From Atoms to Bits: Personal Data Privacy and Security in the Information Society

Marck Joseph I. Macaraeg[*]

I. INTRODUCTION

> *The financial value of data is such that individual privacy is often set aside in the pursuit of commercial advantage. The information society makes it easy for individuals to be monitored and tracked [—] how much data are we willing to trade for convenience? How does the law strike a balance between data privacy and data brokering?*
>
> — Andrew Murray[1]

---

* '12, J.D., Ateneo de Manila University School of Law. The Author is a Foreign Consulting Attorney at Kelvin Chia Yangon Ltd. Previously, he was an Associate at Gatmaytan Yap Patacsil Gutierrez & Protacio. His practice primarily involves

The collection, use, and processing of information has become the foundation upon which the information society[2] has been built. Information is now a basic asset — the fuel — driving the information economy.[3] As Professor Ian Walden had observed, during the dotcom bubble,[4] "much of the value ascribed by stock markets to companies, such as eBay and lastminute.com, was based on the personal data they held [—] millions of registered users, rather than the products and services they had sold."[5] Today, four of the world's five most valuable companies — Apple, Alphabet

---

corporate and commercial transactions, including regulatory compliance, mergers and acquisitions, competition law, and technology, media, and telecommunications. He also serves as a coach and adviser of international law moot court teams of the Ateneo de Manila University School of Law.

Cite as 62 ATENEO L.J. 223 (2017).

1. ANDREW MURRAY, INFORMATION TECHNOLOGY LAW: THE LAW AND SOCIETY 539 (3d ed. 2016).
2. The information society is characterized by the shift from industrial production to one where information and digital technologies drive economic, social, and political activity. It gives rise to a corollary economic model referred to as the "information economy." In this connection, the three main characteristics of the information society are as follows: (a) information is used as an economic resource, i.e., organizations make greater use of information to increase their efficiency, to stimulate innovation, and to increase their effectiveness and competitive position; (b) there is greater use of information in the general public; and (c) the development of the information sector within the economy aims to satisfy the general demand for information facilities and services. Nick Moore, *The information society*, *in* WORLD INFORMATION REPORT 1997/98 271-72 (Yves Courrier & Andrew Large eds., 1997).
3. Ian Walden, *Privacy and Data Protection*, *in* COMPUTER LAW: THE LAW AND REGULATION OF INFORMATION TECHNOLOGY 573 (Chris Reed & John Angel eds., 2011).
4. The dot-com bubble was a period of excessive speculation and growth in the information and communication technology (ICT) sector between 1997 and 2001. During this period, the value of equity markets grew exponentially, with the technology-dominated NASDAQ index rising from under 1,000 to more than 5,000 between 1995 and 2000. *See* Eric Roberts, A History of Capacity Challenges in Computer Science, *available at* http://cs.stanford.edu/people/eroberts/CSCapacity.pdf (last accessed Aug. 10, 2017).
5. Walden, *supra* note 3.

(Google's parent company), Microsoft, and Facebook[6] — all come from the information and communications technology (ICT) sector and hold vast amounts of information.

Similarly, the internet and digital technologies, which allow the seamless flow of information across networks and international borders, are transforming Philippine society and its economy. In the past decade, the country has witnessed the historically unprecedented growth of electronic commerce, social media, and business process outsourcing (BPO). Indeed, the Philippines is now widely regarded as the BPO,[7] social media,[8] and selfie[9] capital of the world;[10] and its economy relies substantially on ICT

6. Stephen Gandel, *These Are the 10 Most Valuable Companies in the Fortune 500*, FORTUNE, Feb. 4, 2016, *available at* fortune.com/2016/02/04/most-valuable-companies-fortune-500-apple (last accessed Aug. 10, 2017).

7. Don Lee, *The Philippines has become the call-center capital of the world*, L.A. TIMES, Feb. 1, 2015, *available at* www.latimes.com/business/la-fi-philippines-economy-20150202-story.html (last accessed Aug. 10, 2017).

8. Yahoo! News, Research Confirms: The Philippines is Still the Social Media Capital of the World, *available at* https://sg.news.yahoo.com/research-confirms-philippines-still-social-033045566.html (last accessed Aug. 10, 2017).

9. Chris Wilson, *The Selfiest Cities in the World: TIME's Definitive Ranking*, TIME, Mar. 10, 2014, *available at* time.com/selfies-cities-world-rankings (last accessed Aug. 10, 2017).

10. The Philippine business process outsourcing (BPO) industry has been driving the country's overall growth in the last decade. By 2012, the industry's total contribution to value-added growth through services exports, real estate, construction, retail trade, and telecommunications was estimated to be around 10% of the Gross Domestic Product. World Bank Philippine Office East Asia and Pacific Region, Philippine Development Report: Creating More and Better Jobs at 127, *available at* http://www.documents.worldbank.org/curated/en/895661468092965770/pdf/ACS58420WP0P120Box0382112B00PUBLIC0.pdf (last accessed Aug. 10, 2017). Moreover, the Philippines has also become a global outsourcing hub, overtaking India as the world's BPO capital. In recent years, however, there appears to be a significant shift in the industry from low-end, voice-based BPOs to more sophisticated knowledge process outsourcing in fields such as web development, information technology, actuarial engineering, medical transcription, banking and finance, accounting, and law. J. Albert Gamboa, *Growth prospects for the BPO industry*, BUSINESSWORLD, May 1, 2015, *available at* www.bworldonline.com/content.php?section=Finance&title=growth-prospects-for-the-bpo-industry&id=107125 (last accessed Aug. 10, 2017).

networks and infrastructure to sustain its growth.[11] This was observed by Supreme Court Chief Justice Maria Lourdes P.A. Sereno, who opined that

> ICTs are fast becoming the most widely used and accessible means of communication and of expression. Educational institutions encourage the study of ICT and the acquisition of the corresponding skills. Businesses, government institutions[,] and civil society organizations rely so heavily on ICT that it is no exaggeration to say that, without it, their operations may grind to a halt. News organizations are increasingly shifting to online publications, too. The introduction of social networking sites has increased public participation in socially and politically relevant issues. In a way, the [i]nternet has been transformed into ['']freedom parks.['][12]

That being said, while the rapidly evolving ICT sector has been an unequivocal source of innovation and growth,[13] the rise of the information economy also carries its own associated risks.[14] Particularly, considering that a substantial share of the information fuelling the information economy pertains to personal data, its use and potential misuse, or even abuse, engage and impinge on the right to privacy.[15] In this regard, as information continues to increase in value, and as digital technologies evolve to facilitate the faster and ever more seamless flow of information, these associated risks similarly increase.[16] It is in this context that the legal regime governing individuals and society in the information age must be examined and made to appropriately adapt.

---

11. *See generally* Department of Information and Communications Technology, National Cybersecurity Plan 2022, *available at* www.dict.gov.ph/wp-content/uploads/2017/04/FINAL_NationalCyberSecurityPlan2022-1.pdf (last accessed Aug. 10, 2017).

12. Disini, Jr. v. The Secretary of Justice, 716 SCRA 237, 380 (2014) (C.J. Sereno, concurring and dissenting opinion).

13. Silja Baller, et al., *The Networked Readiness Index 2016*, *in* THE GLOBAL INFORMATION TECHNOLOGY REPORT 2016: INNOVATING IN THE DIGITAL ECONOMY 3 (Silja Baller, et al. eds., 2016).

14. This was recognized by Supreme Court Chief Justice Maria Lourdes P.A. Sereno in her separate concurring and dissenting opinion in Disini, Jr. v. Secretary of Justice, where she opined that information and communications technology "has been an enormous force for good as well as for evil." *Disini, Jr.*, 716 SCRA at 358 (C.J. Sereno, concurring and dissenting opinion).

