kinds of cases, whether Philippine law would apply would depend on the particular circumstances of the case, taking into account international law and comity.

In order for the National Privacy Commission to effectively implement the extra-territorial application of the Data Privacy Act, it should participate in regional and international initiatives for cross-border enforcement, such as the Global Privacy Enforcement Network or Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement. One of the controversial cases on personal data breach involved an investigation on the reported hacking of the Ashley Madison website, targeted at people seeking a discreet affair. [68] Through the APEC Cross-border Privacy Enforcement Arrangement, the privacy authorities of Canada and Australia conducted a joint investigation, which lead to resolution of the case.[69] Working towards effective cross-border enforcement, the National Privacy Commission, during its first year, had been accepted as member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC),[70] and the Asia Pacific Privacy Authorities forum.

[65] Data Privacy Act, §3(h); IRR, §3(m).

[66] Data Privacy Act, §§4,6; IRR, §4.

[67] Data Privacy Act, §§4,6; IRR, §4.

[68] Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner, available at https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison (last accessed Dec. 30, 2016).

[69] Id.

[70] Kenny, Kathy (October 2016), PH Privacy Commission Gets International Accreditation, accessed on 16 December 2016,

As a general rule, the Data Privacy Act applies to the processing of all types of personal data. The Act specifies categories of information where it will not apply. These are:

a. Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

1. The fact that the individual is or was an officer or employee of the government institution;
2. The title, business address and office telephone number of the individual;
3. The classification, salary range and responsibilities of the position held by the individual; and
4. The name of the individual on a document prepared by the individual in the course of employment with the government;

b. Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

c. Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

d. Personal information processed for journalistic, artistic, literary or research purposes;

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);

f. Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

g. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.[71]

The enumeration identifies special cases which are given greater flexibility under the Act. This is because the special cases refer to information that are being processed in the exercise of a constitutional right, a necessary public function for national or economic security, or because of the conceded public benefit of the processing activity. This proceeds from the recognition that the right to privacy, particularly information privacy, is not absolute. Under the General Data Protection Regulation (GDPR), while there is no absolute exemption, the GDPR allows member States to "restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation,

available at http://www.psst.ph/ph-privacy-commission-gets-international-accreditation/

[71] Data Privacy Act, §4; *See also* IRR, §§5-6.

detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[72]

In most cases, the right to privacy would need to be balanced with other fundamental freedoms or the State's exercise of its police power. A claim therefore that the Data Privacy Act does not apply to a particular information would have to be evaluated on a case to case basis. As guiding principles:

1. The non-applicability should be understood as being limited to the particular information only, and does not extend to personal information controllers or personal information processors. This means that those involved in the processing of personal data remain subject to the obligation of implementing security measures for personal data protection. Unless directly incompatible or inconsistent with the processing of the enumerated information, the personal information controller or personal information processor shall uphold the rights of data subjects, and adhere to general data privacy principles and the requirements of lawful processing.[73]

2. The non-applicability of the Act for the special cases will only be to the minimum extent of collection, access, use, disclosure or other processing necessary to achieve the specific purpose, function, or activity. The flexibility allowed the special cases is to be understood as the information being exempted from specific provisions of the Data Privacy Act only when complying with the same will frustrate the collection, access, use, disclosure or other processing needed for the achievement of the specific purpose, function or activity. [74]

3. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.[75]

For example, while the Act does not apply to information necessary to comply with the reporting requirements of the Anti-Money Laundering Act, this does not mean that the banks processing the information will be exempted from complying with the other obligations and requirements under the Act. To the minimum extent necessary to comply with the AMLA reporting requirements, the banks may process the relevant personal data without need of asking for consent from data subjects. The bank is, however, still prohibited to disclose without authority the same information to any third party outside those provided for in the Anti-Money Laundering Act. Also, the bank, as personal information controller, remains obligated to implement organizational, physical and technical security measures for personal data protection.

The non-applicability in the Act is intended to support particular interests because of their presumed benefit to the public or because they relate to fundamental freedoms guaranteed by the Constitution. In Sections 4(a), (b) and (c) of the Act, the non-applicability is for purpose of allowing public access to information that fall within matters of public concern.

---

[72] GDPR, Recital 19.

[73] IRR, §§5-6.

