Privacy and Data Protection in the Philippines

*Christopher L. Lim**

I. INTRODUCTION

Recent changes in information technology have brought down the costs of providing back-office services across countries. Companies, particularly those in Europe and the United States, have strategically opted to outsource their information technology and business process services to other countries.

---

* '82 LL.B., *with honors*, Ateneo de Manila University, School of Law. The author is teaches *Intellectual Property Law* at the Ateneo Law School, and is a Partner with the Quisumbing Torres Law Offices, where he heads the firm's Intellectual Property and Information Technology Departments. He is a founding trustee of the Intellectual Property Foundation, Director and Past President of the Council to Combat Counterfeiting and Piracy of Patents and Trademarks (COMPACT), a member of the Intellectual Property Association of the Philippines, the Asian Patents Attorney Association and the Intellectual Trademark Association, and has worked closely with the Philippine Congress in drafting the new Intellectual Property Code, Republic Act No. 8293 (1997).

The author was Article Editor of Volumes 24 and 26, and Notes Editor of Volume 25, *Ateneo Law Journal*. His previous works published by the *Journal* include: *Developments in Philippine Copyright Law*, 41 ATENEO L.J. 384 (1997); *An Insight on Copyright*, 33 ATENEO L.J. 13 (1989); *Insights on Marriage and Divorce Under the Muslim Code*, 26 ATENEO L.J. 138 (1982), *Rights and Status of Common Law Spouses under Philippine Law and Jurisprudence*, 25 ATENEO L.J. 33 (1981) and *Development of Philippine Copyright Lau*, 46 ATENEO L.J. 368 (2001).

Cite as 50 ATENEO L.J. 670 (2005).

The offshore movement continues unabated and there is no indication it will slow down in the coming years. In fact, studies indicate that spending in the United States for global sourcing of computer software and services will increase at a yearly compound rate of over 20%, growing from US$15.2 billion in 2005 to US$38.2 billion in 2010.[1]

The Philippines has created a niche in Information Technology (IT) and business process outsourcing.[2] By continually promoting the country's low labor costs and the Filipino workforce's ability to speak English, the government hopes to entice companies to choose the Philippines as its offshore IT and business partner. A.T. Kearney, a U.S.-based management-consulting firm, published a report regarding the offshore prospects of eleven countries, including the Philippines.[3] The study employed a quantitative evaluation tool that rated eleven offshore prospects according to cost, people[4] and environment.[5] The Philippines scored quite well in the cost category and averaged fairly on people and environment. Overall, it is considered a top candidate for offshore business processing due to its cultural affinities with the United States, American-style English speakers, the low employee turn-over rates, and the workforce's knowledge of U.S. standards of customer service.[6]

This rising trend on offshore IT and business processing unavoidably involves the transfer of data across countries. Recently, the United States raised concerns about the effect of offshore outsourcing on data provided by American companies. Legislators in the United States question the privacy

1. Global Insight, *Executive Summary: The Comprehensive Impact of Offshore Software and IT Services Outsourcing on the U.S. Economy and the IT Industry*, GLOBAL INSIGHT, Oct. 2005 at 1 and 4.

2. For a discussion of the features of the Philippines that make it a prime candidate for Information Technology and business processing outsourcing, *see Research Summary: Outsourcing to the Philippines: Metro Manila and Beyond*, 3 NEOIT (Oct. 2005).

3. These countries included India, Canada, Brazil, Mexico, Hungary, Ireland, Australia, Czech Republic, Russia, and China. *See* A.T. Kearney, *Selecting a Country for Offshore Business Processing*, *available at* http://www.atkearney.com/shared_res/pdf/Where_to_Locate_S.pdf (last accessed Dec. 8, 2005).

4. The following country characteristics were covered: business processing and IT process experience, size of labor market, education level of workforce, language barriers and literacy rates, and employee retention.

5. The following country characteristics were covered: economic and political risks, country infrastructure, cultural compatibility, geographic proximity and security of intellectual property.

6. A.T. KEARNEY, *supra* note 3, at 7.

protections accorded to Americans by offshore countries including the Philippines.[7] In particular, two members of the United States Congress, Representative Ed Markey and Senator Hillary Rodham Clinton, proposed the Safeguarding Americans from Exporting Identification Act[8] that, among others, tasks the Federal Trade Commission to certify that a particular country has a legal system that provides adequate privacy protection for personal data. If the country is not certified as such, American business enterprises may not transmit personal data regarding a United States citizen to any foreign affiliate or subcontractor located in that country subject to specific conditions.[9] The more developed European data protection legislation already covers the adequate level of protection threshold that must be met before personal data may be transferred to a non-European Economic Area country.[10]

---

7. Ed Markey, *Outsourcing Consumer Privacy: Do You Know Where Your Personal Data Is?*, *available at* http://www.house.gov/markey/Issues/iss_privacy_pi050914.pdf (last accessed Sept. 14, 2005).