15. Walden, *supra* note 3.

16. *Id.*

II. FROM ATOMS TO BITS: DIGITIZING THE PHYSICAL REALM

An atom is the smallest unit of matter.[17] All physical objects — from this copy of the *Ateneo Law Journal* to music tapes and CDs — are made up of atoms.[18] In this connection, inasmuch as atoms can be used to construct any and all physical objects, bits form the basic building blocks of the information society.[19] "Bit" is a truncation of the term "binary digit;" and at its most basic level, a bit can only have one of two values (represented by either a 0 or a 1).[20] Like atoms, which individually are unimpressive, it is how bits can be combined and used to construct larger, more complex systems that give them their economic value and social importance.[21] In fact, virtually every type of physical information, such as text, image, sound, or object, can be converted and represented in bits.[22] This process of representing information in bits is referred to as digitization and the information thus represented is called digital information.[23]

Before the widespread adoption of digital information, information was generally held in discrete and often poorly catalogued packets.[24] For example, libraries traditionally maintained card catalog systems where

17. Stanford Encyclopedia of Philosophy Archive: Winter 2016 Edition, Philosophy of Chemistry, *available at* https://plato.stanford.edu/archives/win2016/entries/chemistry (last accessed Aug. 10, 2017).

18. *Id.*

19. MURRAY, *supra* note 1, at 6.

20. Andrew Murray explains that

> a bit represents a single instruction to the computer. This instruction is either to do (1) or not to do (0) a particular function. The instruction is read by the brain of the computer, the [m]icroprocessor or [c]entral [p]rocessing [u]nit (CPU). The CPU may be thought of as a superfast calculator which works in binary. Bits of information are fed to the CPU from the computer memory, the CPU does a calculation and based upon the result[,] the personal computer [ ] carries out a pre-determined function.

Id.

21. *Id.*

22. *Id.*

23. For a more detailed exposition of this process, please refer to an article from Wellesley College on the matter. Wellesley College Computer Science Staff, Information Representation: Bits and Bytes, *available at* cs.wellesley.edu/~cs110/reading/information-representation.html (last accessed Aug. 10, 2017).

24. MURRAY, *supra* note 1, at 42.

bibliographic information was kept.[25] In these systems, each title would have to be manually recorded and indexed and, if a group of libraries was involved, copied and delivered to the other libraries. In addition, shelving space for these cataloging systems was limited — hence only key bibliographic information was indexed[26] — and each card catalog could be used only by one individual at any given time. Thus, adding information to the catalog and searching for information therein were both laborious and time-consuming exercises. There was also a risk that information may degrade over time due to the nature of the medium (e.g., card catalogs that are usually made of paper) and because of potential mistakes in manually encoding information each time copies are made. The development of information technology management systems, however, allows the simultaneous access of a single record of information.[27] These systems may likewise be searched almost instantaneously by any key word (e.g., in the case of books, title, author, subject, etc.),[28] and do not take as much physical space as traditional card cataloging systems. Information can also be copied quickly through the click of a button and transmitted with no degradation.[29] The Author believes that it is precisely for these reasons that the manual library card cataloging system has been effectively replaced by the online public access catalog. Atoms have become bits.

Similarly, when music is downloaded from iTunes and stored in an iPhone or iPod (instead of being kept in CDs or cassette tapes), atoms have become bits. When newspapers and magazines are read online (instead of through their print versions), atoms have become bits. And when videos are uploaded and streamed on YouTube (instead of being recorded in and

25. A library catalog or library catalogue is a register of all bibliographic items found in a library or group of libraries. Encyclopædia Britannica, Cataloging, *available at* https://www.britannica.com/topic/library/Cataloging#ref320751 (last accessed Aug. 10, 2017).

26. A bibliographic item can be any information entity (e.g., books, computer files, graphics, realia, cartographic materials, etc.) that is considered library material (e.g., a single novel in an anthology), or a group of library materials (e.g., a trilogy), or linked from the catalog (e.g., a webpage) as far as it is relevant to the catalog and to the users (patrons) of the library. *Id.*

27. MURRAY, *supra* note 1, at 42.

28. *Id.*

29. Walden, *supra* note 3, at 592 & Elizabeth Buchanan & James Campbell, *New Threats to Intellectual Freedom: The Loss of the Information Commons through Law and Technology in the US*, *in* INTELLECTUAL PROPERTY RIGHTS IN A NETWORKED WORLD: THEORY AND PRACTICE 231 (Richard A. Spinello & Herman T. Tavani eds., 2005).

watched through DVDs), atoms have become bits.[30] These illustrate the supremacy of digital information over its physical or analog counterpart, and demonstrate why digital information is commercially more valuable than analog information.[31] In *Information Technology Law*, Professor Andrew Murray, citing Professor Fred H. Cate, identified the following characteristics of digital information that gave rise to this:

> (1) Information is easier to generate, manipulate, transmit, and store[;]
>
> (2) The cost of collecting, manipulating, storing, and transmitting data is lowered[;]
>
> (3) Electronic information has developed an intrinsic value not found in [analog] information due to its very nature[;]
>
> (4) The operating parameters of computer systems and networks generate additional digital information through back-up copies and cache copies.[32]

Digital convergence has also allowed digital data to be traded across platforms more easily.[33]

---

30. According to William H. Janeway,

> [w]hen a search is conducted on Google, the work of finding relevant information by consulting physical repositories of information, with or without the additional work of a librarian, has been replaced[—] atoms have become bits. When a consumer buys a book on Amazon, massive economies of scale are deployed to reduce the aggregate work previously distributed across multiple supply chains: atoms have become bits. When a designer uses a software program to specify the characteristics of a prototype for submission to a 3D printer, the work of hand-crafting a model has been replaced[—] atoms have come bits. When one of many customers requests transportation through Uber or overnight accommodation through Airbnb and the request is fulfilled by one of many possible suppliers, the work of matching demand and supply has been radically reduced[—] atoms have become bits.

William H. Janeway, *From Atoms to Bits To Atoms: Friction On The Path To The Digital Future*, FORBES, July 30, 2015, *available at* https://www.forbes.com/sites/valleyvoices/2015/07/30/from-atoms-to-bits-to-atoms-friction-on-the-path-to-the-digital-future/#634e5a0227bc (last accessed Aug. 10, 2017).

31. MURRAY, *supra* note 1, at 326.

32. *Id.* at 43 (citing FRED H. CATE, PRIVACY IN THE INFORMATION AGE 14-16 (1997)). *See also* Moore, *supra* note 2, at 273.

33. MURRAY, *supra* note 1, at 43.

Thus, companies increasingly want personal data.[34] In fact, when then European Union (EU) Justice Commissioner Viviane Reding introduced the EU's new General Data Protection Regulation,[35] she referred to personal data as the "currency" of the "digital economy."[36] In this regard, multibillion dollar industries have emerged to capitalize on the explosion of digital data — some companies gather data to act as an advisor to others, others do so to improve their services, some carry out market research using gathered data with a view to selling their insights or tailored advertising products to clients, and others gather information to sell as packaged data for purposes of product development, advertising, and promotion.[37] The International Data Corporation (IDC) foresees global revenue for big data and business analytics to rise from US$130 billion in 2016 to more than US$203 billion by 2020.[38] According to Dan Vesset, IDC Group Vice President, the "availability of data, a new generation of technology, and a cultural shift toward data-driven decision making continue to drive demand for big data and analytics technology and services."[39] Accordingly, by reason of the increasing value of personal data, these companies have developed automated digital processes allowing the more efficient collection and processing of personal data.[40] As will be explained below, however, these developments come with informational privacy risks.[41]

---

34. *Id.* at 542.

35. Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation) 2016 O.J. (L 119) 1 (EU) [hereinafter General Data Protection Regulation].

36. *Privacy laws: Private data, public rules*, ECONOMIST, Jan. 28, 2012, *available at* www.economist.com/node/21543489 (last accessed Aug. 10, 2017).

37. MURRAY, *supra* note 1, at 542.

38. Press Release *by* International Data Corporation, *Double-Digit Growth Forecast for the Worldwide Big Data and Business Analytics Market Through 2020 Led by Banking and Manufacturing Investments, According to IDC* (Oct. 3, 2016) *available at* www.idc.com/getdoc.jsp?containerId=prUS41826116 (last accessed Aug. 10, 2017).

39. *Id.*

40. MURRAY, *supra* note 1, at 542.

41. *Id.*

III. THE RIGHT TO PRIVACY IN THE INFORMATION SOCIETY

While the privacy of personal data is not a novel issue, developments in digital technologies and the internet have made its protection a particularly difficult task.[42] The challenge of applying rules made for atoms to the digital world of bits has previously been identified by Chief Justice Sereno, who opined that the task "is complicated by the context in which [it should] be discharged [—] a rapidly evolving [ICT sector],"[43] where regulators are "forced to grapple with the challenge of applying, to the illimitable cyberspace, legal doctrines that have heretofore been applied only to finite physical space."[44] For this reason, before examining the legal framework governing the privacy of personal data, the Author finds it necessary to first discuss the constitutional right to privacy, the extent to which it extends to personal information, and the threats posed by the information society to this constitutional right.