[74] IRR, §§5-6

[75] IRR, §6; See also Data Privacy Act, §38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

The right to data privacy and right to information are often viewed to be irreconcilable and incompatible, however, these two rights complement each other and are both geared towards promoting personal protection and government accountability.[76] The Data Privacy Act envisaged the limitations on the right to privacy prescribed by the State policy of full public disclosure of all its transactions involving public interest, and by the fundamental right of the people to information on matters of public concern.[77] The Act also does not apply to personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, expression, and the press, and to personal information that will be processed for research purpose, in order to support ethical and responsible research intended for a public benefit. [78]

The Act does not apply to information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, or to the extent of processing required to comply with the Credit Information System Act and the Anti-Money Laundering Act.[79] This means that public authorities will not be hindered from performing lawful activities intended for public health, public order, and national or economic security. In the exercise of governmental function, however, it is critical to emphasize that the non-applicability provided in the Data Privacy Act is not absolute, and that the right to privacy finds greatest relevance when the infringement is being justified as a legitimate act of government. The non-applicability provided in the law does not also mean that an individual can no longer inquire upon the validity or legitimacy of the data processing being done by government. The Bill of Rights is, after all, intended precisely for the protection of an individual against possible abuses of the State.

In Section 4(g), the non-applicability of the Act to personal information originally collected from residents of foreign jurisdictions, in accordance with their laws,[80] was meant to support BPO industries in recognition of their contribution to the Philippine economy. The intent is to accommodate the possible difference in laws governing the collection of personal information, and would have to be evaluated on the particular circumstances of the claim of non-applicability. In all cases, the personal information controllers and personal information processors remain to be covered by the law including the implementation of security measures for data protection.

The interpretation of the non-applicability provided in the Data Privacy Act should be strictly construed in order to uphold the rights of the data subject. These are in the nature of exceptions which are subject to the rule of strict construction:[81]

---

[76] Banisar, David. (2011). The Right to Information and Privacy: Balancing Rights and Managing Conflicts, accessed on 21 December 2016, available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf

[77] Phil Const. art. II §28. Subject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest; Phil Const. art III. §7. The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.

[78] Data Privacy Act, §4(d); IRR, §5(b)(c).

[79] Data Privacy Act, §4(e)(f); IRR, §5(d)(e).

[80] Data Privacy Act, §4(g); IRR, §5(f).

[81] Luis K Lokin, Jr. v. Commission on Elections and the House of Representatives, G.R No. 179431-32 and Luis K. Lokin, Jr. v. Commission on Elections, et. al., G.R No. 180443 (22 June 2010).

> When the statute itself enumerates the exceptions to the application of the general rule, the exceptions are strictly but reasonably construed. The exceptions extend only as far as their language fairly warrants, and all doubts should be resolved in favor of the general provision rather than the exceptions. xxx Consequently, the existence of an exception in a statute clarifies the intent that the statute shall apply to all cases not excepted. Excepton are subject to the rule of strict construction; xxx[82]

*Data Privacy Principles*

Section 11 of the Data Privacy Act allows the processing personal data, as a general rule, subject to the following:

1. Compliance with the requirements of the Act and other laws allowing disclosure of information to the public; and
2. Adherence to the principles of transparency, legitimate purpose and proportionality.[83]

While the principles emphasized by the Data Privacy Act are transparency, legitimate purpose and proportionality, these principles should be interpreted in the context of the general data privacy principles recognized in other jurisdictions. The APEC Privacy Framework, for instance, enumerates nine (9) basic principles which are similar to the European Union's Directive and the Data Privacy Act, such as: (1) Preventing Harm; (2) Notice; (3) Collection Limitations; (4) Uses of Personal Information; (5) Choice; (6) Integrity of Personal Information; (7) Security Safeguards; (8) Assess and Correction; and (9) Accountability.[84] The APEC Framework likewise explicitly stated that the right to privacy must not thwart governmental interests authorized by law, including activities intended to protect national security, public safety or other relevant and imperative public policies.[85]

The principles of transparency, legitimate purpose and proportionality are also consistent with the Data Privacy Principles under the EU Data Protection Directive and GDPR. These principles serve as backbone of the data privacy principles defended by the Act:

> a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
>
> b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy

[82] *Id.*

[83] Data Privacy Act, §11; IRR, §§17-20.

