Zones of Privacy: How Private?

By: Llewellyn L. Llanillo and Khersien Y. Baustista

Llewellyn L. Llanillo is a Senior Partner at the Philippine law firm of Salvador Llanillo Bernardo Attorneys-at-Law in Metro Manila, and is a member of the Philippine bar and the New York Bar. He has been in law practice for more than 40 years, advising on corporate and commercial law, intellectual property law, advertising, media and entertainment, e-commerce and technology, personal data protection, franchising and distribution, and investments, mergers and acquisitions. In 2010 he was appointed as a Bar Examiner in Commercial Law. He has a BA in Social Sciences (Ateneo de Davao University), LLB (University of the Philippines), LLM in U.S. and Global Business Law (Suffolk University Law School), and LLM in Transnational Commercial Practice (Lazarski University).

Khersien Y. Bautista is an associate of Salvador Llanillo Bernardo Attorneys-at-Law, and assists in tax advisory and litigation, corporate services, and special projects. She earned her J.D. from the University of the Philippines (UP) in 2015 and was admitted to the Philippine Bar in 2016. Prior to joining SLB, she was a research assistant with the UP Law Center and an editorial assistant with the UP Third World Studies Center.

> *"All the forces of a technological age…operate to narrow the area of privacy and facilitate intrusions 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."*[1]

[1] Disini v. Secretary of Justice, G.R. No. 203335, February 11, 2014, *citing* Morfe v. Mutuc, G.R. No. L-20387, January 31, 1968, citing Thomas I. Emerson, *Nine Justices in Search of a Doctrine*, 64 MICH. LAW REV. 219, 229 (1965).

LAW as a normative tool was invented to maintain order in society; laws, however, continually evolve to accommodate changing times and respond to society's needs. In the information age, ideas and news become accessible in an instant.[2] Along with the ease of the flow of information, the system of connections and the collection of data have greatly improved, benefiting not only human relations, but the development of the economy as well.

Along with the upside, however, is the downside of these new technological advances – from the inconvenience caused by prank calls, to the more serious problems of harassment, scams, and acts of terror. Society must respond with measures deemed appropriate, reasonable, and efficacious, to keep abreast of technological progress.

This article discusses the constitutional and legal implications engendered by the collision between the right to individual privacy and the exercise of the state's police power pursuant to the demands of public interest and state security under Philippine law. We touch on the tension between privacy rights and public interest embedded in the various laws enacted to meet new threats, and elaborates on this tension as the courts balance competing interests in the following legislation: (a) Human Security Act of 2007,[3] (b) Anti-Money Laundering Act of 2001,[4] (c) Terrorism Financing Prevention and Suppression Act of 2012,[5] (d) Cybercrime Prevention Act of 2012,[6] (e) Data Privacy Act of 2012,[7] (f) the proposed national centralized identification system, and (g) the proposed registration of prepaid mobile phones.

I. Right to Privacy Under Philippine Law: A Survey of Jurisprudence

The right to privacy means the "right to be let alone"[8] and is the

[2] History World, *History of Communication.* [online] available at: http://www.historyworld.net/wrldhis/PlainTextHistories.asp?historyid=aa93 [last accessed June 1, 2017]. Long ago, Native Americans used smoke signals for long distance communication to convey a limited number of messages such as "danger" or "victory." By the 11th century, the "pigeon post" was developed in ancient Egypt.

For this generation, one would most likely use e-mail or a mobile device for long distance communication, and additionally, post or share events on an almost daily basis, on social media pages.

[3] Rep. Act No. 9372 (2007).

[4] Rep. Act No. 9160 (2001), as amended by Rep. Act No. 9194 (2003); Rep. Act No. 10167 (2012); and Rep. Act No. 10365 (2013).

[5] Rep. Act No. 10168 (2012).

[6] Rep. Act No. 10175 (2012).

[7] Rep. Act No. 10173 (2012).

[8] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. (1890). available at: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. (last accessed June 6 2017).

"beginning of all freedoms."[9] Discussing the origin of the right to privacy, *Pavesich v. New England Life Insurance Co.* held that the right to privacy has its foundation in natural law and the instinct of nature.[10] In Philippine law, the concept of privacy is enshrined in the Constitution and is regarded as the right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to a person's ordinary sensibilities.[11] It has been described as the most comprehensive of rights and the right most valued by civilized men.[12]

A. Privacy – an Independent Right

In *Morfe v. Mutuc*, the Philippine Supreme Court affirmed that the right to privacy exists independently of its identification with liberty, and in itself fully deserving of constitutional protection.[13] *Disini v. Secretary of Justice,*[14] citing *Sabio v. Gordon,*[15] also recognized the importance of the different zones of privacy protected under Philippine law. This right could also be derived from the Universal Declaration of Human Rights, which mandates that "no one shall be subjected to arbitrary interference with his privacy" and "everyone has the right to the protection of the law against such interference or attacks."[16]

The Philippine Constitution guarantees the right against unreasonable searches and seizure, as well as the right to privacy of communication and correspondence.[17] It expressly guarantees the right against self-incrimination,[18] liberty of abode,[19] right to due process,[20] and the right to and freedom of association.[21]

1. Situational, Informational, and Decisional Privacy

The concept of privacy has, through time, greatly evolved, with technological advancements playing an influential role. This evolution was briefly recounted in former Chief Justice Reynato S. Puno's speech, *The Common Right to*

---

[9] Morfe v. Mutuc, G.R. No. L-20387, January 31, 1968.
[10] Pavesich v. New England Life Ins. Co., 122 Ga. 190 (Ga. 1905).
[11] Hing v. Choachuy, Sr., G.R. No. 179736, June 26, 2013.
[12] Morfe v. Mutuc, G.R. No. L-20387, *supra* note 1.
[13] *Id.*
[14] Disini v. Secretary of Justice, G.R. No. 203335, February 11, 2014.
[15] In the Matter of the Petition for Issuance of Writ of Habeas Corpus of Sabio v. Sen. Gordon, G.R. No. 174340, October 17, 2006.
[16] *Id.*
[17] CONST. art. III, §§ 2-3.
[18] CONST. art. III.
[19] *Id*.
[20] *Id.* at § 1.
[21] *Id.* at § 6.