A. The Constitutional Right to Informational Privacy

The right to privacy has been alluded to as the "beginning of all freedoms,"[45] the "most comprehensive of rights,"[46] and the "right most valued by civilized men."[47] It derives from the common law recognition that "a man's house [is] his [or her] castle, impregnable, often, even to its own officers engaged in the execution of its commands."[48] In its most basic sense, the right to privacy involves an individual's "inalienable right to be let alone."[49] Drawing from American jurisprudence and constitutional law practice, Philippine law has long recognized and protected the "constitutional right to privacy." According to the Supreme Court in *Morfe v. Mutuc*[50] —

42. JACQUELINE KLOSEK, DATA PRIVACY IN THE INFORMATION AGE 7 (2000).

43. *Disini, Jr.*, 716 SCRA at 358 (C.J. Sereno, concurring and dissenting opinion).

44. *Id.*

45. Public Utilities Commission v. Pollak, 343 U.S. 451, 467 (1952).

46. Olmstead v. United States, 277 U.S. 438, 478 (1928) (J. Brandeis, dissenting opinion).

47. *Id.*

48. Kilusang Mayo Uno v. Director-General, National Economic Development Authority, 487 SCRA 623, 666 (2006) (J. Ynares-Santiago, dissenting opinion).

49. *Id.*

50. Morfe v. Mutuc, 22 SCRA 424 (1968) (citing Grisworld v. Connecticut, 381 U.S. 479, 484 (1965)).

> The [leading case of *Grisworld v. Connecticut*] invalidated a Connecticut statute which made the use of contraceptives a criminal offense on the ground of its amounting to an unconstitutional invasion of the right of privacy of married persons; rightfully[,] it stressed ['Ja relationship lying within the zone of privacy created by several fundamental constitutional guarantees.['] It has wider implications though. The constitutional right to privacy has come into its own.
>
> *So it is likewise in our jurisdiction. The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection.* The language of [Professor Thomas I.] Emerson is particularly apt [—] ['JThe concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his [or her] life, is the hallmark of the absolute [S]tate. In contrast, a system of limited government, safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the [S]tate can control. Protection of this private sector[ ]—[ ]protection, in other words, of the dignity and integrity of the individual[ ]—[ ]has become increasingly important as modern society has developed. All the forces of a technological age[ ]—[ ]industrialization, urbanization, and organization [ ]—[ ]operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society.[']51

Indeed, unlike in the United States where the Constitution does not expressly mention a "right to privacy," and, thus, the right only exists within the "penumbra" of other constitutionally protected rights,52 the Philippine Constitution expressly enshrines and protects the right to privacy. According to the Supreme Court in *Ople v. Torres*,53

> if we extend our judicial gaze[,] we will find that the right of privacy is recognized and enshrined in several provisions of our Constitution. It is *expressly* recognized in Section 3[ ](1) of the Bill of Rights:
>
> ['Section 3]. (1) The 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.[']

51. *Id.* at 444-45 (citing Thomas I. Emerson, *Nine Justices in Search of a Doctrine*, 64 MICH. L. REV. 219, 229 (1965)) (emphasis supplied).

52. *Grisworld*, 381 U.S at. 484.

53. Ople v. Torres, 293 SCRA 141 (1998).

> Other facets of the right to privacy are protected in various provisions of the *Bill of Rights*, viz:
>
> ['Section 1]. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.
>
> [Section 2.] The right of the people to be secure in their persons, houses papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he [or she] may produce, and particularly describing the place to be searched and the persons or things to be seized.
>
> ...
>
> [Section 6]. The liberty of abode and of changing the same within the limits prescribed by law shall not be impaired except upon lawful order of the court. Neither shall the right to travel be impaired except in the interest of national security, public safety, or public health, as may be provided by law.
>
> ...
>
> [Section 8]. The right of the people, including those employed in the public and private sectors, to form unions, associations, or societies for purposes not contrary to law shall not be abridged.
>
> [Section 17]. No person shall be compelled to be a witness against himself [or herself].[']
>
> *Zones of privacy* are likewise recognized and protected in our laws. The *Civil Code* provides that ['][e]very person shall respect the dignity, personality, privacy[,] and peace of mind of his [or her] neighbors and other persons['] and punishes as actionable torts several acts by a person of meddling and prying into the privacy of another. It also holds a public officer or employee or any private individual liable for damages for any violation of the rights and liberties of another person, and recognizes the privacy of letters and other private communications. The *Revised Penal Code* makes a crime the violation of secrets by an officer, the revelation of trade and industrial secrets, and trespass to dwelling. Invasion of privacy is an offense in special laws like the Anti-Wiretapping Law, the Secrecy of Bank Deposits Act[,] and the Intellectual Property Code. The Rules of Court on privileged communication likewise recognize the privacy of certain information.[54]

54. *Id.* at 156–58 (citing PHIL. CONST. art. 3, §§ 1–3, 6, 8, & 17; An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE], Republic Act

Moreover, and perhaps more importantly, Philippine law recognizes that the constitutional right to privacy extends to the right to informational privacy. This departs from the United States' practice where the Supreme Court has not yet acknowledged (although it has alluded to)[55] a constitutional right to informational privacy.[56] In this regard, the Philippine Supreme Court in *Ople* declared Administrative Order (A.O.) No. 308, on the adoption of a national computerized identification reference system, as unconstitutional for violating the right to informational privacy.[57] According to the Court,

> [*W*]*e prescind from the premise that the right to privacy is a fundamental right guaranteed by the Constitution*, hence, it is the burden of government to show that A.O. No. 308 is justified by some compelling state interest and that it is narrowly drawn. ... .
>
> The *heart of A.O. No. 308* lies in its Section 4 which provides for a Population Reference Number (PRN) as a ['] common reference number to establish a linkage among concerned agencies['] through the use of ['] Biometrics Technology['] and ['] computer application designs.[']
>
> ...
>
> In the last few decades, technology has progressed at a galloping rate. Some science fictions are now science facts. Today, biometrics is no longer limited to the use of fingerprint to identify an individual. It is a new science that uses various technologies in encoding any and all biological characteristics of an individual for identification. It is noteworthy that A.O. No. 308 does not state what specific biological characteristics and what particular biometrics technology shall be used to identify people who will seek its coverage. Considering the banquet of options available to the

---

No. 386, arts. 26 & 32 (1949); An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE], Act No. 3815, arts. 229-230, 280-281, & 292 (1932); An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purposes, Republic Act No. 4200 (1965); An Act Instituting a Foreign Currency Deposit System in the Philippines, and for Other Purposes [Foreign Currency Deposit Act], Republic Act No. 6426 (1972); An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, Providing for its Powers and Functions, and for Other Purposes [INTELL. PROP. CODE], Republic Act No. 8293 (1997); & 1989 RULES ON EVIDENCE, rule 130, § 24) (emphasis supplied).

55. *See* Whalen v. Roe, 429 U.S. 589, 598-99 (1977).

56. *Kilusang Mayo Uno*, 487 SCRA at 669-70 (J. Ynares-Santiago, dissenting opinion).

57. *Ople*, 293 SCRA at 170.