[84] APEC Privacy Framework, accessed on 16 December 2016, available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[85] *Id.*

> c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. [86]

The principle of transparency substantially empowers the data subject to exercise control over the processing of his or her personal data. It includes the principle of fairness,[87] and requires that personal data be "collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only."[88] Adhering to the principle of transparency means upholding the rights of data subjects. These rights, provided in Section 16 of the Data Privacy Act, gives the Data Subjects the demandable right to have access to information about themselves being processed by a personal information controller or personal information processor.[89] A data subject should know that his or her data is being processed, and he or she should be furnished information about what personal data is being processed, the why and how of the processing, intended disclosures, access and storage of the personal data, and the identity and contact details of the personal information controller or its representative. A data subject should always be informed that he or she has a right to file a complaint before the National Privacy Commission.

The rights of data subjects, in general, include:

1. Right to be informed on matters pertaining to the processing of personal data, including intended changes to the processing;[90]
2. Right to object to the processing of personal data;[91]
3. Right to access upon demand;[92]
4. Right to correct errors and inaccuracies in the personal data being processed;[93]
5. Right to erasure or blocking of personal data when no longer necessary for the purpose of collection, and when rights of data subjects are already being violated;[94]
6. Right to data portability, or the right to request for copies of his or her personal data which are being processed by electronic means in commonly used formats;[95]
7. Right to damages when the data subject is injured by an unlawful or unauthorized processing, or by other acts

[86] IRR, §18

[87] Data Privacy Act, §11(b)

[88] Data Privacy Act, §11(a).

[89] Data Privacy Act, §§16-19; IRR, §§34-37.

[90] Data Privacy Act, §§16(a)(b); IRR, §34(a).

[91] Data Privacy Act, §§16(b); IRR, §§34(b).

[92] Data Privacy Act, §16(c); IRR, §§34(c).

[93] Data Privacy Act, §16(d); IRR, §§34(d).

[94] Data Privacy Act, §16(e); IRR, §§34(e)

[95] Data Privacy Act, §18; IRR, §36.

violating his or her rights as data subject;[96] and
8. Right to file a complaint with the National Privacy Commission.[97]

The principle of legitimate purpose requires that personal data be processed fairly and lawfully.[98] Those who process personal data should also ensure that the personal data is accurate, relevant and where necessary for purposes for which it is to be used, kept up to date.[99] The Act provides the criteria for lawful processing in Sections 12 and 13.[100] Personal information, as distinguished from sensitive personal and privileged information, may be processed unless a law prohibits the processing.[101] On the other hand, processing of sensitive personal and privileged information is prohibited, except when the data subject consents, or when specifically authorized by law.[102]

In both the Data Privacy Act and the GDPR, consent, as a general rule, is required for processing of personal data. Consent refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information.[103] Based on the Act and its IRR, there is consent:

1. The Data subject agrees to the collection and processing of his or her personal or sensitive personal information, or all the parties to the exchange agrees to the collection and processing of privileged information;
2. The consent was freely given, specific and proceeds from being informed of:
   a. The purpose, nature and extent of processing;
   b. The period or conditions when consent is deemed effective, or information on how consent can be withdrawn;
   c. Rights of data subject;
3. Consent is evidenced by written, electronic or recorded means. A lawful representative or an agent specifically authorized by the data subject to do so may also give consent on behalf of the data subject.

Obtaining consent is a process, and should not be viewed as limited to having a data subject sign a form or tick a box. Efforts should be directed towards obtaining meaningful consent, or one that is premised on actually informing the data subject the purpose and the processing activities for which consent is being obtained. The test to determine whether consent was obtained fairly and lawfully is whether the data subject would be unreasonably surprised by the processing activities. The Data Privacy Act does not allow implied consent, and consent should be evidenced by written, electronic or recorded means. The data subject should opt in to the processing of his or her personal data as opposed to making "consent" the

[96] Data Privacy Act, §16(f); IRR, §§34(f).

[97] Data Privacy Act, §§7(b)(k), 16-19; IRR, §§19(b),(d),(e),(f)34-37.

[98] Data Privacy Act, §11(b).

[99] Data Privacy Act, §11(c).

[100] Data Privacy Act, §§12-13.

[101] Data Privacy Act, §12.

[102] Data Privacy Act, §13.