Privacy, where he explained the three strands of the right to privacy: (1) locational or situational privacy; (2) informational privacy; and (3) decisional privacy.[22]

Applying the United States case of *Whalen v. Roe*,[23] the Philippine Supreme Court explained "decisional privacy" and "informational privacy."[24] "Decisional privacy" involves the right to independence in making important decisions, while "informational privacy" refers to the interest in avoiding disclosure of personal matters. "Informational privacy" has two aspects: the right not to have private information disclosed, and the right to live freely without surveillance and intrusion.[25] This is the right of an individual to control information about oneself,[26] and those who oppose government collection or recording of traffic data in real time seek to protect this aspect of the right to privacy.[27]

On September 12, 2012, Republic Act (RA) No. 10175, otherwise known as the Cybercrime Prevention Act of 2012, was signed into law. A contentious provision was Section 12, on real-time collection of traffic data associated with specified communications transmitted by means of a computer system. Critics questioned whether this provision has a proper governmental purpose, since a law may require the disclosure of matters normally considered private only upon showing that such requirement has a rational relation to the purpose of the law, that there is a compelling State interest, and that the provision itself is narrowly drawn.[28]

In discussing the collection of traffic data, the Philippine Supreme Court held that "when seemingly random bits of traffic data are gathered in bulk, pooled together, and analyzed," these would lead to the creation of "profiles of the persons under surveillance. With enough traffic data, analysts may be able to determine a person's close associations, religious views, political affiliations, even sexual preferences."[29] These clearly fall within matters protected by the right to privacy.[30] Because of a failure to provide safeguards sufficient to protect constitutional guarantees and the vague purpose offered in the provision for collection, the provision was declared unconstitutional. Chief Justice Ma. Lourdes Sereno in a separate opinion[31] clarified that real-time collection of traffic data is

[22] Vivares v. St. Theresa's College, G.R. No. 202666, September 29, 2014.
[23] 429 U.S. 589 (1977).
[24] *Disini*, G.R. No. 203335, *supra* note 1.
[25] *Id*.
[26] Vivares v. St. Theresa's College, G.R. No. 202666, *supra* note 22.
[27] *Disini*, G.R. No. 203335, *supra* note 1.
[28] *Disini*, G.R. No. 203335, *supra* note 1.
[29] *Id*.
[30] *Id*.
[31] Separate Opinion in *Disini*, G.R. No. 203335, *supra* note 1.

not invalid per se. However, there must be "robust safeguards" and an explanation for the need and nature of the traffic data for warrantless real-time collection.

2. Privacy in the Workplace

Two significant cases in Philippine jurisprudence on privacy in the workplace are the cases of *Pollo v. Constantino-David,* [32] involving the search of a government employee's computer data files, and *Social Justice Security (SJS) v. Dangerous Drugs Board,* [33] dealing with the mandatory drug testing of, among others, officers and employees of public and private offices. [34] In *Pollo,* the Philippine Supreme Court held that a search by a government employer of an employee's office is justified when there are reasonable grounds for suspecting that it will turn up evidence that the employee is guilty of work-related misconduct. [35] The concept of "workplace privacy policy," as discussed in the United States case of *O'Connor v. Ortega* [36] played a central role in the decision. In determining whether privacy rights would be violated, searches must pass the test of "reasonableness for warrantless searches in the workplace." [37] "Reasonableness" is the touchstone of the validity of a government search or intrusion.[38]

Pollo stressed the relevance of the surrounding circumstances: whether a particular act of the employer impinges on an employee's right to privacy; the employee's relationship to the item seized; whether the item was in the immediate control of the employee when it was seized; and whether the employee took actions to maintain his privacy in the item. [39] It is important to note that the Supreme Court added that reasonable expectation of privacy is negated by the presence of a policy that puts its employees on notice that they have no expectation of privacy in anything they create, store, send, or receive on office computers. [40] Based on the foregoing, privacy in an office is circumscribed by the company's work policies, the collective bargaining agreement, if any, and the inherent right of the employer to maintain discipline and efficiency in the workplace. Their expectation of privacy in a regulated office environment is reduced, and a degree of impingement upon such privacy has been upheld.[41]

---

[32] G.R. No. 181881, October 18, 2011.
[33] G.R. No. 157870, November 3, 2008.
[34] Rep. Act No. 9165 (2002), § 36 (d). Comprehensive Dangerous Drugs Act of 2002.
[35] *Pollo*, G.R. No. 181881, *supra* note 32.
[36] 480 U.S. 709, 715-716 (1987).
[37] *Pollo*, G.R. No. 181881, *supra* note 32.
[38] *SJS*, G.R. No. 157870, *supra* note 33.
[39] *Pollo*, G.R. No. 181881, *supra* note 32.
[40] *Id*.
[41] *SJS*, G.R. No. 157870, *supra* note 33.

In *SJS*, the Philippine Supreme Court found the mandatory testing requirement for officers and employees of public and private offices [42] reasonable and valid. Reasonableness is the touchstone of the validity of a government search or intrusion. Whether a search at issue complies with the reasonableness standard is judged by the balancing of the government-mandated intrusion on the individual's privacy interest against the promotion of some compelling state interest. [43] Authorities have agreed that the right to privacy yields to certain rights of the public and defers to police power. [44] Also, for a law touching on the privacy rights of employees to be valid, there must be well-defined limits to properly guide authorities.[45]

B. The State's Police Power and Its Limits

A counterweight to protected privacy is the state's police power: the power to restrain and regulate the use of liberty and property to promote the public welfare. This power outpaces easily the other two inherent powers of government, eminent domain and taxation, with respect to interfering with private rights. Police power regulates not only property but, more importantly, the liberty of virtually all individuals. In this sense, it is infinitely more important than eminent domain and taxation.[46]

Because of its function, police power is described as the most pervasive, the least limitable, and the most demanding of the three inherent powers of the state.[47] Here, the individual is compelled to surrender to society rights and privileges which he would otherwise be free to exercise in a state of nature, in exchange for the benefits which he receives as a member of society.[48] The individual, as a member of society, is restrained by police power, which affects him even before he is born and follows him after he is dead. It is a ubiquitous and often unwelcome intrusion. Still, as long as the activity or the property has some relevance to the public welfare, its regulation under police power is not only proper but necessary. [49]

Police power is lodged primarily in the national legislature, and its exercise lies primarily in the

---

[42] Rep. Act No. 9165 (2002), § 36 (d). Comprehensive Dangerous Drugs Act of 2002.
[43] *SJS*, G.R. No. 157870, *supra* note 33.
[44] *Id*.
[45] *Id*.
[46] ISAGANI A. CRUZ, CONSTITUTIONAL LAW (2007 ed).
[47] *Id*.
[48] *Pavesich*, 122 Ga. 190, *supra* note 10.
[49] CRUZ, *supra* note 46, citing Ynot v. IAC, G.R. No. 74457, March 20, 1987. As the Latin maxims go, *salus populi est suprema lex* and *sic utere tuo ut alienum non laedas*, which call for the subordination of individual interests to the benefit of the greater number.