8. An Act to Prohibit the Transfer of Personal Information to Any Person Outside the United States, Without Notice and Consent, and for other purposes [Safeguarding Americans From Exporting Identification Act], H.R. 165, 109th Cong. (2005); A Bill to Regulate the Transmission of Personally Identifiable Information to Foreign Affiliates and Subcontractors [Safeguarding Americans From Exporting Identification Act], S. 810, 109th Cong. (2005).

9. *Id*. For an assessment of the provisions of the proposed bills as introduced during the 108th Congress, *see* Eugene Oscapella, *U.S. Politicians Act on Offshore Privacy Fears*, 73 PRIVACY LAWS & BUSINESS 2-3 and 25 (May-June 2004).

10. 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, art. 25 (Oct. 24, 1995) which provides:

> 1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
>
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and

With the rising concern about the protection provided by an offshore host, a spate of issues arise regarding the current state of the Philippine legal and administrative system on privacy and data protection. Clearly, a reliable system is necessary if the Philippines wishes to maintain its positioning as a choice outsourcing venue. This note looks at the present state of Philippine laws on privacy and data protection. While privacy involves many facets, such as the right to privacy of communication[11] or of the person,[12] this note

---

> the professional rules and security measures which are complied with in that country.
>
> 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
>
> 4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
>
> 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
>
> 6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
>
> Member States shall take the measures necessary to comply with the Commission's decision.

11. There are several Philippine laws that seek to protect the privacy of communications. These laws include: An Act to Ordain and Institute the Civil Code of the Philippines [NEW CIVIL CODE] Republic Act No. 386 (1950); An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purposes [ANTI-WIRETAPPING ACT] Republic Act No. 4200 (1965).

Article 723 of the Civil Code provides for the privacy of correspondence as follows:

> [L]etters and other private communications in writing are owned by the person to whom they are addressed and delivered, but they cannot be published or disseminated without the consent of the writer or his heirs. However, the court may authorize their publication or dissemination if the public good or the interest of justice so requires.

limits its discussion of privacy to an individual's interest and capacity to control the handling of data regarding himself or herself -- that is the privacy of personal data or what is called informational privacy.[13] The state of privacy and data protection in the Philippines are discussed with specific reference to legislation and case law that relate to personal data used, collected, stored and transferred to and from the Philippines.

Under the concept of data privacy or information privacy, an individual may claim that data about himself should not be automatically available to other individuals and organizations, but when that data is made available to

---

> The Anti-Wiretapping Act is a special law that penalizes unauthorized recordings of any private communication or spoken word. It provides in §1:
>
> It shall be unlawful for any person, not being authorized by all the parties to any private communication to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or detectaphone or walkie-talkie or tape recorder, or however otherwise described... It shall also be unlawful for any person, be he a participant or not in the act or acts penalized under the Act, to knowingly possess any tape record, wire record, disc record, or any other such record, or copies thereof, of any communication or spoken word; or to replay the same for any other person or persons; or to communicate the contents thereof, either verbally or in writing, or to furnish transcriptions thereof, whether complete or partial, to any other person.

12. Under the Philippine Constitution, the clauses on due process, protection against unreasonable searches and seizures, and the right against self-incrimination seek to protect the right to privacy of an individual against the State.

13. For discussions on the concept of informational privacy, *see* Roger Clarke, *Introduction to Dataveillance and Information Privacy and Defintions of Terms*, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (last accessed Dec. 8, 2005); Susan E. Gidin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, *available at* http://www.info-law.com/lost.html (last accessed Dec. 8, 2005); Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 STANFORD LAW REVIEW 1461 (May 2000); Andrew A. Fornier, *Comprehensive Privacy Law in the Philippines and Adaptation to Combat Terrorism* (2004) (unpublished J.D. Thesis, Ateneo de Manila University School of Law) *citing* JUDITH DECREW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 75 (1997); David Banisar and Simon Davies, *Global Trend in Privacy Protection: An international Survey of Privacy, Data Protection, and Surveillance Law and Development*, 18 MARSHALL J. COMPUTER & INFO. L., 1, *cited in* ROY GIRASA, CYBERLAW: NATIONAL AND INTERNATIONAL PERSPECTIVES 272.

another party, the individual must be able to exercise a substantial degree of control over that data and its use.[14] In general, informational privacy laws are drafted based on this premise. In the Philippines, there is no particular law that deals with the protection of informational privacy. There are, however, general laws and jurisprudence that an individual can cite should the right to his personal data privacy be violated. What is certain is that personal information falls within the penumbra of the right to privacy.[15] What is lacking is a specific law establishing rules and guidelines on the collection, handling and disclosure of personal data.