[103] Data Privacy Act, §3(b); IRR, §3(c).

default.

Given however the changing times and rapid technological advancements, a framework based on consent would have to accommodate a framework centered on accountability. The principle of accountability requires the personal information controller to be accountable for complying with the law, to use contractual and reasonable means to provide a comparable level of protection when personal data under its control or custody is being processed by a personal information processor or third party, and to be able be able to demonstrate this compliance.[104] In the digital age, collection of volumes of personal data occur either because data subjects would easily choose convenience and benefits over their information privacy, or because the direction of legislative thrusts and policy making is towards greater data sharing. The Data Privacy Act itself recognizes that there are processing activities where consent is no longer required, and where the rights of data subject may be limited. Part of the principle of legitimate purpose is to ensure that the rights of data subject are protected even as they consent to the use of their personal data, and even more so, when the use of their personal data is compelled or otherwise authorized by law.

The principle of proportionality[105] requires that the processing of personal data be only to the minimum extent necessary to achieve the declared, specified and legitimate purpose. It includes the principle of purpose limitation and data minimization, such that from the time of collection, only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected. The personal data collected shall be retained or stored only in so far as may be necessary for the said purpose, or when the retention is specifically authorized by law.

The principle of proportionality is important when evaluating the data processing activities in both government and private sector. While consent may have been given for a particular purpose, or while a law may authorize the collection of personal data by a government agency, these should not be taken as an authority to collect any and all personal data without restriction. If personal data is not necessary for the purpose of processing, then the personal data should no longer be collected. Keeping and storing personal data that are not really needed to achieve a particular purpose only serves to increase the risks to the data subjects in the event of a personal data breach. Also, the nature of the personal data being processed and the extent of processing determines the level of security required for personal data protection. The larger the volume and the more sensitive the personal data processed, the greater will the required security measures be.

*Organizational, Physical and Technical Security Measures*

The Data Privacy Act does not prohibit processing of personal data but merely imposes obligations and requirements on those involved in personal data processing to ensure protection of the fundamental rights and freedoms of the data subjects.

In *Whalen v. Roe*, the United States Supreme Court was called upon to decide on the constitutionality of a statute allowing the State of New York to collect, record and store personal data of individuals in a centralized computer file, where the individuals, pursuant to a doctor's prescription, obtained drugs with known medical benefits but at the same time

[104] Data Privacy Act, §21; IRR §§50-51.

[105] Data Privacy Act, §11(c)(d)(e)(f).

can be potentially abused.[106] It was argued that the existence of the database poses a threat to the privacy of the individuals, which if disclosed could damage their reputations. It was alleged that the privacy concern was sufficient to make patients reluctant to use and physicians reluctant to prescribe such drugs. The Court was of the opinion that the statute on its face was not a threat to privacy, and that there were sufficient safeguards to protect personal data. The decision included a recognition of the threat to privacy in the government processing of personal data:

> **We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.** The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. **The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.** Recognizing that, in some circumstances, that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data -- whether intentional or unintentional -- or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[107]

The Court rejected the claim of violation of informational privacy due to the legitimate interests of the State to control drug abuse in the United States and uphold the health of the citizens while assuring the public that there are numerous safeguards implemented to avoid the danger of unauthorized disclosure.[108] This case, decided in 1977, already recognized that processing of personal data comes with a responsibility. It is, in all cases, never enough to obtain meaningful consent from a data subject, or to have legal authority to process personal data. Upholding the right to information privacy requires more than a legitimate basis for processing. It must go hand-in-hand with a commitment to ensure that the personal data being processed is protected. Under the Data Privacy Act, those who process personal data are obligated to implement organizational, physical and technical security measures.

Before the Data Privacy Act became law, these principles were argued by Justice Consuelo Ynares-Santiago in her dissent in *KMU v. The Director General, NEDA*[109] when the Court was called upon to rule on the constitutionality of *Executive Order No. 420* (2005) requiring all government agencies and government-owned and controlled corporations to streamline and harmonize their identification systems. Justice Ynares-Santiago wrote:

> As the erosion of personal privacy by computer technology and advanced information systems accelerate, the individual's ability to control its use has diminished. Sharing of data among government agencies and private and

[106] Whalen v. Roe 429 U.S. 589 (1977).