discretion of the legislative department. If the legislature does decide to act, the choice of measures or remedies, provided only that these conform to the requisites, lies also within its exclusive jurisdiction. Once determined, the remedy chosen cannot be attacked on the ground that it is not the best of the suggested solutions, or that it is unwise, or impractical or inefficacious, or even immoral.[50]

The tests to determine the validity of a police measure are: first, it must appear that the interests of the public generally, as distinguished from those of a particular class, require such interference; and second, the means are reasonably necessary for the accomplishment of the purpose, and not unduly oppressive upon individuals. [51] As ubiquitous as police power may be, it is fortunate for individual liberty that there are still some areas of human activity that are not within its reach. This will be so where the subject sought to be regulated has no bearing whatever upon the public welfare.[52]

The means employed for the accomplishment of the police objective must also be reasonable. Failing this, the law will be annulled for violation of the second requirement.[53]

The lawful exercise of police power in constitutionally protected zones of privacy is illustrated by the enactment of the Human Security Act of 2007, Anti-Money Laundering Act of 2001, and the Terrorism Financing Prevention and Suppression Act of 2012.

C. Human Security Act of 2007

Under the Human Security Act of 2007 (otherwise known as Anti-Terrorism Law or "HSA"), any person who commits an act of terrorism as defined under the Act,[54] "thereby sowing and creating a condition of widespread and extraordinary fear and panic among the populace, in order to coerce the

---

[50] CRUZ, *supra* note 46.

[51] Ynot v. IAC, G.R. No. 74457, March 20, 1987 citing U.S. v. Toribio, G.R. No. L-5060, January 26, 1910.

[52] CRUZ, *supra* note 46.

[53] *Id*.

[54] The following are the predicate criminal acts: REV. PEN. CODE art. 122 (*Piracy in General and Mutiny in the High Seas or in Philippine Waters*); art. 134 (*Rebellion or Insurrection*); art. 134a (*Coup d'Etat*), including acts committed by private persons; art. 248 (*Murder*); art. 267 (*Kidnapping and Serious Illegal Detention*); art. 324 (*Crimes Involving Destruction*); or under Pres. Dec. No. 1613 (*The Law on Arson*); Rep. Act No. 6969 (*Toxic Substances and Hazardous and Nuclear Waste Control Act of 1990*); Rep. Act No. 5207 (*Atomic Energy Regulatory and Liability Act of 1968*); RA No. 6235 (*Anti-Hijacking Law*); Pres. Dec. No. 532 (*Anti-Piracy and Anti-Highway Robbery Law of 1974;)* and Pres. Dec. No. 1866, as amended (*Decree codifying the Laws on Illegal and Unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunitions or Explosives).*

government to give in to an unlawful demand, shall be guilty of the crime of terrorism and shall suffer the penalty of forty (40) years of imprisonment, without the benefit of parole as provided for under Act. 4103, otherwise known as the Indeterminate Sentence Law as amended."

The HSA intrudes into privacy by permitting surveillance of suspects and interception and recording of communications. Notwithstanding the injunction under the Anti-Wire Tapping Law[55] against surveillance, a police or law enforcement official and the members of his team may, upon a written order of the Court of Appeals, listen to, intercept, and record, with the use of any mode, form, kind or type of electronic or other surveillance equipment or intercepting and tracking devices, or with the use of any other suitable ways and means for that purpose, any communication, message, conversation, discussion, or spoken or written words between members of a judicially declared and outlawed terrorist organization, association, or group of persons or of any person charged with or suspected of the crime of terrorism of conspiracy to commit terrorism.[56]

Privacy is still paramount, despite this broad grant of police power. The law requires an order from the Court of Appeals, and prohibits the surveillance, interception, and recording of communications between lawyers and clients, doctors and patients, journalists and their sources and of confidential business correspondence.[57]

D. Anti-Money Laundering Act of 2001 and Terrorism Financing Prevention and Suppression Act of 2012

The Anti-Money Laundering Act of 2001, as amended ("AMLA"), enacted to penalize money laundering also has safeguards to protect privacy. The AMLA created the Anti-Money Laundering Council ("AMLC"), which is mandated along with other concerned agencies, to implement its provision.[58]

---

[55] Rep. Act No. 4200 (1965).

[56] Rep. Act No. 9372 (2007), § 7. Human Security Act of 2007.

[57] *Id*.

[58] The Bangko Sentral ng Pilipinas (BSP), the Insurance Commission (IC) and the Securities and Exchange Commission (SEC) promulgated the Revised Implementing Rules and Regulations (RIRR) of Rep. Act No. 9160. The BSP also issued Circular No. 706, series of 2011, the Updated Anti-Money Laundering Rules and Regulations for banks, trust entities, and other institutions under its supervisory authority. The Supreme Court also promulgated Administrative Matter (AM) No. 05-11-04, or the Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, and Freezing of Monetary Instrument, Property or Proceeds Representing, Involving, or Relating to an

The AMLA provides the different court remedies available to the AMLC, like freeze orders, authorization to inquire into bank deposits and forfeiture; [59] and further prescribes preventive measures, including customer identification, record keeping, and reporting of covered and suspicious transactions by covered persons.[60]

Covered persons are required to maintain and safely store records of all transactions for five years from the dates of transactions. These records must contain the full and true identity of the owners or holders of the accounts and all other customer identification documents. To ensure privacy, all records must be kept confidential.[61]

Pursuant to bank secrecy laws,[62] all deposits in Philippine or foreign currency of whatever nature are confidential. Banks are prohibited from disclosing any information related to these deposits. Pursuant to the AMLA, however, the reporting of covered and suspicious transactions to the AMLC is an exception to bank secrecy laws, and such transactions must be reported to the AMLC.[63]

The rules applicable to bank inquiries are as follows:[64]

a. Bank Inquiry with Court Order. [65] – The AMLC may inquire into or examine any particular deposit or investment account, including related accounts, with any banking institution or non-bank financial institution, upon order by the Court of Appeals based on an *ex parte* application in cases of violation of the AMLA when it has been established that probable cause exists that the deposits or investments involved, including related accounts, are in any way related to an unlawful activity or a money laundering offense.

1. Inquiry Into or Examination of Related Accounts. [66] A court order *ex parte* must be obtained before the AMLC can

Unlawful Activity or Money Laundering Offence under Rep. Act No. 9160, as amended.

[59] Rep. Act No. 9160 (2001), §§ 10-12. Anti-Money Laundering Act of 2001.

[60] § 9.

[61] § 9(b); RIRR, Rule 9.2.