> implementors of A.O. No. 308, the fear that it threatens the right to privacy of our people is not groundless.
>
> ...
>
> *We can even grant, arguendo, that the computer data file will be limited to the name, address*[,] *and other basic personal information about the individual. Even that hospitable assumption will not save A.O. No. 308 from constitutional infirmity for again said order does not tell us in clear and categorical terms how these information gathered shall be handled. It does not provide who shall control and access the data, under what circumstances*[,] *and for what purpose. These factors are essential to safeguard the privacy and guaranty the integrity of the information.* Well to note, the computer linkage gives other government agencies access to the information. Yet, there are no controls to guard against leakage of information. When the access code of the control programs of the particular computer system is broken, an intruder, without fear of sanction or penalty, can make use of the data for whatever purpose, or worse, manipulate the data stored within the system.
>
> ...
>
> The ability of a sophisticated data center to generate a comprehensive *cradle-to-grave* dossier on an individual and transmit it over a national network is one of the most graphic threats of the computer revolution. The computer is capable of producing a comprehensive dossier on individuals out of information given at different times and for varied purposes. It can continue adding to the stored data and keeping the information up to date. Retrieval of stored data is simple. *When information of a privileged character finds its way into the computer, it can be extracted together with other data on the subject. Once extracted, the information is putty in the hands of any person. The end of privacy begins.*[58]

In fact, in recognition of the constitutional right to informational privacy, the Supreme Court has promulgated the rule on the Writ of *Habeas Data* in 2008.[59] The Writ, according to the Court, is an "independent and summary remedy to protect the right to privacy [—] *especially* the right to informational privacy"[60] or the "right to control information regarding oneself."[61] Indubitably, therefore, insofar as Philippine constitutional law is

58. *Id.* at 158-163 (citations omitted) (emphasis supplied).

59. *See* THE RULE ON THE WRIT OF HABEAS DATA, A.M. No. 08-1-16-SC (Jan. 22, 2008).

60. In the Matter of the Petition for the Writ of *Amparo* and *Habeas Data* in Favor of Noriel H. Rodriguez: Rodriguez v. Macapagal-Arroyo, 660 SCRA 84, 102 (2011) (citing SUPREME COURT, ANNOTATION TO THE RULE ON THE WRIT OF *HABEAS DATA* 23 (2008)).

61. *Id.*

concerned, the right to privacy includes and extends to the right to informational privacy. In other words, the security and privacy of personal information is guaranteed and protected by no less than the Philippine constitution itself. The challenge, however, is determining the extent of this constitutional right and enforcing it in the information society.

In this regard, the extent of the right to informational privacy, particularly in the context of the information society where information is shared in varying modes and degrees through the ICT and internet infrastructure, can be determined by using the *two-fold test* traditionally applied by the Supreme Court in examining privacy claims.[62] Under this test, an informational privacy claim should be upheld if the claimant establishes that, *subjectively*, he or she has exhibited an actual expectation of privacy; and *objectively*, his or her subjective expectation of privacy is one that society is prepared to accept as reasonable.[63]

The subjective element of the test involves the assessment of an individual's expectation of privacy in a given situation or context, which is manifested through his or her conduct.[64] For instance, individuals who create social media accounts may have varying expectations of privacy depending on the privacy settings they each have chosen for their respective accounts or for each post that they upload on those accounts. As will be explained in greater detail below, utilizing the appropriate privacy or security tools, not only in social media but in most digital transactions, may have serious implications on an individual's objective expectation of privacy. The objective element, on the other hand, is determined by the customs, norms, and practices of the community, all of which may limit or extend an individual's expectation of privacy.[65] Hence, the reasonableness of a person's expectation of privacy is determined on a case-to-case basis since it depends on the factual circumstances surrounding the case.[66] This two-fold test shall be used in determining the extent of the right to informational privacy in the information society.

62. Pollo v. Constantino-David, 659 SCRA 189, 242 (2011).

63. *Id.* (citing Katz v. United States, 389 U.S. 347, 350-51 (1967) (J. Harlan, concurring opinion)).

64. Peter Goldberger, *Consent, Expectations of Privacy, and the Meaning of Searches in the Fourth Amendment*, 75 J. CRIM. L. & CRIMINOLOGY 319, 322 (1984).

65. Spouses Hing v. Choachuy, Sr., 699 SCRA 667, 679 (2013) (citing *Ople*, 293 SCRA at 164).

66. *Id.*

B. Threats to Informational Privacy

In no small measure, the information society has transformed the way individuals deal and interact with each other and with society as a whole; particularly, in the manner by which identity is increasingly being divorced from the individual himself or herself.[67] To illustrate, an individual, through a smartphone connected to the internet, may readily access his or her bank accounts by using his or her bank's mobile device application and typing in his or her username and password. From there, that individual may check his or her account balance, pay his or her utility bills, or transfer money to another account. Likewise, he or she may go to Google Play or the Apple Store and, by using his or her smartphone's fingerprint (or in some instances, iris or facial) scanner, purchase, and download applications. He or she may likewise log on to any one of his or her social media accounts such as Facebook and upload digital images or send an instant message to virtually anyone wherever in the world located.

These situations demonstrate that individuals in the information society rely heavily on proxies and credentials — such as passwords, user IDs, account numbers, and personal or biometric data — to identify themselves online and engage in digital transactions, which may have real world implications.[68] Unfortunately, this practice places their identities at a unique and unprecedented risk because "a large proportion of transactions are validated [only] by reference to [such] proxies rather than direct identification."[69] This leads to the two distinct threats of identity theft or fraud and the misapplication, mishandling, or misprocessing of data.[70] Indeed, the ability of individuals or agents to easily access personal information in the information society increases the risks of harm, inequality, discrimination, and loss of autonomy.[71] Accordingly, Professor Murray suggests that "a strict legal regime [ ] [must] regulate the industry as a

67. MURRAY, *supra* note 1, at 486.

68. *Id.*

69. *Id.*

70. *Id.*

71. Stanford Encyclopedia of Philosophy Archive: Spring 2016 Edition, Privacy and Information Technology, *available at* https://plato.stanford.edu/archives/spr2016/entries/it-privacy (last accessed Aug. 10, 2017). For example, your enemies may have less difficulty finding out where you are, users may be tempted to give up privacy for perceived benefits in online environments, and employers may use online information to avoid hiring certain groups of people. Furthermore, systems rather than users may decide which information is displayed, thus confronting users only with news that matches their profiles.

whole."[72] This regime should ensure that the rights of individuals whose data are being collected are respected and upheld, the processing of data remains fair and secure, and an enforcement procedure is available.[73]

IV. ENFORCING THE RIGHT TO INFORMATIONAL PRIVACY: THE DATA PRIVACY ACT OF 2012 AND ITS IMPLEMENTING RULES AND REGULATIONS

The Data Privacy Act[74] (DPA) is the first comprehensive law of general application governing the security and privacy of personal data in the Philippines.[75] It was enacted on 15 August 2012 and took effect on 8 September 2012;[76] while its Implementing Rules and Regulations[77] (DPA IRR) was promulgated on 24 August 2016 and became enforceable on 9 September 2016.[78] Notably, the provisions of the DPA were based mainly on and incorporate principles embodied in the Asia Pacific Economic Cooperation (APEC) Privacy Framework[79] and the European Union (EU)

72. MURRAY, *supra* note 1, at 542-43.

73. *Id.*

74. *See* 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 of 2012], Republic Act No. 10173 (2012).

75. Prior to the Data Privacy Act, statutory provisions governing the confidentiality of personal information in certain sectors were found in various laws. *See, e.g.*, Providing for Incentives in the Pursuit of Economic Development Programs by Restricting the Use of Documents and Information Vital to the National Interest in Certain Proceedings and Processes, Presidential Decree No. 1718 (1980).

76. *See* Data Privacy Act of 2012, § 45.

77. National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016). The Implementing Rules and Regulations (IRR) provides in greater detail the requirements that must be complied with by individuals and entities collecting and processing personal data as well as the sanctions for violations of the law. *See* Marck Joseph I. Macaraeg, et al., Data Privacy Overview: Philippines, *available at* http://www.dataguidance.com (last accessed Aug. 10, 2017).

78. *See* Rules and Regulations Implementing the Data Privacy Act of 2012, § 72.

79. 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 Aug. 10, 2017).

Data Protection Directive[80] (EU Directive). Moreover, reform initiatives that led to the EU General Data Protection Regulation (GDPR) were also considered.[81]

The National Privacy Commission (NPC), the body mandated to administer and implement the DPA, was constituted some time in March 2016.[82] Its functions include rule-making, advisory, public education, compliance and monitoring, investigations and complaints, and enforcement.[83] For purposes of policy and program coordination, the NPC is attached to the newly established Department of Information and Communications Technology (DICT) together with the National Telecommunications Commission and Cybercrime Investigation and Coordination Center.[84]

A. Protected Information

The DPA and DPA IRR cover personal information, sensitive personal information, and privileged information. In this regard, the DPA and DPA IRR define "personal information" as "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."[85] Based on this definition, personal information includes, among others, someone's name, address, and telephone or mobile numbers. In the information society, it may also

80. 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, 1995 O.J. (L 281) (EU) [hereinafter Directive 95/46/EC].