[107] Whalen v. Roe, 429 U.S. 589 (1977) (emphasis supplied).

[108] Concurring opinion of Justice Brennan, Whalen v. Roe, 429 U.S. 589 (22 February 1977).

[109] Dissenting Opinion of Justice Consuelo Ynares-Santiago in G.R No 167798 and G.R No. 167930 (19 April 2006).

> public organizations are not uncommon. Aside from the chilling prospect that one's profile is being formed from the gathering of data from various sources, there is also the unsettling thought that these data may be inaccurate, outdated or worse, misused. There is therefore a pressing need to define the parameters on the use of electronic files or information, to be properly initiated by a legislative act and not formulated in a mere executive order masquerading as an internal regulation, as in the case of E.O. No. 420.
>
> Even granting that E.O. No. 420 constitutes a valid exercise of executive power, it must still be struck down because it falls short of the guarantees laid down in Whalen v. Roe and Ople v. Torres. **There is no specific and foolproof provision against the invasion of the right to privacy, particularly, those dealing with indiscriminate disclosure, the procedure for the gathering, storage, and retrieval of the information, an enumeration of the persons who may be authorized to access the data; and the sanctions to be imposed against unauthorized use and disclosure.** Although it was mentioned in Section 3 of E.O. No. 420 that the data to be collected will be limited to the enumeration therein, yet it failed to provide the yardstick on how to handle the subsequent and additional data that will be accumulated when the ID is used for future governmental and private transactions.
>
> Thus, we reiterate the caveat enunciated in Ople v. Torres that **'the right to privacy does not bar all incursions into individual privacy. The right is not intended to stifle scientific and technological advancements that enhance public service and the common good. It merely requires that the law be narrowly focused and a compelling interest justifies such intrusions. Intrusions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions.** We reiterate that any law or order that invades individual privacy will be subjected by this Court to strict scrutiny. [110]

Under the Data Privacy Act and its IRR, the processing of personal data comes with the duty of implementing proper safeguards to uphold the right to information privacy.[111] These measures should aim to maintain the confidentiality, integrity and availability of personal data being processed:

> Personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.
>
> The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law.
>
> The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as

[110] Dissenting Opinion of Justice Consuelo Ynares-Santiago in G.R No 167798 and G.R No. 167930 (19 April 2006) (emphasis supplied).

[111] Data Privacy Act, §§20-24; IRR, §§25-33, 38-51.

> against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.[112]

Organizational security measures include the designation of an individual or individuals accountable for the compliance with the Data Privacy Act, developing data privacy policies, capacity building for human resource, and procedures for personal data breach management.[113] Physical security measures include limiting physical access to workstations and ensuring that the data processing systems will be secured against natural disasters, power disturbances, external access, and other similar threats.[114] Technical security measures refer to measures intended to maintain the confidentiality, integrity, availability, and resilience of their processing systems and services.[115] These also include implementing safeguards to protect computer networks, regular monitoring for security breaches and a process for regularly testing, assessing, and evaluating the effectiveness of security measures.[116] These measures impress the need for change, which must involve the decision-makers and top management. These also clarify that data privacy must be approached holistically, with a view to strengthening the data processing system as whole rather than as an exclusive concern of IT personnel or cybersecurity experts.

The Data Privacy Act provides that the "determination of the appropriate level of security under this section 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."[117] It is important that an individual or organization processing personal data be aware of the risks represented by the their processing. One of the recommendations of the National Privacy Commission is to conduct a privacy impact assessment, which should guide the implementation of policies, procedures and security measures for data protection. In addition, the National Privacy Commission provided further guidelines on data protection through its circulars on *Security of Personal Data in Government Agencies*,[118] *Data Sharing involving Government Agencies*[119] and *Personal Data Breach Management.*[120]

The obligation to implement security measures cuts across industries, and covers both public and private sector. These may entail additional time, costs and manpower, but to refuse to assume the obligation for data protection while continuing to enjoy the benefits of using personal data is irresponsible and shows disregard for rights of data subjects. In cases of personal data breach, the cost of a breach will be much higher than the cost of compliance.[121]

[112] IRR, §25.

[113] Data Privacy Act, §20; IRR, §26.

[114] Data Privacy Act, §20; IRR, §27.

[115] Data Privacy Act, §20; IRR, §28.