II. PHILIPPINE PRIVACY LANDSCAPE

A. The Philippine Constitution

The 1987 Constitution enshrined the right of privacy of communication thus, "[t]he privacy of communications and correspondence shall be inviolable except upon lawful order of the court or when public safety or order requires otherwise as prescribed by law. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding."[16] This right to privacy guaranteed by the Constitution has been recognized since the 1935 Constitution of the Philippines. The framers of the 1935 Constitution must have found that the search and seizure clause was insufficient to protect the privacy of Filipinos, and this must have motivated them, at least in part, to insert the privacy of communication clause into the 1935 Constitution. Such clause had no counterpart in the American constitution nor in Philippine organic law prior to the 1935 Constitution.[17]

The present version of the privacy of communication clause contains the added words "as prescribed by law." Joaquin Bernas makes the following comment, thus:

> [t]he effect of this addition, made in the interest of safeguarding liberty, is not only that the discretion of the executive officer is limitable by law but also that a public officer who exercises this power must be able to point to a law under which he acts. To hold otherwise would be to opt for a

14. Roger Clarke, *Introduction to Dataveillance and Information Privacy and Definition of Terms*, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (last accessed Dec. 8, 2005).

15. Ople v. Torres, 293 SCRA 141, 162 (1998).

16. PHIL. CONST. art. III, §3 ¶1.

17. JOAQUIN G. BERNAS, THE 1987 CONSTITUTION OF THE REPUBLIC OF THE PHILIPPINES: A COMMENTARY 210 (2003 ed.).

> government of men and not of laws. Every police agent would feel authorized to snoop. Moreover, it goes without saying that "abuse of discretion amounting to lack or excess of jurisdiction" can be checked through judicial review.[18]

Much as the Constitution however protects the rights of an individual to privacy, it must be kept in mind that the Constitution, and Article III or the Bill of Rights in particular, protects a citizen from intrusion by the government itself, and not against other private individuals. As such, it can only be invoked against the State and not against private individuals or entities.[19] For instance, the Constitutional provision finds no application to a complaint by a customer against a company that collects, stores and transfers information he or she provided in case of a violation of his or her right to privacy. The Supreme Court in the case of *People v. Marti* states, thus:

> The constitutional proscription against unlawful searches and seizures therefore applies as a restraint directed only against the government and its agencies tasked with the enforcement of the law. Thus, it could only be invoked against the State to whom the restraint against arbitrary and unreasonable exercise of power is imposed.[20]

Although the Constitution provides data and information protection, it does so only as regards the State, but not as against private individuals. It safeguards informational privacy by ensuring that the government is not able to have instant access to data regarding an individual, and particularly, the transmission of this data from another country to the Philippines. Such data may only be acquired upon lawful order of the court, or when public safety or order requires, and if so, only as prescribed by law. Such protection might have been ample enough if the only privacy that is required is that against the government. Such is not the case however. As a matter of fact, informational privacy is more importantly needed as regards private individuals and organizations, particularly with regard to those who might handle or come into contact with one's personal data. It is in this area that the fundamental law of the land on its own is insufficient. Thus, resort to statutory law must be had.

B. Civil Code of the Philippines

The Civil Code protects personal privacy through Articles 26 and 32. Article 26 provides that "every person must respect the dignity, personality,

---

18. *Id.* at 213.

19 . People v. Marti, 193 SCRA 57, 60 (1991).

20. *Id.* at 67.

privacy, and peace of mind of his neighbors and other persons."[21] The same provision identifies the following acts that give a person a right to sue for damages for violation of his privacy:

1. Prying into the privacy of another's residence;
2. Meddling or disturbing the private life or family relations of another;
3. Intriguing to cause another to be alienated from his friends;
4. Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition.[22]

It must be noted that although the Civil Code enumerates the abovementioned acts as giving rise to a cause of action for damages, the above enumeration is not exclusive as the said article is broadened by the words "and similar acts."[23]

Under Article 26 of the Civil Code, the right to privacy refers to the right of an individual to be left alone, or to be free from unwarranted publicity, or to live without unwarranted interference by the public in matters in which the public is not necessarily concerned. The Civil Code Commission explained the article:

> [t]he privacy of one's home is an inviolable right. Yet, the laws in force do not squarely and effectively protect this right.
>
> The acts referred to in No. 2 are multifarious, and yet many of them are not within the purview of the laws in force.
>
> x x x
>
> …there is the meddling of so-called friends who poison the mind of one or more members of the family against the other members of the family. In this manner, many a happy family is broken up or estranged. Why should not the law try to stop this by creating a civil action for moral damages?
>
> Of the same nature is that class of acts specified in No. 3: intriguing to cause another to be alienated from his friends.
>
> Not less serious are the acts mentioned in No. 4: vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect or other personal conditions. The penal laws against defamation and unjust vexation are glaringly inadequate.
>
> x x x

---

21. NEW CIVIL CODE, art. 26 (emphasis supplied).
22. *Id.*
23. *Id.*

> The article under study denounced "similar acts" which could readily be named, for they occur with unpleasant frequency.[24]

It can thus be gleaned that article 26 of the Civil Code is more focused on residential privacy, meddling by neighbors, and vexation and defamation. It makes no reference to data privacy or informational privacy, probably because at the time of the enactment of the Civil Code, the concept of data privacy and informational privacy as known and understood today was alien. Article 26 in this regard is rather broad. It does not define informational privacy, nor does it protect the use and transfer of personal data. As such, although the said article may be generally cited, it is highly insufficient as regards its use in the field of informational privacy.