81. Ivy D. Patdu & Rasiele Rebekah DL. Rellosa, *Data Privacy Act*, 5 BEDAN REV. 79, 88 (2017). *See* General Data Protection Regulation, *supra* note 35.

82. Raymund Enriquez Liboro was appointed National Privacy Commission Commissioner and Chairman, while Atty. Ivy D. Patdu and Damian Domingo O. Mapa were appointed Deputy Commissioners. National Privacy Commission, About Us: The Commission, *available at* https://privacy.gov.ph/about-us/ (last accessed Aug. 10, 2017).

83. Rules and Regulations Implementing the Data Privacy Act of 2012, § 9.

84. An Act Creating the Department of Information and Communications Technology, Defining its Powers and Functions Appropriating Funds Therefor, and for Other Purposes [Department of Information And Communications Technology Act of 2015], Republic Act No. 10844, § 15 (2016).

85. Data Privacy Act of 2012, § 3 (g) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (l).

include, in some instances, device identifiers such as Media Access Control (MAC) addresses and internet protocol (IP) addresses.[86]

"Sensitive personal information," on the other hand, refers to personal information:

(1) [a]bout an individual's race, ethnic origin, marital status, age, color[,] and religious, philosophical[,] or political affiliations;

(2) [a]bout 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) [i]ssued 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) [s]pecifically established by an executive order or an act of Congress to be kept classified.[87]

Finally, "privileged information" refers to "any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication."[88]

Notably, while all types of personal information are protected by the DPA and DPA IRR, and while the same privacy principles apply regardless of the type of personal information involved, a stricter standard of protection is imposed on the processing of sensitive personal information.[89] For instance, the processing of sensitive personal information is generally prohibited except upon the express consent of the data subject.[90] Further, the imposable penalty for violating the DPA and DPA IRR is higher when sensitive personal information is involved.[91] Furthermore, a lower threshold

86. *See* Patrick Breyer v. Federal Republic of Germany, Judgment, Case C-582/14, ECLI:EU:C:2016:779, ¶ 65 (CJEU Oct. 19, 2016).

87. Data Privacy Act of 2012, § 3 (l) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (t).

88. Data Privacy Act of 2012, § 3 (k) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (q).

89. Macaraeg, et al., *supra* note 77.

90. Data Privacy Act of 2012, § 13 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 22.

91. *See* Data Privacy Act of 2012, ch. VIII & Rules and Regulations Implementing the Data Privacy Act of 2012, rule XIII.

is required in relation to the registration of data processing systems involving sensitive personal information.[92] This differential treatment between categories of personal information is rooted in EU data protection law, where special categories of information are given greater protection because, by their very nature, they are capable of infringing fundamental freedoms or privacy.[93]

B. Scope

The DPA applies to the processing of all types of personal information by any natural or juridical person, whether in the private or public sector.[94] For this purpose, processing is defined as "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."[95] This is a key definition since the provisions of the DPA and DPA IRR will only be triggered when the *processing* of personal information is involved. The definition of processing in the DPA and DPA IRR also follows the expansive definition under the EU Directive[96] and EU GDPR[97] and makes it clear that mere storage and consultation of personal information are considered as processing falling with the ambit of regulation.[98] In this connection, an entity that processes personal information could either be a personal information controller[99] or a personal information processor.[100]

92. Rules and Regulations Implementing the Data Privacy Act of 2012, § 47.

93. Walden, *supra* note 3.

94. Data Privacy Act of 2012, §§ 2, 3 (h), 3 (i), & 4.

95. Data Privacy Act, § 3 (j) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (o).

96. Directive 95/46/EC, *supra* note 80, art. 2 (b).

97. General Data Protection Regulation, *supra* note 35, art. 4, § 2.

98. *Cf.* R v. Brown, 1 AC 543, (HL 1996) (U.K.).

99. The Data Privacy Act of 2012 defines a "personal information controller" as "a person or organization who *controls* the collection, holding, processing[,] or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer[,] or disclose personal information on his or her behalf." Data Privacy Act of 2012, Section 3 (h). It excludes a "natural or juridical person, or any other body, who performs such functions as instructed by another person or organization" or "a natural person who processes personal data in connection with his or her personal, family, or household affairs." Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (m) (1-2). For this purpose, there is control

The DPA and DPA IRR apply to the processing of personal information, whether within or outside of the Philippines, in the following instances:

(a) the natural or juridical person involved in the processing of personal data is founded or established in the Philippines;[101]

(b) the processing relates to personal data about a Philippine citizen or Philippine resident;[102]

(c) the processing of personal data is done in the Philippines;[103] and

(d) the processing of personal data is done or engaged by an entity with links to the Philippines which include, among others, organizations that have equipment located in the Philippines that is used to process personal data or entities who have branches or subsidiaries, affiliates[,] and even affiliates in another country which has access to that personal data.[104]

The DPA and DPA IRR, however, do not apply to the following specified information, to the minimum extent of collection, access, use, disclosure, or other processing necessary for the purpose, function, or activity concerned:

(a) personal information about any individual who is or was an officer or employee of the government that relates to his or her position or functions;[105]

---

whenever "the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing." *Id.*

100. The Data Privacy Act of 2012 defines a "personal information processor" as "any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject." Data Privacy Act of 2012, Section 3 (i).

101. Data Privacy Act of 2012, § 4 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 4 (a).

102. Data Privacy Act of 2012, § 4 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 4 (b).

103. Data Privacy Act of 2012, § 4 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 4 (c).

104. Data Privacy Act of 2012, § 4 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 4 (d).

105. Data Privacy Act of 2012, § 4 (a) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 5 (a) (1).

(b) personal information processed for journalistic, artistic[,] or literary purpose, in order to uphold freedom of speech, of expression, or of the press;[106]

(c) personal information that will be processed for research purpose, intended for a public benefit;[107]

(d) personal 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, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law;[108]

(e) information necessary for banks and other bodies authorized by law to the extent necessary to comply with [Republic Act No.] 9510 or the "Credit Information System Act" and [Republic Act No.] 9160 or the "Anti-Money Laundering Act[;"][109] and

(f) personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdiction including any applicable data privacy laws, which is being processed in the Philippines.[110]

Moreover, publishers, editors, or duly accredited reporters of any newspaper, magazine, or periodical of general circulation are still bound to follow the provisions of the DPA and DPA IRR, and thus cannot be compelled to reveal the source of any news report or information appearing in the publication if it was relayed in confidence to them.[111] Further, while not specified in the DPA and DPA IRR, the Author believes that their provisions should generally not apply to the collection, use, processing,

106. Data Privacy Act of 2012, § 4 (b) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 5 (b).

107. Data Privacy Act of 2012, § 4 (c) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 5 (c).

108. Data Privacy Act of 2012, § 4 (d) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 5 (d).

109. Data Privacy Act of 2012, § 4 (e) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 5 (e).

110. Data Privacy Act of 2012, § 4 (f) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 5 (f).

111. Data Privacy Act of 2012, § 5 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 7.

disclosure, or transfer of personal data by a foreign government engaged in sovereign acts by reason of sovereign immunity.[112]

Notably, Deputy Privacy Commissioner Atty. Ivy D. Patdu and Atty. Rasiele Rebekah DL. Rellosa have expressed the view that the exceptions to the DPA and DPA IRR must be "strictly construed in order to uphold the rights of the data subject."[113]

C. Information Protection Principles

The DPA and DPA IRR provide that the processing of personal information shall be allowed subject to the principles of transparency,[114] legitimate purpose,[115] and proportionality.[116] While these principles are derived mainly from the EU Directive and GDPR, and, thus, EU practice is relevant, it should be stressed that the DPA and DPA IRR must be interpreted in the broader context of a growing international privacy framework.[117] Hence, privacy instruments adopted in other jurisdictions or by international organizations, such as the APEC Privacy Framework and

112. *See generally* The Holy See v. Rosario, Jr., 238 SCRA 524 (1994).

113. Patdu & Rellosa, *supra* note 81, at 94.

114. Section 18 (a) of the Implementing Rules and Regulations of the Data Privacy Act provides —

> 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.

Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (a).

115. Section 18 (b) of the Implementing Rules and Regulations of the Data Privacy Act states that "the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy." Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (b).