[62] Rep. Act No. 1405 (1955) Law on Secrecy of Bank Deposits, as *amended*; and Rep. Act No. 6426 (1974), Foreign Currency Deposit Act of the Philippines, as *amended*.

[63] Rep. Act No. 9160 (2001), § 9.

[64] RIRR, Rule XI.

[65] RIRR, Rule 11.1.

[66] Rep. Act No. 9160 (2001), § 11.

inquire into related accounts. The procedure for the *ex parte* application for an order of inquiry into the principal account shall be the same for that of the related accounts.

2. Compliance with Article III, Section 2 and 3 of the Constitution. [67] The authority to inquire into or examine the main account and the related accounts shall comply with the requirements of Article III, Sections 2 and 3 of the 1987 Constitution.[68]

b. Bank Inquiry without Court Order. [69] The AMLC shall issue a resolution authorizing the AMLC Secretariat to inquire into or examine any particular deposit or investment account, including related accounts, with any banking institution or non-bank financial institution and their subsidiaries and affiliates when probable cause exists that the deposits or investments involved, including related accounts, are in any way related to any of the following unlawful activities:

1. Kidnapping for ransom;[70]
2. Drug-related offenses;[71]
3. Hijacking and other violations and destructive arson and murder;[72]
4. Felonies or offenses of a nature similar to the

[67] *Id.*

[68] CONST. art. III, § 2. The right of the people to be secure in their persons, houses, papers, and effect 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 may produce, and particularly describing the place to be searched and the persons or things to be seized.

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. (2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceedings.

[69] RIRR, Rule 11.2.

[70] REV. PEN. CODE, art. 267.

[71] Rep. Act No. 9165 (2002), §§ 4-6, 8-16.

[72] Rep. Act No. 6235 (1971) An Act Prohibiting Certain Acts Inimical to Civil Aviation, and for Other Purposes; and REV. PEN. CODE.

above which are punishable under the penal laws of other countries;
5. Terrorism and conspiracy to commit terrorism;[73] and
6. Financing of terrorism and related offenses.[74]

To ensure confidentiality, covered persons, their officers and employees, are prohibited from communicating, directly or indirectly, in any manner to any person or entity, including the media, that a report on covered and suspicious transactions was made, the contents of such transactions or other related information. These reports may not be published or aired in any manner, including by mass media, in electronic mail or similar devices.[75] The members of the AMLC, the executive director, and all members of the secretariat, whether permanent, on detail or on secondment, are also prohibited from disclosing any information known to them by reason of their office.

E. Cybercrime Prevention Act of 2012

Advances in tele-communications technology today have resulted in the pervasive and easy collection and transmission of information through cyberspace. Mobile and wireless broadband have propelled widespread use of a variety of information technology devices such that individuals are not limited to for example just a desktop but to a combination of desktop, a mobile laptop, a tablet, several smart mobile phones, a smart television, etc. It is common to find homes with Wi-Fi routers and broadband connection to the internet.[76]

The pervasive use of the internet has produced heightened dangers to data privacy. Two pieces of legislation were enacted in 2012

[73] As defined and penalized under Rep. Act No. 9372 (2007).

[74] Punishable under Rep. Act No. 10168 (2012) §§ 5-8. The Terrorism Financing Prevention and Suppression Act of 2012.

[75] Rep. Act No. 9160 (2001), § 9; RIRR, Rule XIV (E).

[76] In a recent decision (*Disini*, *supra* note 1), the Philippine Supreme Court provided a succinct sketch of internet and cyberspace to clarify legal questions raised concerning the constitutionality of the Cybercrime Prevention Act of 2012. One might imagine cyberspace as a system that accommodates billions of simultaneous accesses and uses of the internet ("inter-networking" – combination of networks that communicate between themselves via an agreed protocol (TCP/IP).) In 1962, the pioneering head of the Advance Research Projects Agency (ARPA) of the US Department of Defense, JCR Licklider discussed his concept of "Galactic Network." In 1989, Tim Berners-Lee of the European Organization for Nuclear Research (CERN) developed the World Wide Web (www), which allowed documents, images and videos to be linked and stored through browsers. The driving force of the internet is email and the World Wide Web.

to respond to the emerging threats: The Cybercrime Prevention Act of 2012 and the Data Privacy Act of 2012.

The Cybercrime Prevention Act does not define the term "cybercrime," but simply lists the acts penalized under the law as falling under the broad umbrella of "cybercrime." The Comprehensive Study on Cybercrime prepared by the United Nations Office of Drugs and Crime for the Inter-Governmental Expert Group on Cybercrime [77] suggests that cybercrime is best considered as a collection of acts or conduct. In the Philippines, the Cybercrime Prevention Act adopts this approach. The acts that constitute the offense of cybercrime are grouped into[78] – (a) offenses against confidentiality, integrity and availability of computer data and systems, [79] (b) computer-related offenses,[80] and (c) content-related offenses.[81]

Under (a) are: illegal access; [82] illegal interception; [83] data interference; [84] system interference; [85] misuse of devices; [86] and cyber-squatting. [87] Under (b) are: computer-related forgery; [88] computer-related fraud; [89] and computer-related identity theft. [90] Under (c) are: cybersex; [91] child pornography; [92] unsolicited commercial communications;[93] and libel.[94] Interestingly, the provision penalizing unsolicited commercial communications was declared unconstitutional in *Disini v. Secretary of Justice* for violating the constitutionally guaranteed right of freedom of expression. A divided court held that unsolicited advertisements are "legitimate forms of expression." The provision in question reads:

> (3) Unsolicited Commercial Communications. – The transmission of commercial electronic communication with the use of computer systems which seek to advertise, sell, or offer for sale products and services are prohibited unless:

[77] Dated February 20, 2013.
[78] Rep. Act No. 10175 (2012), § 4. Cybercrime Prevention Act of 2012.
[79] § 4(a).
[80] § 4(b).
[81] § 4(c).
[82] § 4(a)(1).
[83] § 4(a)(2).
[84] § 4(a)(3).
[85] § 4(a)(4).
[86] § 4(a)(5).
[87] § 4(a)(6). Cyber-squatting. The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same.
[88] § 4(b)(1).
[89] § 4(b)(2).
[90] § 4(b)(3).
[91] § 4(c)(1).
[92] § 4(c)(2).
[93] § 4(c)(3).
[94] § 4(c)(4).

(i) there is prior affirmative consent from the recipient; or

(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

(ii) 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 messages; 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 penalty for these offenses may be a fine ranging from P200,000 to P5M or imprisonment of up to 12 years or more, or both.