Article 32 of the Civil Code, in relation to paragraph 11 of the same article provides that "any public officer or employee, or *any private individual*, who directly or indirectly obstructs, defeats, violates or in any manner impedes or impairs any of the following rights and liberties of another person shall be liable to the latter for damages: ...[t]he privacy of communication and correspondence..."[25] This particular provision refers to the right of an individual against intrusion into his private communication and correspondence by public officers and employees and even private individuals. Article 32 is an implementation of the civil liberties guaranteed by the Constitution. It creates a separate and independent civil action for violation of civil liberties. Further, Article 32 does what the Constitutional provision on privacy does not – that is, the Civil Code provision covers an unwarranted intrusion by a *private individual* against another's right to privacy, and grants the latter a right to damages for such violation. Although this article would probably give rise to a cause of action for damages for any individual who misuses another's personal data, it is more reactive than proactive. It is insufficient, merely providing a cause of action for damages. It does not specifically provide for the handling of data as it passes on from an individual to another party, and even yet to another party. It is rather broad in the sense that it does not define personal data, nor does it provide for its protection when it is collected, stored, and transferred to and from the Philippines. Neither does the said article contain a provision on control of personal data once it is transferred to another party.

In a similar light is Article 19 of the Civil Code, which provides that: "Every person must, in the exercise of his rights and in the performance of his duties, act with justice, give everyone his due, and observe honesty and

---

24. MELENCIO S. STA. MARIA, PERSONS AND FAMILY RELATIONS LAW 44-45 (4th ed. 2004) (*citing* the Report of the Civil Code Commission 32-34 (1947)).

25. NEW CIVIL CODE, art. 32 (emphasis supplied).

good faith."[26] This is a broad and encompassing provision that deals with abuse of rights. The basic premise for Article 19 is that a person should be protected only when he acts in the legitimate exercise of his right, that is, when he acts with prudence and in good faith. There is an abuse of right when it is exercised for the sole purpose of prejudicing or injuring another. The absence of good faith is essential to abuse of right. Article 19 finds its legal sanction under Article 20 of the same Code which provides: "[e]very person who, contrary to law, willfully or negligently causes damage to another shall indemnify the latter for the same."[27]

The provisions on privacy in the Civil Code govern the involuntary collection and use of private information or intrusion into an individual's privacy only in a general manner. There are no specific provisions in the Civil Code covering personally identifiable information that are voluntarily provided by a person. Hence, it does not specifically relate to informational or data privacy. The Civil Code has no provision defining personal data. Consequently and more importantly, it has no provisions protecting the collection, transfer, and use of personal data supported by ill-motives. At best, it provides a resort to an action for damages. It does not provide preventive legislation, but rather resorts to deterrence as a defense mechanism. In this regard, the Civil Code provisions on the right to privacy are insufficient with regard to informational privacy.

The lack of specific provisions under the Constitution and the Civil Code on informational privacy, however, has not prevented the Supreme Court from using these two general laws to deal with a claimed intrusion into an individual's right to privacy in the case of *Ople v. Torres*.[28]

C. Unconstitutionality of the National Identification Reference System

In *Ople v. Torres*,[29] a 1998 Supreme Court decision, the right to privacy was weighed in relation to the proposed National Computerized Identification Reference System. The plaintiff, Senator Ople, brought suit to strike down Administrative Order No. 308 on the grounds that it was an unlawful exercise of legislative power by the executive and that it was repugnant to the constitutionally enshrined right of an individual to privacy. The administrative order proposed a computerized system to facilitate transactions with basic service and social security providers and identify persons seeking basic services on social security and to reduce fraudulent transactions. In this

26. *Id.* art. 19.

27. NEW CIVIL CODE, art. 20.

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

29. *Id.*

connection, the administrative issuance sought to introduce a Population Reference Number (PRN) to establish a linkage among concerned agencies through the use of *Biometrics Technology* (for example, finger-scanning, retinal scanning, artificial nose, thermogram) and *computer application designs.* Identification cards are then to be issued to all persons transacting with the government, the holders of which will be assigned a PRN.

