DLSU Business & Economics Review 24.1 (2014), pp. 96-103

The Philippine Cybercrime Prevention Act of 2012: To Protect or Destroy?

James Keith C. Heffron
De La Salle University, Manila, Philippines
Heffron Esguerra Dy & de Jesus Law Office
Tycoon Centre, Pearl Drive, Ortigas Center 1605, Pasig City
james.heffron@dlsu.edu.ph / jkheffron@hedjlaw.com

Relatively new breeds of technology-related felonies called "cybercrimes" have proven to be a bane to different sectors of society, especially to business. The glaring damaging effects that it has caused to different business industries cannot anymore be ignored. However, is the Philippines adequately protected? Are its present laws sufficient to tackle the prongs of this blight? On the contrary, are these laws too myopically focused on eliminating cybercrime that certain freedoms have been overlooked, or worse, compromised? The aim of this paper is to essentially give an overview of the current protection and its effects on our basic rights. A special focus is given on the Cybercrime Prevention Act of 2012 and the perceived constitutionality or unconstitutionality of its provisions. The paper also aims to recommend a plausible alternative, which may provide an answer to the objectives of the anti-cybercrime thrust of the government but without sacrificing the consitutuional rights of the people.

JEL Classifications: K10, K14

Keywords: cybercrime, internet and business, civil and constitutional rights, information technology

"The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." – Eric Schimdt, Executive Chairman, Google (CNET News.com Staff, 1997, par. 5).

We live in a time when knowledge is just but a click away. Gone are the days when one had to painstakingly go over hard copies of literature just to do research. In fact, whole libraries of books may now be reduced to retrievable data that may be readily accessed through the simple swipe of the fingers, whether in the workplace, in transit, or in the comfort of our own homes. However, over two decades ago, this concept is almost unheard of.

Indeed, there has not been an evolution of such great magnitude in information technology as that we have seen for the past decade. At the helm of this evolution is this world-wide system of interconnected networks of computers that we now know as the Internet. According to www.internetworldstats.com, an international website which monitors global internet usage, the number of internet users as of June 30, 2012 is 2,405,518,376, which is 34.3% of the world population, and the growth of users from 2000 to 2012 is 566.4% (Internet Usage Statistics, 2012). This therefore shows that arguably, the Internet is steadily gaining a stature of power at a rate that may even be more than that of its less outrageous cousins—the so-called tri-media: print, television and radio.

As the world begins to realize the magnitude of this power, a new breed of business models

has rapidly emerged. From online market places where people can buy and sell all types of goods and services, to incentive marketing and advertising, where potential customers are given rewards for viewing certain websites, a myriad of internet related business ideas have prompted the rise of the so-called web entrepreneurs.

However, as with any other developing industry, it is not uncommon for some scheming groups or individuals to think of ways and means to take advantage and commit felonious acts for purpose of profit or gain. These acts, which have proven to be a bane in information technology or IT businesses, have been coined as "cybercrimes."

CYBERCRIME

The Oxford English Dictionary (n.d.) defined cybercrime as a *"*crime committed using computers or the Internet.*"* In the Philippines, the word has no express definition under the law. However, according to the Department of Justice (DOJ) (2012, p. 1) Primer on Cybercrime Law, it has been defined as *"*a crime committed with or through the use of information and communication technologies such as radio, television, cellular phone, computer and network, and other communication device or application." Following this definition, it seems that in our country, the term "cybercrime" is far-reaching and is not merely confined to felonies committed with the aid of computers or the Internet.

According to the Norton Cyber Crime Report of 2013, (Edelman Berland, 2013), which is a research commissioned by software company Symantec on the effects of cybercrime on consumers, cybercrime is notoriously becoming a big thorn in the IT dependent economies of the developed world. In 2013, the report says, the cost of consumer cybercrime has reached USD 113 billion with the number of victims rising to 378 million. In the Philippines, the DOJ (2012) Primer cited a 2010 report of Symantec, which stated that *"*87% of Filipino internet users were identified as victims of crimes and malicious activities committed online" (p. 2). It continues to state that "the Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP) has encountered 2,778 referred cases of computer crimes from government agencies and private individuals nationwide from 2003 to 2012" (p. 2).

With these glaring findings, one cannot any longer turn a blind eye on the looming fact that cybercrime may become an indubitable threat to the stability of our economy. Thus, an important question arises: are we and our businesses adequately protected under the law from the commission of cybercrimes?