The Philippine Supreme Court also held the following provision unconstitutional:

> Sec. 12. Real-Time Collection of Traffic Data – Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with the specified communications transmitted by means of a computer system.
>
> Traffic data refer only to the communication's origin, destination, route, time, date, size, duration,

or type of underlying service, but not content, nor identities….

The above-quoted portion of Section 12 was deemed overly broad and lacking in safeguards if exercised by law enforcement authorities without court intervention. The rest of Section 12 which covers content and identities, quoted below, requires a court order and remains valid:

Section 12. … All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed: (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

F. Data Privacy Act of 2012 and its Implementing Rules and Regulations (IRR)

In the private zone of personal information, the legislature has ensured that personal data privacy trumps police power by providing all the measures and safeguards it deemed reasonable.

1. Coverage

The Data Privacy Act of 2012 applies to "the processing of all types of personal information and to any natural or juridical person involved in personal information

processing" [95] except for specified instances such as information about an individual who is or was an officer or employee of a government institution that relates to the position or functions, [96] information processed for journalistic, artistic, literary or research purposes, [97] information necessary for banks and financial institutions, [98] and personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions.[99]

For purposes of this law, "personal information" means "any information whether recorded in 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."[100] Personal information can be processed by either a personal information controller [101] or a personal information processor.[102]

2. Data Privacy Principles

The processing of personal data must comply with the requirements of the Data Privacy Act of 2012 and other laws. It must adhere to the principles of transparency, legitimate purpose, and proportionality, [103] and the collection must be for a declared, specified, and legitimate purpose.[104] Personal data must be processed fairly and lawfully, and the processing thereof should ensure data quality.[105] Personal data should not be retained longer than necessary, and any authorized further processing must have adequate safeguards.[106]

3. Processing of Sensitive Personal Information and Privileged Information

Any and all forms of data which under the Rules of Court and pertinent laws are considered privileged communication are considered privileged information. Sensitive personal information

---

[95] Rep. Act No. 10173 (2012), § 4. Data Privacy Act of 2012.
[96] § 4(a).
[97] § 4(d).
[98] § 4(f).
[99] § 4(g).
[100] § 3(g).
[101] 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.
[102] Any person qualified as such and to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
[103] IRR of the Data Privacy Act of 2012, § 17, Rule IV.
[104] § 19, Rule IV.
[105] *Id.*
[106] *Id.*

pertains to personal information (i) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;[107] (ii) about an individual's health, education, genetic make-up, or sexual life, or to any proceeding for an offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;[108] (iii) issued by government agencies peculiar to an individual including social security numbers, previous or current health records, licenses or their denials, suspensions or revocations, and tax returns;[109] and (iv) specifically established by an executive order or an act of Congress to be kept classified.[110]

Processing of privileged information and sensitive personal information is allowed in specific instances, such as when the data subject has given his or her specific consent prior to processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;[111] processing is necessary to protect the life and health of the data subject or another person and the data subject is not able to express consent prior to the processing;[112] and processing concerns such personal information as is necessary for the protection of lawful rights and interests.[113]

4. Security Requirements

The Data Privacy Act of 2012 requires personal information controllers and personal information processors to implement reasonable and appropriate security measures for the protection of personal data.[114] They must take steps to ensure that any person who has access to personal data and under their authority only processes the data upon their instructions or as required by law.[115] The security measures should maintain the availability, integrity, and confidentiality of the personal data and these measures are intended to protect the personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as any other unlawful processing.[116]

Personal information controllers are required to comply with various safeguards including registering personal data processing systems operating in the country that involves accessing or requiring sensitive personal

[107] § 3(l)(1).
[108] § 3(l)(2).
[109] § 3(l)(3).
[110] § 3(l)(4).
[111] § 13(a).
[112] § 13(c).
[113] § 13(f).
[114] IRR, § 25, Rule VI.
[115] *Id.*
[116] *Id.*

information of at least 1,000 individuals, including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies and submitting an annual report of the summary of documented security incidents and personal data breaches.[117]

The personal data controller is given great responsibility and accountability, including being responsible for any personal data under its control or custody[118] and for complying with the requirements of the Data Privacy Act of 2012 and its IRR and other issuances of the National Privacy Commission.[119] The personal data controller carries a huge responsibility and is essential in a subject entity's compliance with the Data Privacy Act of 2012 and related governmental issuances.

5. Acts Penalized by the Data Privacy Act of 2012

The following are the acts penalized by the Data Privacy Act of 2012:

1. Unauthorized Processing of Personal Information and Sensitive Personal Information;[120]
2. Accessing Personal Information and Sensitive Personal Information Due to Negligence;[121]
3. Improper Disposal of Personal Information and Sensitive Personal Information;[122]
4. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes;[123]
5. Unauthorized Access or Intentional Breach;[124]
6. Concealment of Security Breaches Involving Sensitive Personal Information;[125]
7. Malicious Disclosure;[126]
8. Unauthorized Disclosure;[127] and
9. Combination or Series of Acts.[128]

The penalties for the commission of the foregoing

[117] § 46, Rule XI.
[118] § 50, Rule XII.
[119] *Id.*
[120] Rep. Act No. 10173 (2012), § 25.
[121] § 26.
[122] § 27.
[123] § 28.
[124] § 29.
[125] § 30.
[126] § 31.
[127] § 32.
[128] § 33.

offenses ranges from Php100,000 to Php5,000,000 and imprisonment of at least six months. Furthermore, the Data Privacy Act of 2012 also imposes stiffer penalties when the information involved is sensitive personal information.

G. National Centralized Identification System

A national identification (ID) system is a governmental tool for order and efficiency. Specifically, it is used to assist public agencies to identify and verify citizens availing of government services.[129] For this purpose, then Philippine President, Gloria Macapagal-Arroyo, issued Executive Order (EO) No. 420, which directed all government agencies, including government-owned and controlled corporations, which issue ID cards to their members or constituents, to adopt a unified multi-purpose ID system.[130] Section 3 of EO 420 limited the data to be collected and recorded, thus:

1. Name;
2. Home address;
3. Sex;
4. Picture;
5. Signature;
6. Date of birth;
7. Place of birth;
8. Marital status;
9. Names of parents;
10. Height;
11. Weight;
12. Two index fingers and two thumb marks;
13. Any prominent distinguishing features like moles and others; and
14. Tax Identification Number (TIN).