116. Section 18 (c) of the Implementing Rules and Regulations of the Data Privacy Act states that, "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." Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c).

117. *See* Patdu & Rellosa, *supra* note 81, at 95.

the Organisation for Economic Cooperation and Development Guidelines on the protection of privacy and transborder flows of personal data,[118] may also serve as a guide in interpreting these principles.

Consistent with the foregoing information protection principles, the DPA and DPA IRR thus require that the collection of personal information must be for a "declared, specified, and legitimate purpose."[119] This is corollary to the fundamental rule on consent — that the data subject's consent must be obtained through written, electronic, or recorded means[120] — prior to the collection, use, processing, disclosure, or transfer of personal information.[121] Moreover, personal information must be processed fairly and lawfully,[122] kept accurate and up to date,[123] and collected and retained only

118. Organisation for Economic Cooperation and Development (OECD), Guidelines governing the protection of privacy and transborder flows of personal data, *available at* www.refworld.org/docid/3dde56854.html (last accessed Aug. 10, 2017).

119. Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (a).

120. Data Privacy Act of 2012, § 3 (b) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (c).

121. Data Privacy Act of 2012, § 12 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (a) (1).

122. Data Privacy Act of 2012, § 11 (b). Section 21 Implementing Rules and Regulations of the Data Privacy Act provides

> Section 21. Criteria for Lawful Processing of Personal Information. Processing of personal information is allowed, unless prohibited by law. For processing to be lawful, any of the following conditions must be complied with:
>
> (a) The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;
>
> (b) The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
>
> (d) The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;

in relation to and for a period necessary for the purpose of collection.[124] Finally, further processing of personal information collected from a party other than the data subject is allowed only when (1) the consent of the data subject is obtained, (2) such further processing adheres to these principles, and (3) adequate safeguards to protect the integrity, availability, and confidentiality of personal information are in place.[125]

D. Rights of the Data Subject

The DPA recognizes the rights of data subjects to:

(a) be informed and notified when personal information pertaining to them is being processed;[126]

(b) object to the processing of their personal information, including processing for direct marketing, automated processing, or profiling;[127]

(c) reasonably access matters relating to the processing of their personal information;[128]

(e) The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;

(f) The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or

(g) The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.

Rules and Regulations Implementing the Data Privacy Act of 2012, § 21.

123. Data Privacy Act of 2012, § 11 (c) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (c).

124. Data Privacy Act of 2012, § 11 (d) & (e) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (d).

125. Rules and Regulations Implementing the Data Privacy Act of 2012, §§ 19 (e) & 20.

126. Data Privacy Act of 2012, § 16 (a) & (b) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (a).

127. Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (c).

128. *Id.* & Data Privacy Act of 2012, Section 16 (c).

(d) rectification or to dispute the inaccuracy or error in their personal information and have the personal information controller immediately correct it;[129]

(e) suspend, withdraw, or order the blocking, removal, or destruction of their personal information from the personal information controller's filing system;[130]

(f) data portability;[131] and

(g) be indemnified for damages sustained due to the processing in violation of the DPA and DPA IRR.[132]

These rights may be invoked by the lawful heirs and assigns of the data subject at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising these rights.[133]

E. Maintaining the Integrity, Availability, and Confidentiality of Personal Information

While the obligation to maintain the availability, integrity, and confidentiality of personal information applies to all entities involved in the processing of personal information, the accountability for complying with the provisions of the DPA and DPA IRR is vested primarily on the personal information controller.[134] This means that the personal information controller is responsible not only for personal information under its control or custody, but also for information outsourced or transferred to a personal information processor or another third party for processing.[135] Thus, the personal information controller is required to use contractual or other reasonable means to provide a comparable level of protection to personal

129. Data Privacy Act of 2012, § 16 (d) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (d).

130. Data Privacy Act of 2012, § 16 (e) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (e).

131. Data Privacy Act of 2012, § 18 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 36.

132. Data Privacy Act of 2012, § 16 (f) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (f).

133. Data Privacy Act of 2012, § 17 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 35.

134. Data Privacy Act of 2012, § 21 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 50.

135. *Id.*

information while it is being processed by a personal information processor or any other third party.[136]

Moreover, personal information controllers and processors are required to implement appropriate and reasonable organizational,[137] physical,[138] and technical[139] security measures to ensure the availability, integrity, and confidentiality of personal information.[140] These include the appointment of a data protection officer (DPO), who shall be an "organic employee" of the personal information controller or processor responsible for ensuring compliance with the DPA and DPA IRR.[141] A breach reporting system has likewise been established by the DPA and DPA IRR where, in certain instances, a personal information controller is required to notify the NPC and the affected data subjects within 72 hours from knowledge of a personal data breach.[142]

---

136. Data Privacy Act of 2012, § 21 (a) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 50 (a).

137. *Organizational security measures* include, among others, the appointment of compliance officers, development of procedure for processing personal data, adoption of data protection policies, and recording of processing activities. Rules and Regulations Implementing the Data Privacy Act of 2012, § 26. *See* Macaraeg, et al., *supra* note 77.

138. *Physical security measures* include, among others, limiting access to areas where personal data is processed and implementing procedures to prevent the mechanical destruction of files and equipment. Rules and Regulations Implementing the Data Privacy Act of 2012, § 27. *See* Macaraeg, et al., *supra* note 77.

139. *Technical security measures* include, among others, adopting of a security policy with respect to the processing of personal data, establishing safeguards to protect computer networks against accidental, unlawful, or unauthorized usage or interference, regularly monitoring security breaches and taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach. Rules and Regulations Implementing the Data Privacy Act of 2012, § 28. *See* Macaraeg, et al., *supra* note 77.

140. Data Privacy Act of 2012, § 20 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 25.

141. Data Privacy Act of 2012, § 21 (b) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 26 (a). *See also* National Privacy Commission, Designation of Data Protection Officers, Advisory No. 2017-01 (Mar. 14, 2017).

142. Rules and Regulations Implementing the Data Privacy Act of 2012, § 38. Notification of the breach shall be required when sensitive personal information or other information that may be used for identity fraud are reasonably believed

V. CHALLENGES AND OPPORTUNITIES

A. Commercial Communications: Informational Privacy v. Freedom of Expression

The protection of the right to informational privacy requires a delicate balancing act between the right to privacy, on the one hand, and other similar constitutionally protected rights, such as the right to freedom of expression,[143] on the other. In this regard, as mentioned above, among the rights of the data subject is the right to object to the processing of his or her personal information. This right, according to the DPA IRR, includes the right to object to the processing of personal information for direct marketing[144] or "communication by whatever means of any advertising or marketing material which is directed to particular individuals."[145] This means that direct marketing communications sent to an individual who did not consent to or who opted out of such direct marketing violate the DPA and DPA IRR. The Author notes, however, that the Supreme Court previously struck down Section 4 (c) (3) of the Cybercrime Prevention Act of 2012,[146] which prohibits unsolicited commercial communications in *Disini, Jr. v. The Secretary of Justice*,[147] supposedly for violating the right to freedom of speech and expression.[148] According to the Court:

> (3) Unsolicited Commercial Communications. [—] The transmission of commercial electronic communication with the use of computer system which seeks to advertise, sell, or offer for sale products and services are prohibited unless:
>
> (i) There is prior affirmative consent from the recipient; or

---

to have been acquired by an unauthorized person, and the personal information controller or the National Privacy Commission believes that it will give rise to a real risk of serious harm to the affected data subject. Data Privacy Act of 2012, § 20 (f) & Rules and Regulations Implementing the Data Privacy Act of 2012, § 38. *See also* National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 [NPC Circ. No. 16-03] (Dec. 15, 2016).

143. PHIL. CONST. art. III, § 4.

144. Rules and Regulations Implementing the Data Privacy Act of 2012, § 34 (b).

145. Data Privacy Act of 2012, § 3 (d).

146. An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes [Cybercrime Prevention Act of 2012], Republic Act No. 10175 (2012).

147. Disini, Jr. v. The Secretary of Justice, 716 SCRA 237 (2014).

148. *Id.* at 354.

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

The above penalizes the transmission of unsolicited commercial communications, also known as ['']spam.['] The term ['']spam['] surfaced in early internet chat rooms and interactive fantasy games. One who repeats the same sentence or comment was said to be making a ['']spam.['] The term referred to a Monty Python's Flying Circus scene in which actors would keep saying ['']Spam, Spam, Spam, and Spam['] when reading options from a menu.