[116] Data Privacy Act, §20; IRR, §28.

[117] Data Privacy Act, §20; IRR, §29.

[118] NPC Circular 16-01, Security of personal data in government agencies (Oct. 10, 2016).

[119] NPC Circular 16-02, Data sharing agreement involving government agencies (Oct. 10, 2016).

[120] NPC Circular 16-03, Personal Data breach management (Dec. 15, 2016).

[121] Cost of Data Breach Study: Global Analysis, (May 2015), available at https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF (last accessed Dec. 29, 2016); Robert Hackett, Data Breaches Now Cost $4 Million on Average (16 June 2016), available at http://fortune.com/2016/06/15/data-breach-cost-study-ibm/ (last accessed Dec. 29, 2016).

As in most cases in life, an ounce of prevention is better than a pound of cure. It is well to note that violation of the Data Privacy Act may correspond to criminal acts, for which the law imposes heavy penalties.[122] In addition to recommending the prosecution of crimes to the Department of Justice (DOJ),[123] the National Privacy Commission may impose sanctions for violations of the Act, such as:

1. Issuing compliance or enforcement orders;
2. Awarding indemnity on matters affecting any personal data, or rights of data subjects;
3. Issuing cease and desist orders, or imposing a temporary or permanent ban on the processing of personal data, upon finding that the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects;
4. Recommending to the Department of Justice (DOJ) the prosecution of crimes and imposition of penalties specified in the Act;
5. Compelling or petitioning any entity, government agency, or instrumentality, to abide by its orders or take action on a matter affecting data privacy;
6. Imposing administrative fines for violations of the Act, these Rules, and other issuances of the Commission.[124]

In order to ensure free flow of information and enjoy the benefits of technological advancements, those involved in the processing of personal data must commit to comply with the law, which means upholding the rights of data subjects, adhering to data privacy principles and implementing adequate safeguards for data protection. The Data subjects deserve no less

## IV. Culture of Privacy

The Data Privacy Act of 2012 is a law that upholds the right to information privacy. It puts at center stage the data subject or the individual whose personal data is being collected, accessed, used or stored. Those who process the personal data of data subjects are either the personal information controllers or personal information processors, and the law requires them to adhere to the data privacy principles of transparency, legitimate purpose and proportionality. The personal information controllers and personal information processors are also mandated to implement organizational, physical and technical security measures appropriate to the risks represented by their processing. The National Privacy Commission, the body tasked to administer and implement the law, is mandated to assist both public and private sector in complying with the Act, and to provide a remedy for those persons who may have experienced a privacy violation or personal data breach.

The Data Privacy Act is a statute that heavily borrows from similar laws or regulations in other countries. It is a comprehensive law that if enforced effectively would significantly increase trust and confidence in companies processing personal data in the Philippines. This is important if the country intends to continue attracting foreign investment and capturing

[122] Data Privacy Act, §§25-37.

[123] Data Privacy Act, §7(i).

[124] IRR , §9(f); *See also* Data Privacy Act, §§7 (a)(b)(c)(d)(i); *See also* Soriano v. Laguardia, G.R. No. 164785, April 29, 2009.

the market for Business Process Outsourcing industry, among others. Internationally, many countries have an established data privacy framework, and their laws restrict transfer of personal data to jurisdictions without an adequate level of protection. The Philippines must meet the challenge of demonstrating a robust data protection regime, not just for the potential economic gains, but also because the digital age requires protection of data subjects.

There is a need to embrace a culture of privacy if true change is to be achieved. Both public and private sectors must acknowledge information privacy as an important component of nation building. Complying with the Data Privacy Act should not be seen as a burden, but as a means towards establishing best practices that would, in the end, be for the benefit of all. Complying with the Data Privacy Act should not be seen as an obstacle, but as a foundation for establishing best practices, that would, in the end, be for the benefit of all. For the people, this requires awareness of their rights under the Act, an appreciation of the value of their personal data, and their own commitments to upholding the right to information privacy.

Admittedly, embracing a culture of privacy is not without challenges. The right to privacy had a strong proponent in Justice Louis Brandeis who wrote *The Right to Privacy*[125] with Samuel D. Warren more than a century ago. Justice Brandeis continued articulating the right to privacy as member of the Supreme Court, notably in his dissent in *Olmstead v. US*, [126] but it would not be until decades later that the right to privacy would be acknowledged as a fundamental human right.[127] It would seem, however, that the right to privacy remains hounded by continuing questions on its relevance.