The Supreme Court ruled that EO No. 420 "narrowly limit[ed] the data that can be collected, recorded, and shown," and it "provide[d] strict safeguards to protect the confidentiality of the data collected."[131]

We contrast this with the case of *Ople v. Torres*, [132] involving Administrative Order (AO) No. 308 entitled "Adoption of a National Computerized Identification Reference System" issued by then President Fidel V. Ramos. AO No. 308 sought to establish a decentralized national computerized ID reference system among the key basic services and

[129] Senate Economic Planning Office Policy Insights, *National Identification System: Do We Need One?* (2005), available at https://www.senate.gov.ph/publications/PI%202005-12%20-%20National%20Identification%20System%20-%20Do%20We%20Need%20One.pdf (last accessed June 6, 2017).

[130] Exec. Order No. 420 (2005), §§ 1-2. This required all government agencies and government-owned and controlled corporations to streamline and harmonize their identification (ID) systems.

[131] Kilusang Mayo Uno v. Director General, G.R. No. 167798, April 19, 2006.

[132] G.R. No. 127685, July 23, 1998.

social security providers.[133] However, there is no limitation or enumeration of data to be collected, nor was there a provision on safeguards. This was struck down by the Supreme Court for being unconstitutional for its broadness, vagueness, and overbreadth, "which if implemented, will put [the] people's right to privacy in clear and present danger."[134] The Supreme Court clarified that it "is not *per se* against the use of computers to accumulate, store, process, retrieve and transmit data" so long as this is exercised within the limits set by the Constitution. It warned, however, that, "[g]iven the record-keeping power of the computer, only the indifferent will fail to perceive the danger that A. O. No. 308 gives the government the power to compile a devastating dossier against unsuspecting citizens."

While the establishment of a national ID system is proposed to help fight terrorism and prevent crimes and improve the delivery of government services, various groups continue to oppose it invoking privacy concerns, as well as administrative and financial arguments.[135] However, the Supreme Court has already held that privacy rights would not be a bar to government agencies adopting an ID system that is reasonable and constitutionally compliant. A number of countries have already implemented compulsory national ID systems, thus:[136]

> Some one hundred countries have compulsory national ID systems, including democracies such as Spain, France, Germany, Belgium, Greece, Luxembourg, and Portugal. Other countries which do not have national ID systems like the United States, Canada, Australia, New Zealand, Ireland, the Nordic Countries and Sweden, have sectoral cards for health, social or other public services.

Without a reliable ID system, government agencies like those involved in social security[137] and vehicular licensing[138] cannot perform their functions and even stand to suffer substantial losses from false names and identities.

---

[133] Adm. Order No. 308 (1996), § 1. This adopts a National ID System.

[134] *Kilusang Mayo Uno*, G.R. No. 167798, *supra* note 130. The Supreme Court also held that the adoption of a national ID system should be by legislation, not executive order.

[135] Senate Economic Planning Office Policy Insights, *supra* note 129.

[136] *Ople*, G.R. No. 127685, *supra* note 132.

[137] Government Insurance Security System and Social Security System.

[138] Land Transportation Office.

H. Registration of Prepaid Phones

While there has been some legislative action[139] to register the use of prepaid mobile devices for security purposes, this has been met with serious opposition in the Philippines, where 96 percent are subscribers of prepaid plans, on the basis that it is an intrusion into their private lives.

Additionally, there are arguments against the proposal to store personal identification data of all citizens related to the security of the storage of data, the economic burden, and the ineffectiveness of this as a solution for the problem sought to be addressed. These are arguments against the exercise of the state's police power in its aim to protect national security.

However, for the reasons cited below, we argue that legislation should be enacted to require registration of prepaid mobile phones.

1. Mobile Subscription in the Philippines

Registration of prepaid mobile phone subscriber identity module (SIM) has been objected to as an unconstitutional intrusion into one's privacy. With the enactment of the Data Privacy Act of 2012, and all the safeguards it offers, it is now submitted that registration of prepaid SIMs constitutes a

[139] H. No. 2328, 17th Congress (2016). An Act Requiring the Registration of All Users of Pre-Paid Subscriber Identity Module (SIM) Cards and Providing Penalties Therefor; H. No. 2588, 16th Congress (2013). An Act Requiring the Registration of Buyers of Prepaid SIM Cards and Providing Penalties Therefor; H. No. 2648, 17th Congress (2016). An Act Mandating the Registration of All Prepaid and Postpaid SIM Cards and Requiring the Telecommunication Companies to Keep a Registry of these Subscribers and Providing for the Penalties for Violation Thereof; H. No. 2809, 17th Congress (2016). An Act Requiring the Recording of the Identity of All Buyers of Prepaid SIM Cards for Cellular Phone Units and for Other Purposes; H. No. 3649, 17th Congress (2016). An Act Requiring the Recording of the Identity of All Buyers of Prepaid SIM Cards for Cellular Telephone Units and for Other Purposes; H. No. 3661, 17th Congress (2016). An Act Requiring the Registration of All Users of Prepaid Subscriber SIM Cards; S. No. 252, 17th Congress (2016). An Act Regulating the Sale of Prepaid SIM Cards, Providing Penalties for Violation Thereof, and for Other Purposes; S. No. 1202, 17th Congress (2016). An Act Prohibiting Text Scams, Misleading Advertisements, and Fraudulent Sales Promotions, Mandating for this Purpose the Registration of All Users of SIM Cards, and Providing Penalties for the Violations Thereof; S. No. 2911, 16th Congress (2015). An Act Requiring the Registration of All Users of Pre-paid SIM Cards; S. No. 2644, 15th Congress (2011). An Act Requiring the Registration of the Buyers of Prepaid SIM Cards, and Providing Penalties for the Violations Thereof; S. No. 2771, 15th Congress (2011). An Act Regulation the Sale of Pre-paid SIM Cards, Providing Penalty for Violation Thereof and for Other Purposes; S. No. 2911, 16th Congress (2015). An Act Requiring the Registration of All Users of Pre-paid SIM Cards.

legitimate exercise of the state's police power.

Prepaid customers buy SIM cards for their phones that they register with the cellular network. When the chip runs out of credit, they can buy a card with a new code allowing them to replenish their credit.[140] To illustrate the state of phone registration in the Philippines, in 2011, there were around 101 mobile cellular subscriptions per 100 people, a jump from 41 per 100 people in 2005. In 2011, 96 percent of the total subscriptions in the Philippines were prepaid.

In 2010, 99 percent of the population was covered by a cellular network and 80 percent of households reported usage of a mobile telephone.[141]

2. Prepaid Phones as Instruments of Criminality

Although there are many legitimate users of prepaid cell phones, they have become the communication device of choice for criminals, including terrorists, drug lords and gangs intent on masking their identities. Since prepaid phones can be purchased and activated without signing a contract or any other means of tracing the identity of the user, prepaid cell phones provide virtual anonymity.[142]

Terrorists use prepaid cell phone cards purchased anonymously to keep their communications secure. [143] A terrorist cell needs reliable channels of communication for its members, including highly secret channels to its leadership.[144] The 9/11 hijackers

---

[140] Shyam Tekwani, THE LOW END OF HI-TECH: NEW MEDIA AND COMMUNICATION TECHNOLOGIES AND TERRORISM IN ASIA (2004). *Paper presented at the annual meeting of the International Communication Association, New Orleans*. Available at http://www.allacademic.com/meta/p113115_index.html (last accessed June 6, 2017).