The Government, represented by the Solicitor General, points out that unsolicited commercial communications or spams are a nuisance that wastes the storage and network capacities of internet service providers, reduces the efficiency of commerce and technology, and interferes with the owner's peaceful enjoyment of his property. Transmitting spams amounts to trespass to one's privacy since the person sending out spams enters the recipient's domain without prior permission. The [Office of the Solicitor General (OSG)] contends that commercial speech enjoys less protection in law.

But, *firstly*, the government presents no basis for holding that unsolicited electronic ads reduce the ['']efficiency of computers.['] *Secondly*, people, before the arrival of the age of computers, have already been receiving such unsolicited ads by mail. These have never been outlawed as nuisance since people might have interest in such ads. What matters is that the recipient has the option of not opening or reading these mail ads. That is true with spams. Their recipients always have the option to delete or not to read them.

To prohibit the transmission of unsolicited ads would deny a person the right to read his emails, even unsolicited commercial ads addressed to him. Commercial speech is a separate category of speech which is not accorded the same level of protection as that given to other constitutionally guaranteed forms of expression but is nonetheless entitled to protection. The State cannot rob him of this right without violating the

> constitutionally guaranteed freedom of expression. Unsolicited advertisements are legitimate forms of expression.[149]

In view of the foregoing pronouncements of the Supreme Court in *Disini*, and considering that direct marketing may fall within the definition of unsolicited commercial communications as defined in the Cybercrime Prevention Act of 2012, there is a risk that a data subject's right to object to the processing of his personal information for direct marketing may be rendered meaningless. Thus, the question now is the extent, if any, of the data subject's right to object. This is something that should be clarified not only by the NPC but also, if the opportunity presents itself, by the Supreme Court as well.

In addition, the NPC may consider establishing a system where data subjects have the option of permanently blocking commercial communications sent through their contact information. This relieves the burden on the data subjects from having to withdraw their consent from all the companies and agencies (which may be so numerous and sometimes unknown to the data subjects until they are contacted) that are able to get a hold of their data information. "Do Not Call" (DNC) registries established in other jurisdictions do this and shift the burden on the companies to first check the relevant DNC Registry prior to targeting any data subject for marketing.

B. Protected Internet Information: Content v. Non-Content Data

It goes without saying that vast amounts of information in the information society are transmitted and shared across networks through the internet.[150] In

---

149. *Id.* at 313–15.

150. Jonathan Strickland says that

> Data travels across the internet in packets. Each packet can carry a maximum of 1,500 bytes. Around these packets is a wrapper with a header and a footer. The information contained in the wrapper tells computers what kind of data is in the packet, how it fits together with other data, where the data came from[,] and the data's final destination.
>
> When you send an [email] to someone, the message breaks up into packets that travel across the network. Different packets from the same message don't have to follow the same path. That's part of what makes the [i]nternet so robust and fast. Packets will travel from one machine to another until they reach their destination. As the packets arrive, the computer receiving the data assembles the packets like a puzzle, recreating the message.

this regard, before information from point A reaches point B, it would necessarily have to pass through the networks of several entities such as Internet Service Providers, Network Service Providers, and Email Service Providers before reaching its intended recipient.[151] Thus, considering that data, when transmitted through the internet, would necessarily pass through a number of third persons before reaching its intended recipient, can an individual legitimately claim a right to informational privacy on internet data? For a better perspective, in the physical world of atoms, letters containing private correspondence may be transmitted through the postal system. Traditionally, information found outside the envelope or packet containing a letter, e.g., the names and addresses of the sender and recipient, are not considered private information.[152] Meanwhile, the contents of the letter itself may be considered private.[153] A similar distinction appears to apply to information transmitted digitally through the internet. In this regard, it is necessary to distinguish between "traffic" and "content" data.[154] According to the Supreme Court in *Disini*,

> an ordinary ICT user who courses his [or her] communication through a service provider, must of necessity disclose to the latter, a third person, the traffic data needed for connecting him [or her] to the recipient ICT user. For example, an ICT user who writes a text message intended for another ICT user must furnish his [or her] service provider with his [or her] cellphone number and the cellphone number of his [or her] recipient, accompanying the message sent. It is this information that creates the traffic data. *Transmitting communications is akin to putting a letter in an envelope properly addressed, sealing it closed, and sending it through the postal service. Those who post letters have no expectations that no one will read the information appearing outside the envelope.*
>
> Computer data [—] messages of all kinds [—] travel across the internet in packets and in a way that may be likened to parcels of letters or things that are sent through the posts. When data is sent from any one source, the

---

Jonathan Strickland, How IP Convergence Works, *available at* http://computer.howstuffworks.com/ip-convergence2.htm (last accessed Aug. 10, 2017).

151. Rus Shuler, How Does the Internet Work?, *available at* https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm (last accessed Aug. 10, 2017).

152. *Disini, Jr.*, 716 SCRA at 414-17 (citing Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1019-22 (2010)).

153. *Id.*

154. *Disini, Jr.*, 716 SCRA at 414.

> content is broken up into packets and around each of these packets is a wrapper or header. This header contains the traffic data [—] information that tells computers where the packet originated, what kind of data is in the packet (SMS, voice call, video, internet chat messages, email, online browsing data, etc.), where the packet is going, and how the packet fits together with other packets. The difference is that traffic data sent through the internet at times across the ocean do not disclose the actual names and addresses (residential or office) of the sender and the recipient, only their coded [IP] addresses. The packets travel from one computer system to another where their contents are pieced back together.
>
> ...
>
> For example, when one calls to speak to another through his [or her] cellphone, the service provider's communication's system will put his [or her] voice message into packets and send them to the other person's cellphone where they are refitted together and heard. The latter's spoken reply is sent to the caller in the same way. To be connected by the service provider, the sender reveals his [or her] cellphone number to the service provider when he puts his [or her] call through. He [or she] also reveals the cellphone number to the person he calls. The other ways of communicating electronically follow the same basic pattern.
>
> In *Smith v. Maryland*, cited by the Solicitor General, the United States Supreme Court reasoned that telephone users in the '70s must realize that they necessarily convey phone numbers to the telephone company in order to complete a call. That Court ruled that even if there is an expectation that phone numbers one dials should remain private, such expectation is not one that society is prepared to recognize as reasonable.
>
> In much the same way, *ICT users must know that they cannot communicate or exchange data with one another over cyberspace except through some service providers to whom they must submit certain traffic data that are needed for a successful cyberspace communication. The conveyance of this data takes them out of the private sphere, making the expectation to privacy in regard to them an expectation that society is not prepared to recognize as reasonable.*[155]

As explained by Chief Justice Sereno in her separate concurring and dissenting opinion in *Disini, Jr.*, the reason for the foregoing distinction between traffic and content data is to keep "the balance between protecting privacy and maintaining public order through effective law enforcement."[156] Thus, she similarly concludes that "given the very public nature of the [i]nternet and the nature of traffic data as non-content and non-identifying

155. *Id.* at 340-342 (citing Smith v. Maryland, 442 U.S. 735, 743 (1979)) (emphasis supplied).

156. *Id.* at 414 (C.J. Sereno, concurring and dissenting opinion) (emphasis omitted).

information, individuals cannot have legitimate expectations of privacy in traffic data [per se]."[157]

That being said, while there is a general recognition that content data is considered private, this is not absolute. Using the two-fold test mentioned above, it appears that there can be an objective expectation of privacy if the individual uploading information on the internet specifically limited its recipients by utilizing protective measures, tools, or devices that would have effectively limited access to such information. For instance, an email addressed specifically to only a number of individuals and with a disclaimer stating that such email "is only for the intended recipients" will likely be considered as private information. On the other hand, a photograph or image uploaded on an online social media network (OSN) that has not been specifically restricted to be viewed only by specified individuals may not be considered private information. This has been the holding of the Supreme Court in *Vivares v. St. Theresa's College*,[158] to wit —

> With the availability of numerous avenues for information gathering and data sharing nowadays, not to mention each system's inherent vulnerability to attacks and intrusions, there is more reason that every individual's right to control said flow of information should be protected and that each individual should have at least a reasonable expectation of privacy in cyberspace. ... .
>
> ...
>
> The question now though is up to what extent is the right to privacy protected in OSNs? Bear in mind that informational privacy involves personal information. At the same time, the very purpose of OSNs is socializing [—] sharing a myriad of information, some of which would have otherwise remained personal.
>
> ...
>
> Before one can have an expectation of privacy in his or her OSN activity, *it is first necessary that said user ... manifest the intention to keep certain posts private, through the employment of measures to prevent access thereto or to limit its visibility*. And this intention can materialize in cyberspace through the utilization of the OSN's privacy tools. *In other words, utilization of these privacy tools is the manifestation, in cyber world, of the user's invocation of his or her right to informational privacy.*
>
> Therefore, a Facebook user who opts to make use of a privacy tool to grant or deny access to his or her post or profile detail should not be denied the

157. *Id.* at 418.