CURRENT PROTECTION

As of now there are several laws which protect against the commission of the Philippine version of cybercrimes. The earliest is a 1965 law—Republic Act 4200 or the Anti-Wire Tapping Law—which makes it unlawful for a person to record private communication without the consent of the parties. Then we have Republic Act 8484 or the Access Device Regulation Act of 1998, which punishes acts that *"*obtain money or anything of value through the use of an access device, with intent to defraud or with intent to gain and fleeing thereafter" (Section 9). Access devices are defined as "any card, plate, code, account number, electronic serial number, personal identification number, or other telecommunications service, equipment, or instrumental identifier, or other means of account access that can be used to obtain money, good, services, or any other thing of value or to initiate a transfer of funds (other than a transfer originated solely by paper instrument)" (Section 3 (a)). Then in 2000, Republic Act 8792 or the E-Commerce Act was enacted, which for the first time acknowledged "the vital role of information and communications technology in nation-building" (Section 2). Pursuant to this declaration of policy, this law, among others, punished the following acts: (1) hacking or unauthorized access into a computer system or

server, (2) the introduction of computer viruses which shall result to destruction or theft of electronic data, (3) intellectual piracy, and (4) violations of the Consumer Act via the use of electronic messages. In 2009, recognizing the fact that information technology may be used to proliferate sexually-related crimes especially those that involve minors, Congress enacted Republic Act 9725 or the Anti-Child Pornography Act and Republic Act 9995 or the Anti-Photo and Voyeurism Act.

Though several sectors view that these laws are enough to penalize acts which may be deemed as cybercrimes, there were other sectors clamoring that a unified law should finally be enacted that will have an express, clearer, and more specific definition of acts that would constitute as such. Although this clamor supposedly started back in 2000 when Filipino student Onel de Guzman created the infamous I LOVE YOU virus that caused billions of dollars in damages in computer systems and networks around the world, it was only in 2012 that a law was finally enacted that categorically defined and punished cybercrimes - Republic Act 10175 or the Cybercrime Prevention Act of 2012 (Romero, 2012).

OVERVIEW OF CYBERCRIME PREVENTION ACT OF 2012

Republic Act 10175 or the Cybercrime Prevention Act of 2012 was the product of two bills respectively passed by the House of Representatives and the Philippine Senate in June 2012. In September of the same year, the final consolidated version of the said bills was signed by President Benigno Aquino III, thereby effectively making it into law. It is the very first law to mention the word "cybercrime" and to expressly list down specific acts which may constitute as such.

According to Section 4 of the law, these offenses are categorized into three groups as follows: (1) Offenses against the confidentiality, integrity and availability of computer data and systems; (2) Computer-related offenses; and (3) Content-related offenses. Aside from this, Section 6 effectively added another group when it provided that "all crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of (the law)" and that "the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be."

Aside from defining offenses that constitute cybercrimes and providing for its penalties, the law further laid down the mechanics for its enforcement and implementation. Section 10 mandated the National Bureau of Investigation (NBI) and Philippine National Police (PNP) to create special units within their respective organizations which are to be manned by investigators trained and tasked to only handle cybercrime cases. Section 12 authorizes these law enforcement units, with due cause, to collect or record real-time electronic traffic data which are transmitted through a computer system. "Traffic Data", according to the law, "refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities" (Section 12). However, it continues to add that "all other data to be collected or seized or disclosed will require a court warrant" (Section 12). Section 19 further grants certain prohibitory powers to the DOJ when it finds that there may be a violation of the law. Thus, "when a computer data is *prima facie* found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data."

The law further provides that the jurisdiction for cases falling under this law shall be with the Regional Trial Courts and that Filipinos abroad may be prosecuted as long as the following criteria is met:

> Any of the elements was committed within the Philippines or committed with the use of any

> computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines (Section 21).

THE ACT: BOON OR BANE?

Many argue that the Cybercrime Prevention Act of 2012 is a boon to business, specifically those relating to information technology, communications, business process outsourcing, and intellectual property. As piracy, fraud, and intellectual theft are disputably the greatest profit-killers of these industries, the implementation of this law will definitely limit or even eradicate these blights. Further, since it provides for clear and specific provisions on enforcement and implementation, this law has patently more teeth compared to the other cybercrime-related laws mentioned earlier. Thus, many believe that this law will help safeguard our information technology infrastructures as much of our industries today rely heavily on computer network systems and data security. These measures, as the argument continues, will surely contribute in boosting investor confidence, which in turn may lead to a positive multiplier effect, ultimately resulting in rapid economic growth.

With these advantages, it is not surprising that several business groups have expressed support for the law or at least kept mum on the issue. For one, the Business Processing Association of the Philippines (BPAP), which according to its website *www.bpap.org* is the "umbrella association for the information technology and business process outsourcing (IT-BPO) and GIC (Global In-House Center) industry in the Philippines," has been vocal in praising the passage of the law. BPAP (2012) is of the position that this law "adds another layer of protection for the industry against theft and fraud and will contribute to a sustainable, healthy business environment and reassure global clients" (BPAP welcomes signing of Cybercrime Prevention Act into law, 2012, par.1). In fact, BPAP CEO Benedict Hernandez maintains that

> the anti-cybercrime law will aid the industry in sustaining growth and global leadership. This new law validates the strong partnership we continue to build with the public sector, as well as the government's recognition of the industry's significant contribution to our economy and employment (par. 5).