The Supreme Court struck down the administrative order as violative of the right to privacy. It noted that the order failed to specify what specific biological characteristics will be used to identify people who seek its coverage. It also said that the PRN may be used for generation of other data "for development planning," thus creating avenues for potential misuse of the data to be gathered, as well as possible leakage of the information, or manipulation of data. From the decision, it can be surmised that incursions on the right to privacy must be clearly limited in terms of scope and purpose. Furthermore, adequate safeguards for data protection must be in place. The Supreme Court stated:

> …[t]he 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 compelling interest justify such intrusions. Intrusions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions… [A]ny law or order that invades individual privacy will be subjected by this Court to strict scrutiny.[30]

In the *Ople* case, the Supreme Court also applied the *reasonable expectation of privacy* test. The Supreme Court ruled that the administrative order was so far-reaching that even a minimum standard for a reasonable expectation of privacy could not be inferred from its provisions.

The Supreme Court outlined the relevant considerations in the collection and use of personal data -- the type of data collected must be definite, the purposes for the collection of the data must be specified and limited, the data provider must be advised of the type of data collected and the purpose of the collection of the data, proper safeguards must be provided to safeguard the data provider's privacy and to guarantee the data's integrity (in other words, who has control and access of the data, and under what circumstances access to the data is granted are identified), and a reasonable expectation of privacy must be accorded to the data provider.

In addition to identifying the considerations in the collection and use of data, the *Ople* case is relevant in explaining what *personal data* is and what type of data is protected. Unlike laws in other countries that specifically

30. *Id.* at 147.

define *personal information* or *personal data* covered by legislation, the Philippines does not have legislation that defines personal data. The *Ople* case, however, indicates that *protected data* includes not only an individual's full name, place of birth, date of birth, photograph, signature and thumb mark, but also information relating to loan availment, income tax returns, statement of assets and liabilities, and reimbursements for medicines and hospitalization. However, in as much as the *Ople* case defines what personal data is or can include, it goes no further than that in relation to informational privacy. Furthermore, this case deals with the relation of an individual with the State, and not with another private individual. *Ople* deals with a Constitutional issue wherein the State violated one's right to privacy. In regard to informational privacy, we are more concerned with intrusions of one's personal data by another private entity, rather than the State.

D. Electronic Commerce Act

Shortly after the ILOVEYOU virus, which was circulated around the world via e-mail, was traced to a Philippine source,[31] the Electronic Commerce Act[32] was passed into law. The law provides in its declaration of policy that "the State recognizes the vital role of information and communication technology (ICT) in nation-building"[33] and further provides that the State recognizes "the need to create an information-friendly environment which supports and ensures the availability, diversity and affordability of ICT products and services."[34] Thus, it can be gleaned that the State through its legislature has seen the need to improve the information systems of the country. The declaration of policy further recognizes the "obligation to facilitate the transfer and promotion of adaptation technology, to ensure network security, connectivity and neutrality of technology for the national benefit"[35] and further states "the need to marshal, organize and deploy national information infrastructures, comprising both telecommunications network and strategic information services, including their interconnection

31. There was no specific legislation in the Philippines directly dealing with hacking in 2000. The source of the email virus was prosecuted on the basis of Republic Act No. 8484, the Access Devices Regulation Act of 1998, a law that penalizes use of unauthorized access devices to obtain goods and services.

32. An Act Providing for the Recognition and Use of Electronic, Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for Other Purposes, Republic Act 8792 [ELECTRONIC COMMERCE ACT] (2000).

33. *Id.* §2.

34. *Id.*

35. *Id.*

to the global information networks, with the necessary and appropriate *legal*, financial, diplomatic and technical framework, systems and facilities."[36] A reading of the declaration of policy and of the law itself would show that the law generally encompasses, as it should, information technology, but hardly makes mention, if at all, of privacy, and in particular, informational privacy. The closest provisions with regard to informational privacy are Sections 24 and 32.

Section 24 provides that parties to any electronic transaction are free to determine the type and level of electronic data message or electronic document security needed, and to select and use or implement appropriate technological methods that suit their needs.[37] This section in effect merely provides that the parties involved may control the level of security they need. This may include the type and level of encryption they would like to employ when transmitting data to one another, or maybe the security software they would use to prevent data leakage as the data passes through the network. No reference is made to personal data under this section.

The Act under Section 32 provides for an obligation of confidentiality on the part of the collecting person or entity with regard to any electronic information obtained. Section 32 states:

> [e]xcept for the purposes authorized under this Act, any person who obtained access to any electronic key, electronic data message or electronic document, book, register, correspondence, information or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.[38]

The *information* referred to in this provision may include personal data and covers data about an individual's identity and even his surfing habits.[39] Read with the *Ople* conditions for the collection and use of personal data, under the Electronic Commerce Act, information may only be collected for specified uses, and may only be transferred to another with the consent of the data provider. While the Electronic Commerce Act together with the *Ople* case may provide some form of protection to personal data, such interpretation is still rather general and untested by Jurisprudence. It must be kept in mind that the *Ople* case was used in relation to an individual's relation with the State. Furthermore, while the *Ople* case may have reference to personal data, the Electronic Commerce Act relates more to electronic

---

36. *Id.* (emphasis supplied).