[141] World Bank, *Information and Communications for Development 2012: Maximizing Mobile,* WORLD BANK WEBSITE available at: http://documents.worldbank.org/curated/en/727791468337814878/pdf/722360PUB0EPI00367926B9780821389911.pdf (last accessed June 6, 2017).

[142] Chuck Schumer and John Cornyn, *Prepaid Cell Phones Help Terrorists like Times Square Bomber Evade Detection; Senators Propose First-Ever Federal Law to Require Phone Companies to Keep Records of Buyers' Identities*, (2010) available at: https://votesmart.org/public-statement/511650/schumer-cornyn-prepaid-cell-phones-help-terrorists-like-times-square-bomber-evade-detection-senators-propose-first-ever-federal-law-to-require-phone-companies-to-keep-records-of-buyers-identities#.WMJaFYGGOM8 (last accessed June 6, 2017).

[143] Michelle Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in: J. Arquilla and D. Ronfeldt, eds. NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME, AND MILITANCY. (Rand, 2001).

[144] Juan Miguel del Cid Gómez, *A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates*. PERSPECTIVES ON TERRORISM, [e-

used prepaid phones to communicate in the months prior to their attack. United States Federal Bureau of Investigation Director Robert Mueller cited the plotters' use of the devices to show that they "managed to exploit loopholes and vulnerabilities in our systems, to stay out of sight, and to not let anyone know what they were up to beyond a very closed circle."[145] In 2004, law enforcement authorities intercepted an Al-Qaeda terrorist cell using prepaid mobile phones issued by a Swiss mobile operator.[146] In 2007, three members of a terrorist cell that planned to carry out attacks in the US, Europe, and the Middle East used several stolen credit cards to buy items such as GPS systems, night vision goggles, sleeping bags, and hundreds of pre-paid mobile telephones from hundreds of websites, which were meant to be sent to jihadists in Iraq.[147] In the Philippines, the Abu Sayyaf are as "hi-tech" as they come, utilizing mobile phones to contact relatives and negotiators and are also sending text messages to the relatives of their kidnap victims in Manila.[148]

Aside from communication purposes, prepaid cell phones have been used as detonation devices for bombs, as was the case in the attack on a Madrid train that killed 191 people in Spain in 2004.[149] In the Philippines in 2011, a bomb inside a bus along EDSA, a major thoroughfare in Metro Manila, was detonated by a cellphone, killing five and leaving more than a dozen people injured. In 2013, an attack in a crowded bar in Cagayan de Oro, that killed eight and wounded more than 40, was carried out by a bomb triggered by a cell phone.[150]

Further, prepaid phones have long been used by other types of criminals, like drug sellers, mob figures, and gang leaders. In 2009, these were used by hedge fund managers and Wall Street executives who were implicated in the largest insider trading bust in US history. Traders from the Galleon Group hedge fund communicated with other executives through prepaid phones to try to evade wiretaps.[151] In the United States,

journal] 4(4). Available at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/113/html (last accessed June 6, 2017).

[145] Schumer and Cornyn, *supra* note 142.

[146] swissinfo.ch, *Swiss phone cards help trace al-Qaeda.* [online] Available at http://www.swissinfo.ch/eng/swiss-phone-cards-help-trace-al-qaeda/3799084 (last accessed June 6, 2017).

[147] del Cid Gómez, *supra* note 144.

[148] Tekwani, *supra* note 140.

[149] Schumer and Cornyn, *supra* note 142.

[150] Dexter San Pedro. *Register prepaid SIM cards? Palace wants more time to study proposal*. INTERAKYON, [online] (Last updated 1:54 p.m. July 30, 2013) available at http://www.interaksyon.com/article/67535/register-prepaid-sim-cards-palace-wants-more-time-to-study-proposal (last accessed June 6, 2017)

[151] Schumer and Cornyn, *supra* note 142.

Texas police receive more than 5,000 fraud complaints a year which use prepaid phones and report that there is little they can do because the trails end at the store, leaving the victims with nothing.[152]

In the Philippines, one of the many scams perpetrated with the use of prepaid phones is committed as follows:

> Text scammers use fictitious names or pose as government officials, send fraudulent text messages to their victims saying that their mobile phone numbers won in a raffle allegedly sponsored by the Bangko Sentral ng Pilipinas or other institutions.
>
> The scammers tell their victims that to be able to claim their alleged prize, they should first send money to the scammers thru a designated account in a bank or remittance company.
>
> The scammers also require their victims to send prepaid load to the scammers' prepaid mobile phone numbers.
>
> Once the scammers receive the money and prepaid load, the victims would no longer be able to get in touch with them again.[153]

Another example is when a defrauder dupes a subscriber into sending his own prepaid load via text message. This happens when a subscriber is deceived into sending a text message, the result of which is that the subscriber unwittingly does a "sharing" transaction with the defrauder.[154]

3. Registration of Prepaid Phones in Other Jurisdictions

Prepaid subscriptions represent a significant share of the global mobile phone market, although this varies widely from country to

---

[152] Angel Rodriguez-Miranda, *A case for a national prepaid cellphone registry*. THE HILL (2013) (Last updated 3:00 pm on September 28, 2013) available at http://thehill.hill.com/blogs/congress-blog/technology/325219-a-case-for-a-national-prepaid-cellphone-registry (last accessed June 6, 2017).

[153] Bangko Sentral ng Pilipinas. *Warning: Do not be fooled by text scammers!*, BANGKO SENTRAL NG PILIPINAS WEBSITE (2008), available at: http://www.bsp.gov.hp/publications/media.asp?id=1742 (last accessed June 6, 2017).