However, with all its perceived economic benefits, many likewise contend that the law is a bane for it is teeming with constitutional defects. For instance, Section 6 of the statute states that

> all crimes defined and penalized by the Revised Penal Code . . . and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act . . . (and) the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code . . . and special laws, as the case may be.

In conjunction with this, Section 7 further states that "a prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws." These provisions essentially provide that for the very same felonious act, one may be separately charged for a violation of the said law and other separate criminal laws. This is a clear violation of one's right against double jeopardy, a right which is tightly guarded by Article III of the 1987 Philippine Constitution or the Bill of Rights.

Another is Section 19 of the Cybercrime Prevention Act of 2012, which legal experts call the "takedown clause," where the Department of Justice is empowered to unilaterally—that is without the benefit of a warrant duly issued by a court—to restrict or block access to computer data when it finds sufficient reason that there may be a commission of a cybercrime. Said provision, many perceive, is reminiscent of the notorious Arrest, Search, and Seizure Orders (ASSO) by law enforcement agencies prevalent during the dark days of Martial Law since it is a clear violation

of the due process clause enshrined in Section 1 of the Bill of Rights, which indistinctly states that "no person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of laws."

Finally, we have Section 4(c)(4), or the provision on internet libel, a last minute insertion by the Senate, which states that "unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future" shall likewise be considered as punishable under the Act. Many sectors, especially those in the tri- and social media, have vehemently opposed this provision saying that this provision is an abridgment of the freedoms of speech and the press.

Thus, due to the perceived unconstitutionality of these restrictive provisions, many dissenters have voiced their opposition stating that the repercussions of their implementation are dangerous, as they can serve as fodder for an abusive plaintiff with no other intention but to harass a helpless defendant or worse for a tyrant with no other intention but to silence his dissenters. Oppositionists of the law have not even minced words in going to the extent in calling it a form of E-Martial Law.

THE PHILIPPINE SUPREME COURT CASE

In late 2012, a total of 15 petitions have been filed before the Philippine Supreme Court by several individuals and groups, some respectively seeking the nullity of certain questionable provisions and the others praying for the revocation of the entire law itself. Having the same issues relating to the same law, these petitions were consolidated by the Court and deliberated as one case, the customary title of which is based on the first petition on the list—Disini, et.al. vs. Secretary of Justice, et al. (2014).

In October 9, 2012, the law's implementation was suspended due to an indefinite Temporary Restraining Order issued by the Supreme Court. On February 18, 2014, the Court finally issued a Decision upholding the constitutionality of the law. However, three provisions thereof were categorically stricken down for being unconstitutional: Section 4(c)(3) which refers to unsolicited commercial communications; Section 12 which refers to real-time collection of internet traffic data; and Section 19 which refers to restricting or blocking access to computer data or the so-called "take down clause."

In declaring Section 4(c)(3) as unconstitutional, the Court ruled that,

> to prohibit the transmission of unsolicited ads would deny a person the right to read his emails, even unsolicited commercial ads addressed to him. Commercial speech is a separate category of speech which is not accorded the same level of protection as that given to other constitutionally guaranteed forms of expression but is nonetheless entitled to protection. The State cannot rob him of this right without violating the constitutionally guaranteed freedom of expression. Unsolicited advertisements are legitimate forms of expression. (p. 21)

For Section 12, the Court indubitably criticized the law's vagueness or lack of clear meaning on the phrase "with due cause." Thus, the Court continued,

> indeed, courts are able to save vague provisions of law through statutory construction. But the cybercrime law, dealing with a novel situation, fails to hint at the meaning it intends for the phrase "due cause." The Solicitor General suggests that "due cause" should mean "just reason or motive" and "adherence to a lawful procedure." But the Court cannot draw this meaning since Section 12 does not even bother to relate the collection of data to the probable commission of a particular crime. It just says, "with due cause," thus justifying a general gathering of data. It is akin to the use of a general search warrant that the Constitution prohibits. (p. 39).