37. *Id.* §24.

38. *Id.* § 32.

39. VICENTE B. AMADOR, THE E-COMMERCE ACT AND OTHER LAWS @ CYBERSPACE 419 (2002) (emphasis supplied).

data message, electronic document, book, register, correspondence, and information. Book, Register, Correspondence and Information is not specifically defined by the Electronic Commerce Act nor by its implementing rules and regulations. Taken in their ordinary meanings, book, register, correspondence, and information may -- but not necessarily -- involve personal data. Electronic Data Message is defined as "information generated, sent, received or stored by electronic, optical or similar means."[40] Electronic Document is defined as "information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically."[41] While Section 32 relates to an obligation of confidentiality of data and information by one receiving the same, it makes no particular mention of personal data and the need to safeguard the privacy of this personal data as it is transmitted into the Philippines.

Neither do these two provisions specifically refer to personal data. Without jurisprudence to test these definitions as regards informational privacy, it can at most only be inferred and maybe even hoped that these definitions would cover informational privacy. Such makes the electronic commerce act insufficient.

Further, the electronic commerce act does not have any provisions for the substantial degree of control over the data and its use by the individual who made the data available to another party. As previously mentioned, one of the premises of informational privacy is that once personal data is made available to another party, the individual providing the personal data must be able to exercise a substantial degree of control over that data and its use. There is no provision in the Electronic Commerce Act, which provides such control over personal data made available to another party.

E. Restriction on Transfer of Information

The Philippines has only one law on data transfer, Presidential Decree No. 1718.[42] However, this law has no implementing rules and regulations, and the law is not strictly enforced. Under this law

40. ELECTRONIC COMMERCE ACT, § 5.

41. *Id.*

42. 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).

> [a]ny and all documents and information possessed by or in the custody of Philippine corporations, entities or individuals doing business in the pursuit of the national economic development programs of the Government and/or engaged in the development, promotion, protection and export of Philippine products to increase foreign currency are vital to the national interest and should not be utilized by any foreign person or government to the prejudice and/or detriment of said corporations, entities or individuals, including their officers and employees.[43]

An exception on the prohibition on data transfer, is provided for in Section 2 thereof:

> [a] person is prohibited to take or cause to be taken, send or cause to be sent, or remove or caused to be removed from the Philippines or to deliver to any foreign person or government or its agent or representative, any document or information relating in any manner to any business carried on in the Philippines except if the taking, sending or removal is:
>
> 1. consistent with and forms part of the regular practice of furnishing to a head office or parent company or organization outside the Philippines;
> 2. in connection with a proposed business transaction requiring the furnishing of the document or information; or
> 3. required or necessary for negotiations or conclusion of business transactions; or
> 4. in compliance with an international agreement to which the Philippines is a party; or
> 5. made pursuant to authority granted by the designated representative(s) of the President.

The law provides that authority of the designated representative(s) of the President is required for certain types of data. Unfortunately, the Office of

---

43. *Id.* § 1. *See also* § 2 which states:

> [f]or purposes of this law "document or information" includes, but is not limited to, the originals of all written, printed, typed, recorded, graphic, or photographic matter, or any type of memorial, formal or informal, located in the Philippines (including sound recordings and information stored in computers)…including, but not limited to: telexes, records, books of account, reports, minutes, memoranda, telegrams, diaries, appointment books, log books, desk calendars, notes, inter-office or intra-office communications, bulletins, charges, circulars, maps, expense accounts, working papers, surveys, bid materials, stenographer's notebooks, sales reports, price lists, and all other writings and papers similar to the foregoing, however denominated, including any record or device by means of which material is recorded or stored, and any resume, digest or extract of any such material.

the President has not issued rules and regulations implementing P.D. No. 1718 despite its promulgation more than two decades ago. The rules and regulations would have identified the representative of the President from whom authority would have to be secured to transfer certain types of data abroad.

F. Waiver of Right to Privacy

The right to privacy under the Civil Code is personal.[44] Being personal in nature, the right may be waived. A voluntary consent from the information provider for the use or transfer of data he provides, for instance, may be properly considered a waiver of his right to privacy. This waiver finds sanction under the Civil Code which allows rights to be waived provided "the waiver is not contrary to law, public order, public policy, morals, or good customs, or prejudicial to a third person with a right recognized by law."[45] There is currently no jurisprudence which holds that the waiver of the right to privacy is against law, public order, public policy, morals, or good customs, or prejudicial to a third person with a right recognized by law; and therefore any waiver of the right to privacy is valid.