[154] Globe Telecom. *Globe Public Advisory on New Modus Operandi*, Facebook update, September 19, 2012, https://www.facebook.com/globeph/posts/10151087541159748 (Accessed 21 February 2017).

country. In the Organization for Economic Co-operation and Development (OECD) region, prepaid service accounted for about 40 percent of the mobile phone market in 2006.[155] In Mexico, over 90 percent of the mobile phone market is prepaid. South Korea reported almost no prepaid service in the country.[156] In the EU, Italy has over 90 percent prepaid subscribers and Portugal has almost 80 percent.[157] Finland has less than five percent of its population choosing prepaid subscription. [158] In the United States, prepaid is less than ten percent, and Canada has just over 20 percent.[159] As of July 2013, at least 80 countries, including 37 in Africa, have mandated, or at the least considered, requiring the registration of prepaid mobile subscriptions.[160]

In the regulation of prepaid services, countries like the members of the OECD—Australia, France, Germany, Hungary, Japan, Norway, Slovak Republic, South Africa, and Switzerland—require mobile operators to collect customer information for prepaid service.[161] The rationale for such a policy is for security concerns:

> In all cases, the rationale was to improve efficiency of law enforcement and national security activities. In some countries, the rationale is extended to include support for emergency services response and the commercial provision of public directory services. In a few cases, the requirement was raised in conjunction with specialized valued-added services (e.g., adult content, child minding); in certain cases, prepaid phone regulations are part of a wider legislative mandate that requires registration of all telephone services. [162]

Malaysia, Singapore, and Thailand require registration of prepaid cell phone users due mainly to their use by terrorists.[163] Other countries that have already

---

[155] Centre for Policy Research on Science and Technology. *Privacy Rights and Prepaid Communication Services: A Survey of prepaid mobile phone regulation and registration policies among OECD member states*. Research Report for the Office of the Privacy Commissioner of Canada (2006). Available at http://www.sfu.ca/sfublogs-archive/departments/cprost/uploads/2012/06/0601.pdf (last accessed June 6, 2017).

[156] *Id.*

[157] *Id*.

[158] *Id.*

[159] *Id*.

[160] Groupe Speciale Mobile Association, *The Mandatory Registration of Prepaid SIM Card Users: A White Paper* (2013), available at: http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf (last accessed June 6, 2017).

[161] Centre for Policy Research on Science and Technology, *supra* note 155.

[162] *Id*.

[163] Schumer and Cornyn, *supra* note 142.

implemented the registration of prepaid mobile users include: Algeria, Bolivia, Botswana, Brazil, Cameroon, Central African Republic, Chad, Cote d'Ivoire, Denmark, Democratic Republic of the Congo, Ecuador, Egypt, El Salvador, Eritrea, Ethiopia, Gabon, Ghana, Greece, Honduras, India, Italy, Kenya, Liberia, Madagascar, Morocco, Mozambique, The Netherlands, Niger, Nigeria, Papua New Guinea, Peru, Republic of Congo, Russia, Senegal, Sierra Leone, Spain, Sudan, Tanzania, Togo, Turkey, Vietnam, Zambia, and Zimbabwe.[164]

Telephone companies have prevented the enactment of the law. Citing privacy issues, the major wireless carriers, T-Mobile, AT&T, and Sprint, filed an injunction in Puerto Rico arguing that to require a formal Identification Card violated a person's right to privacy and security concerns such as those of battered women and crime victims. [165] In the United States, a proposed federal law, Senate Bill 3472, regarding the registration of prepaid phones died in 2010.[166]

II. Conclusion

Regulation is a justified exercise of police power by reason of compelling state interests. Rights of privacy are not absolute and must be balanced with the notion that public safety and welfare is paramount.

As criminals adopt new technology, the law must also adapt to ensure continued order in society. While most states in the international community already have some form of regulation to register even prepaid SIM cards, it is somewhat disappointing that the Philippine government has lagged behind.

The Philippines has passed the Cybercrime Prevention Act of 2012, which is patterned after the Budapest Convention on Cybercrime. This Convention is the first and only multinational agreement on cybercrime, "which the Philippine Government requested to be invited to accede to in 2007."[167] It is unfortunate that the section in the Cybercrime Prevention Act of 2012 that defines the term "traffic data" lacks the requisite safeguards to uphold its validity. However, we note that the Cybercrime Prevention Act of 2012 improves on the Budapest Convention "by clearly restricting traffic data to those that are non-content in nature."[168] Furthermore,

---

[164] For a complete list, *see* Groupe Speciale Mobile Association, *supra* note 160.

[165] Groupe Speciale Mobile Association, *supra* note 160.

[166] GovTrack.us. n.d. *S. 3427 (111th): Pre-Paid Mobile Device Identification Act.* Available at https://www.govtrack.us/congress/bills/111/s3427 (last accessed June 6, 2017)

[167] Sereno, J. Separate Opinion in *Disini*, G.R. No. 203335, *supra* note 14.

[168] *Id.*

the section "restricts traffic data to exclude those that refer to the identity of persons." [169] Thus, the Philippines' goal is to enhance the protection of cyberspace users against crime, while ensuring the privacy of individuals and the security of user data. Coupled with the Data Privacy Act of 2012, the Cybercrime Prevention Act of 2012 ensures the protection of the privacy of users of electronic communication.

The political system of each society is a fundamental force in shaping the legal contours of protected privacy, since certain patterns of privacy, disclosure, and surveillance are functional necessities for particular kinds of political regimes. In the Philippines, a compelling state interest must be shown to allow even the slightest intrusion into an individual's right to privacy.

Of course, reports of numerous offenses [170] can be regarded as enough reason to assert a compelling state interest. Law enforcement's need for prepaid phone registration outweighs perceived challenges to individual privacy. The anonymity accorded by prepaid mobile phones presents a massive obstacle to proper investigation of crimes and offenses and leaves society and victims with serious injustice.

Much of the international community has already adapted with the times and developed a system of registration. There is more reason to do so in the Philippines where almost all, about 96% as of 2011, of mobile phone users are prepaid subscribers.

To belong to a society is to sacrifice some measure of individual liberty.[171] As long as the legislature remains content with the laws that this country already has, offenses furthered through the use of prepaid mobile phones will continue to proliferate. Passing a law to register these devices is an important measure to deter and expose criminals hiding behind the anonymity afforded by prepaid mobile phones.

Finally, the legislative branch should not focus solely on the requirement of registration. Regulatory measures must be put in place to ensure safety and confidentiality in the storage of information. Increase in police power necessitates a proportional increase in privacy protection measures for individuals. With the passage of the Data Privacy Act of 2012 and the promulgation of its IRR, custodians of personal data are

---

[169] *Id.*

[170] H. No. 525, 16th Congress (2013). An Act Requiring the Registration of the Pre-Paid SIM Card Users and Mobile Phone Units and for Other Purposes.

[171] Morfe v. Mutuc, G.R. No. L-20387, *supra* note 1, citing RALPH LINTON, "The Individual, Culture, and Society" in THE CULTURAL BACKGROUND OF PERSONALITY, 1 (1945).

now made responsible and accountable for the safekeeping of personal and sensitive information.