158. Vivares v. St. Theresa's College, 737 SCRA 92 (2014).

informational privacy right which necessarily accompanies said choice. Otherwise, using these privacy tools would be a feckless exercise, such that if, for instance, a user uploads a photo or any personal information to his or her Facebook page and sets its privacy level at [']Only Me['] or a custom list so that only the user or a chosen few can view it, said photo would still be deemed public by the courts as if the user never chose to limit the photo's visibility and accessibility. Such position, if adopted, will not only strip these privacy tools of their function but it would also disregard the very intention of the user to keep said photo or information within the confines of his or her private space.

...

Considering that the default setting for Facebook posts is [']Public,['] it can be surmised that the photographs in question were viewable to everyone on Facebook, absent any proof that petitioners' children positively limited the disclosure of the photograph. If such were the case, they cannot invoke the protection attached to the right to informational privacy. The ensuing pronouncement in [*United States of America v. Gines-Perez*] is most instructive [—]

['A] person who places a photograph on the [i]nternet precisely intends to forsake and renounce all privacy rights to such imagery, particularly under circumstances such as here, where the Defendant did not employ protective measures or devices that would have controlled access to the Web page or the photograph itself.[']

Also, [*United States of America v. Maxwell*] held that [']['t]he more open the method of transmission is, the less privacy one can reasonably expect. Messages sent to the public at large in the chat room or [email] that is forwarded from correspondent to correspondent loses any semblance of privacy.[']

That the photos are viewable by [']friends only['] does not necessarily bolster the petitioners' contention. In this regard, the cyber community is agreed that the digital images under this setting still remain to be outside the confines of the zones of privacy in view of the following:

(1) Facebook [']allows the world to be more open and connected by giving its users the tools to interact and hare in any conceivable way[;']

(2) A good number of Facebook users [']befriend[']other users who are total strangers;

(3) The sheer number of [']Friends['] one user has, usually by the hundreds; and

(4) A user's Facebook friend can [']share[']the former's post, or [']tag['] others who are not Facebook friends with the former, despite its being visible only to his or her own Facebook friends.

> It is well to emphasize at this point that setting a post's or profile detail's privacy to [']Friends['] is no assurance that it can no longer be viewed by another user who is not Facebook friends with the source of the content. The user's own Facebook friend can share said content or tag his or her own Facebook friend thereto, regardless of whether the user tagged by the latter is Facebook friends or not with the former. Also, when the post is shared or when a person is tagged, the respective Facebook friends of the person who shared the post or who was tagged can view the post, the privacy setting of which was set at [']Friends.[']
>
> ...
>
> *Had it been proved that the access to the pictures posted were limited to the original uploader, through the* [']*Me Only*['] *privacy setting, or that the user's contact list has been screened to limit access to a select few, through the* [']*Custom*['] *setting, the result may have been different, for in such instances, the intention to limit access to the particular post, instead of being broadcasted to the public at large or all the user's friends en masse, becomes more manifest and palpable.*[159]

Accordingly, in view of the foregoing pronouncements of the Supreme Court, it appears that internet information shall be considered private only when the individual *subjectively* manifested his or her intention to keep the information private by reasonably using available online privacy tools, which *objectively* limited the recipients or audience of such information.

That being said, it appears that the Supreme Court failed to consider a fundamental data privacy question in *Vivares*, i.e., whether the processing of personal information (i.e., the pictures of the students) made by St. Theresa's College is consistent with the DPA and DPA IRR. In other words, does the uploading of photographs containing personal information on the internet automatically allow the processing of such photographs by a third party for whatever purpose simply because the photographs have entered the public sphere? The Author believes that this should be answered in the negative, and that the lawfulness of processing would ultimately depend on the purposes to which the individual consented to at the moment the photograph or personal information was uploaded on the internet.

Moreover, in relation to information posted on OSNs and the internet in general, it bears reiterating that the DPA and DPA IRR do not apply to an individual who collects, holds, processes, or uses personal information in connection with that individual's personal, family, or household affairs. This exemption raises issues relating to the determination of which conduct is

159. *Id.* at 111, 113, 116-17, & 119-23 (citing United States v. Gines Perez, 152 F. Supp.2d 137, 225 (D.P.R. 2001) & United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996)) (emphasis omitted and supplied).

captured by the DPA and DPA IRR and which is not.[160] In a country like the Philippines where OSNs have a high prevalence rate, thousands (if not millions) of images of friends and family members are uploaded by individuals on a daily basis. At what point would these activities enter the public sphere?[161] This is a question that the NPC would have to answer and provide guidelines for.

C. Extraterritoriality

As mentioned above, the DPA and DPA IRR apply to the processing of personal information outside the Philippines in certain circumstances. Needless to state, in view of the speed and efficiency at which information is transferred across networks and borders, the effectivity of the DPA and DPA IRR relies in large part on their interoperability and enforceability in the broader context of the Association of Southeast Asian Nations, the EU, and beyond. For this same reason, the DPA and DPA IRR should be interpreted in light of the growing international privacy framework and must not be applied or enforced extraterritorially in each and every instance where an opportunity to do so arises.

The NPC and Philippine courts must ensure that the appropriate jurisdictional nexus is present before the DPA is sought to be extraterritorially applied or enforced. Failing to do so may result in jurisdictional overreach and other enforcement problems. In this regard, the nexus should be clear and well-established so that the DPA and DPA IRR could have a reasonable degree of enforceability. This is important especially since, as the Author understands it, the DPA and DPA IRR is perceived to be broader in scope than its regional counterparts.

D. Industry Specific Guidelines

The DPA and DPA IRR enjoin personal information controllers and processors to formulate data privacy policies,[162] which may be subject to the review of the NPC.[163] The Author recognizes that mandating the formulation of these data privacy policies is a big step towards fostering a culture of privacy in the Philippines.

160. Walden, *supra* note 3.

161. *Id.*

162. Data Privacy Act of 2012, § 20 & Rules and Regulations Implementing the Data Privacy Act of 2012, § 26 (b).

163. Rules and Regulations Implementing the Data Privacy Act of 2012, § 29.

To strengthen this mandate, however, the Author believes that data protection guidelines specific to the major industries or sectors that will be affected by the operation of the DPA and DPA IRR should be established by the NPC. This is because different industries or sectors may process different categories of personal information differently and in varying degrees. Thus, security measures adopted to protect the availability, integrity, and confidentiality of personal information by controllers and processors in one industry may not necessarily be sufficient in another. In this regard, industry-specific guidelines should provide general guidance on security measures necessary to ensure that personal information controllers and processors operating in a particular sector or industry comply with the provisions of the DPA and DPA IRR. In line with this, the NPC, in coordination with the relevant sector regulator and other bodies or stakeholders, may provide data privacy guidelines for, among others, the government, healthcare, banking and finance, research, real estate, and education.

VI. CONCLUDING REMARKS: MOVING TOWARDS A "CULTURE OF PRIVACY"

Admittedly, the DPA and DPA IRR have only been recently enforced. Therefore, the implementation and enforcement of their provisions largely remain untested in courts. Indeed, there appears to be no reported case yet (although the Author understands that the NPC is currently investigating several complaints and has, in fact, released their findings on some of them). That being said, it bears stressing that one of the main goals of the NPC, which it has emphasized from the beginning, is the development of a culture of privacy in the Philippines.[164] Considering the discussions above, and the risks associated with the information society, this is vital for the protection of the privacy of individuals in an increasingly networked world.

164. Patdu & Rellosa, *supra* note 81, at 102.