Further, as the right to privacy is considered personal in nature, the Supreme Court has ruled that it cannot be invoked by a juridical entity. Thus, the Supreme Court held:

> [w]hen the information requested from the government intrudes into the privacy of a citizen, a potential conflict between the rights to information and to privacy may arise. The right to privacy belongs to the individual in his private capacity, and not to public and governmental agencies like the GSIS. A corporation has no right to privacy since the entire basis of the right to privacy is injury to the feelings and sensibilities of the party and a corporation would have no such ground for relief... The right is purely personal in nature.[46]

G. Pending Legislations on Data Protection

Realizing the importance of having a law that directly relates to data protection, Senator Mar Roxas introduced, during the 13th Congress, Senate Bill No. 2073 or the Data Protection Act of 2005. [47] The bill defines

---

44. Valmonte, et. al. v. Belmonte, 170 SCRA 256. 263 (1989).
45. NEW CIVIL CODE, art. 6.
46. *Valmonte,* at 263.
47. An Act to Establish Fair Practices in the Processing of Information Relating or Personal to Individuals, Creating for the Purpose a Personal Data Protection Commission, and for other purposes, S.B. No. 2073, 13th Cong. (2005).

Personal Data to mean information relating to an identified or identifiable data subject, which can be linked by a data controller or a third person belonging to a specific data subject.[48] The proposed bill stipulates that Personal Data must be set up only for a particular purpose relevant to the interest of the party, and must be obtained legitimately and according to the purpose for which it was collected. The party controlling the data is required to set up measures to ensure that the data processed is complete and accurate, its use compatible with the purpose of the data file, and is not disclosed to unauthorized third persons. The bill grants the data provider the right to unimpeded access to his personal records.

The bill is currently pending and being studied by the Committee on Constitutional Amendments, Revision of Codes and Laws and the Committee on Finance. There is no indication that this is priority bill or that it will pass into law any time soon.

III. THE ASIA PACIFIC ECONOMIC COOPERATION (APEC) PRIVACY FRAMEWORK

One of the pre-conditions for the development of the Information Society is for users to have confidence and trust in the reliability, security, and integrity of electronic communications systems and computerized information processing systems.[49] No individual will disclose private information if he or she lacks trust in the system. Thus, it is crucial that privacy protection be ensured both by the law and the technology being used.

Information privacy or data protection in this context is not about keeping personal information secret; it is about creating a trusted framework for collection, exchange, and use of personal data in commercial and governmental contexts. [50] In 1980, the Organization for Economic Cooperation and Development (OECD) developed guidelines based on the principle that privacy protection is an important human right. The free flow of trans-border data is a prerequisite for a free economy,[51] but such free flow of information is affected by privacy protection.

---

48. *Id.* § 3.2. The bill was introduced on Aug. 2, 2005.

49. The International Legal Framework for Data Protection and its Transposition to Developing and Transitional Countries, *available at* http://www.apec.org (last accessed Dec. 8, 2005).

50. *Id.*

51. Tony Lam, *An Overview of the Principles Established by the APEC Privacy Framework*, *available at* http://www.apec.org (last accessed Dec. 8, 2005).

The OECD Privacy Guidelines broadly influenced policy-making by introducing broad principles that can harmonize privacy protection in different states. It set out the following eight basic privacy principles:

1. Collection Limitation. This requires that the collection of data be limited to what is relevant and necessary for the purposes for which they are collected and that it will be obtained by lawful and fair means with the knowledge of the data subject.

2. Data Quality. Personal data collected should be relevant to the purpose for which it is to be used, to the extent necessary for these purposes, and should be accurate and up to date.

3. Purpose Specification and Notice. The purpose for which personal data are collected should be specified not later than the time of data collection. The subsequent use of data is limited to such purposes and to other purposes not incompatible with such.

4. Use Limitation. As a general rule, data should not be disclosed, made available or used for purposes other than those specified for its collection. The exceptions are when the individual consents or when the law so requires its disclosure.

5. Security Safeguard. This requires that personal data be protected by reasonable security safeguards against risks like loss, unauthorized access, destruction, use, modification or disclosure of data.

6. Openness. This refers to practices and policies regarding personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as identity and usual residence of the data possessor or collector.

7. Individual Participation. The individual should have the right to have reasonable access to data collected, the right to challenge data relating to him or her and, if the challenge is unsuccessful, to have the data erased, rectified, completed or amended.

8. Accountability. The data controller is made accountable for giving effect to these principles by complying with the protection accorded the individual.

These eight principles were adopted in the 1995 European Union (EU) Data Protection Directive (95/46/EC), which directed EU member states to enact laws on privacy and data protection, subject to contextualized changes and additions.