Indeed, one can ask why privacy, particularly information privacy, should matter. What is the place of the right to privacy in a digital world where people freely share details about their personal lives? What is wrong in sharing personal data in exchange of economic or social benefits? Why should privacy be important when majority of the Filipinos worry about how to put food on the table, where to get medicine or find work or how to send their children to school? Why should privacy be important when one has nothing to hide?

It should not be surprising that the right to privacy, by default, has become the expendable right. The right to privacy is readily sacrificed because its violation is relegated to simply being an inconvenience that one can live with in exchange for tangible benefits. This is particularly true for information privacy. Thus, people fill in a raffle entry with their personal details for a chance to win a prize. They would avail of reward and discount cards even if told that data about their spending habits will be collected. They will share their personal data for fifteen minutes of internet fame. The danger, however, is not that people are willing to give up their privacy, but that they do so because privacy for them has little value.

Embracing a culture of privacy means changing this mindset. The value of information privacy goes beyond protecting personal data against unauthorized disclosure to prevent identity theft or related crimes. Justice Brandeis considered the right to privacy as being written in the Constitution to secure the "conditions favorable to the pursuit of happiness."[128] He

[125] Brandeis, Louis D. and Warren, Samuel D., The Right to Privacy, Harvard Law Review Volume IV, No. 5 (15 December 1890), available at http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm (last accessed on 12 December 2016).

[126] Brandeis J, dissenting in *Olmstead v. United States*, 277 U.S. 438 (1928).

[127] Griswold v. Connecticut 381 U.S. 479 (1965). Earlier decisions that relate to the Right to privacy include Meyer v. State of Nebraska 262 U.S. 390 (1923) and Olmstead v. U.S. 277 U.S. 438 (1928).

[128] Olmstead v. United States 277 U.S. 438 (04 June 1928).

believed in man's spiritual nature, and how man would aspire for more than material things. [129] Privacy should be seen as being inherent in the freedoms enshrined in the Constitution. In the same vein, information privacy is necessary to realize all the benefits of being in a society governed by the rule of law. An individual's personal data can both uplift and destroy. When privacy is trivialized, it becomes easier to corrode the human spirit, exposing society to attacks against fairness, justness and common decency. It becomes easy to disregard the privacy of others, paying no heed to consequences.

People share unverified reports and use personal data to shame, bully and spread misinformation, without regard to how quickly reputations are destroyed. An utter indifference to privacy is seen when medical conditions of patients are disclosed and sensitive procedures performed on patients are published online. The fact of a successful treatment does not justify invasions of privacy. These violations of privacy can also be acts of depravity, like those parents using poverty as justification for selling sexual photographs of minors, or allowing their young children to stand naked before a web camera for cash, thinking "no harm, no foul."

Disregard for privacy can also be discriminating. People are quick to waive their right to information privacy—even more so, for those who are underprivileged and who have less in life. It is often easy to ask them to consent to the use of their personal data if what they will get in return go to basic needs-food, medicine, shelter. At a certain point, however, the right to privacy should not be a luxury that is reserved for a few. It should never be the case, for example, that a patient in a government charity hospital deserves less privacy than a prominent personality in a private hospital. The right to information privacy is especially vital when it involves those who feel powerless to claim it, either because they are unaware of its existence or because they are constrained by circumstance to waive their rights.

The right to information privacy shields people from the awesome powers of the state, affords individuals the freedom to make decisions about themselves, and guarantees that there will be accountability when the right is violated. To this end, government, private sector and individuals should exert efforts towards protection of personal data. The zones of privacy should be zealously guarded. Embracing a culture of privacy requires that people do not become complacent, lest the society becomes conditioned that privacy does not matter. Everyone is a data subject and the right to privacy is for all. Becoming callous to privacy violations corrupts the foundations of fundamental rights, making people more exposed and vulnerable with every violation. Upholding the right to privacy and information privacy would be a collective commitment to the empowerment of people to exercise control over their lives free from unwarranted intrusions. While the right to privacy is not absolute, any infringement should be allowed only when absolutely necessary, and never to the extent of sacrificing human dignity.

[129] *Id.*