Even before U.S. legislators questioned the ability of offshore hosts to protect data collected from American citizens, twenty-one APEC nations including the Philippines began consultations in 2003 to develop a standard for privacy within the region. Dubbed the APEC Nine Privacy Principles, the privacy framework developed by the Asia-Pacific Privacy Charter Initiative in consultation with the APEC countries included protocols relating to the transfer of data. In November 2004, the APEC nations

endorsed its Privacy Framework.[52] The framework, which consists of nine principles, aims to balance privacy rights and the public interest in e-commerce. The principles are as follows:

1. Preventing Harm. The aim of privacy protection is to prevent harm to individuals resulting from wrongful collection or misuse of their personal information. This principle endorses *proportionality,* for example, remedies should be proportional to the likelihood and severity of the risk of harm.

2. Notice. A data controller must inform the individual the purpose for which personal information is being collected. This principle also requires that all reasonably practical steps, including the use of web sites, be taken to provide the notice before or at the time of data collection.

3. Collection Limitation. This is similar to the OECD principle.

4. Use of Personal Information. Use of personal information should be limited to fulfilling the purposes of collection and other compatible or related purposes.

5. Choice. This provides individuals with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.

6. Integrity of Personal Information. Personal information should be accurate, complete, and kept up-to-date to the extent necessary for the purpose of use.

7. Security Safeguards. Appropriate security safeguards are required to be applied to personal information provided these safeguards are proportional to the likelihood and severity of the information and the context in which it is held.

8. Access and Correction. Individuals are given the right to access their personal information, challenge its accuracy, and request correction when appropriate. However, access need not be provided if the burden or expense of doing so would be unreasonable or disproportionate to the risks or disclosure to the individual would compromise security or the confidentiality of commercial information.

9. Accountability. The data controller is accountable for complying with measures that give effect to the said principles.

Despite objections from some quarters that the development of a framework will weaken already existing privacy regimes within the region,[53]

52. *APEC Privacy Framework, available at* http://www.apecsec.org.sg (last accessed Dec. 8, 2005).

53. *See* Graham Greenleaf, *The APEC Privacy Initiative: 'OECD Lite' for the Asia-Pacific?*, *available at*

APEC's privacy standards began implementation in June 2005 in a regional meeting in Hong Kong with the end view of creating a regional system for information and data privacy protection that balances privacy protection, on one hand, and access to information, on the other. This is to be achieved by removing unnecessary barriers to information flows and yet ensure that the privacy of personal information is respected.

Since the 1980 Organization for Economic Cooperation and Development (OECD) Privacy Guidelines, it was only when APEC endorsed the nine privacy principles (for example, preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability) during the 17th Annual APEC Ministerial Meeting on 16 November 2005[54] that another initiative harmonizing the protection of privacy rights within a region was implemented.[55] There are very high hopes that the privacy framework will facilitate the flow of information within the region while ensuring the protection of that data although the crucial element missing from APEC's framework concerns data exports and international cooperation in enforcement.

IV. CONCLUSION

If the Philippines is intent on retaining its slot as a prime candidate for outsourcing, it is important that a privacy legislation dealing with data protection be passed and effectively implemented. Having an information system that ensures reliability, security and integrity of electronic communications and computerized information processing systems is crucial for the development of the Philippine business outsourcing industry. The Global Internet Policy Initiative provides that data protection laws should permit, and even facilitate, the commercial and governmental use of personal data while providing to individuals (1) control over what to disclose; (2) awareness of how their personal date will be used; (3) rights to insist that data

---

http://www2.austlii.edu.au/~graham/publications/2004/APEC_V8article.html (last accessed Dec. 8, 2005). *See also Global Internet Policy Initiative, The International Legal Framework for Data Protection and its Transposition to Developing and Transitional Countries, 2004, available at* http://www.internetpolicy.net/privacy/20041228privacy.pdf (last accessed Dec. 8, 2005).

54. APEC Secretariat, APEC Privacy Framework, 2005.

55. For a discussion of the nine principles, *see* Peter Ford, *APEC Privacy Framework: Domestic Implementation, available at* http://www.pco.org.hk/english/files/infocentre/1peterford1.pdf (last accessed Dec. 8, 2005).

are accurate and up-to-date; and (4) protection when personal information is used to make decisions about a person.[56]

A legal regime for the protection of privacy rights will not only assuage fears of other countries, like the U.S., regarding the integrity of data transferred to the Philippines, but will also give confidence to business owners about the protection of relevant information transmitted to the Philippines. A law that complies with APEC's Privacy Framework will clearly pave the way to providing teeth to the general expositions about the right to privacy under the Constitution and the Civil Code.

The current laws and jurisprudence that tangentially deal with data protection do not adequately address the right to informational privacy. In this age of rapidly evolving technology and the broad and non-territorial scope of commercial dealings, reliance on contractual measures to protect information is simply not a viable alternative to an established privacy legislation. Hence, it is important that a well-drafted privacy law be passed and implemented in the Philippines.

56. *The International Legal Framework for Data Protection and Its Transposition to Developing and Transitional Countries*, Dec. 28, 2004.