The Court boldly even stated that Section 12 may lead to unwarranted abuse since law enforcement agencies may use this as a means for blackmail, unjust coercion and extortion. Thus,

> admittedly, nothing can prevent law enforcement agencies holding these data in their hands from looking into the identity of their sender or receiver and what the data contains. This will unnecessarily expose the citizenry to leaked information or, worse, to extortion from certain bad elements in these agencies. (p. 40)

Finally, for Section 19, the Court struck it down for being in violation of the constitutional guarantees against unreasonable search and seizure, not to mention freedom of expression. Thus, the Court, in resolving in favor of the constitutional guarantee against unreasonable search and seizure, stated

> Section 2, Article III of the 1987 Constitution provides that the right to be secure in one's papers and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable. Further, it states that no search warrant shall issue except upon probable cause to be determined personally by the judge. Here, the Government, in effect, seizes and places the computer data under its control and disposition without a warrant. The Department of Justice order cannot substitute for judicial search warrant. (p. 44)

In defending the basic civil right of freedom of expression, the Court categorically stated that government enforcers cannot be made to unilaterally decide, based on their own judgment, when or what data to "take down." Thus,

> the content of the computer data can also constitute speech. In such a case, Section 19 operates as a restriction on the freedom of expression over cyberspace. Certainly not all forms of speech are protected. Legislature may, within constitutional bounds, declare certain kinds of expression as illegal. But for an executive officer to seize content alleged to be unprotected without any judicial warrant, it is not enough for him to be of the opinion that such content violates some law, for to do so would make him judge, jury, and executioner all rolled into one. (pp. 44-45)

On the other hand, much to the dismay of oppositionists, the Supreme Court declared highly contended sections like Sections 4(c)(4) (online libel), 6, and 7 (perceived double jeopardy provisions) as constitutional.

In supporting Section 4(c)(4), the Court opined that said provision is constitutional, subject to the condition that only the original author, and not those who would share it in social media, would be penalized. Thus, the Court stated,

> the Court agrees with the Solicitor General that libel is not a constitutionally protected speech and that the government has an obligation to protect private individuals from defamation. Indeed, cyberlibel is actually not a new crime since Article 353, in relation to Article 355 of the penal code, already punishes it. In effect, Section 4(c)(4) above merely affirms that online defamation constitutes "similar means" for committing libel. But the Court's acquiescence goes only insofar as the cybercrime law penalizes the author of the libelous statement or article. Cyberlibel brings with it certain intricacies, unheard of when the penal code provisions on libel were enacted. The culture associated with internet media is distinct from that of print. (p. 24)

Concerning Section 6, the Court ruled that this provision does not really add another group of offenses but instead "merely makes commission of existing crimes through the internet a qualifying circumstance (p. 32)." Thus,

> As the Solicitor General points out, there exists a substantial distinction between crimes committed through the use of information and communications technology and similar crimes committed using other means. In using the technology in question, the offender often evades identification and is able to reach far more victims or cause greater harm. The distinction, therefore, creates a basis for higher penalties for cybercrimes. (p. 32)

As for Section 7, the Court however qualified its ruling and stated that though the provision is constitutional, this however should not apply to online libel and online child pornography. Thus, the Court stated,

> the Solicitor General points out that Section 7 merely expresses the settled doctrine that a single set of acts may be prosecuted and penalized simultaneously under two laws, a special law and the Revised Penal Code. When two different laws define two crimes, prior jeopardy as to one does not bar prosecution of the other although both offenses arise from the same fact, if each crime involves some important act which is not an essential element of the other. With the exception of the crimes of online libel and online child pornography, the Court would rather leave the determination of the correct application of Section 7 to actual cases. (p. 33)

The Court however continued that

> online libel is different. There should be no question that if the published material on print, said to be libelous, is again posted online or vice versa, that identical material cannot be the subject of two separate libels. The two offenses, one a violation of Article 353 of the Revised Penal Code and the other a violation of Section 4(c)(4) of R.A. 10175 involve essentially the same elements and are in fact one and the same offense. . .Charging the offender under both laws would be a blatant violation of the proscription against double jeopardy. The same is true with child pornography committed online. Section 4(c)(2) merely expands the ACPA's scope so as to include identical activities in cyberspace. As previously discussed, ACPA's definition of child pornography in fact already covers the use of "electronic, mechanical, digital, optical, magnetic or any other means." Thus, charging the offender under both Section 4(c)(2) and ACPA would likewise be tantamount to a violation of the constitutional prohibition against double jeopardy. (p. 33)

Though several motions for reconsideration have been filed by separate groups questioning the said Decision for various reasons, the Supreme Court has already affirmed the same with finality.

BALANCING ECONOMIC BENEFIT VERSUS SAFEGUARD OF CONSTITUTIONAL RIGHTS

With the Decision of the Supreme Court, there appears, as of now, to be a semblance of stability and finality on the legality of the Cybercrime Prevention Act of 2012. However, notwithstanding the declarations of the Court, still, many sectors continue to criticize the law because of its allegedly perceived constitutional violations.

Thus, considering these developments, the next question is: is the current legal system of protection the best that the government can do?

There is no doubt that the spirit and intent of the Cybercrime Prevention Act of 2012 is noble, with many sectors saying that the passage of the law is long overdue. It is worthy to note that it took almost 12 years and several bills filed in Congress by countless lawmakers before the enactment of a real and more comprehensive anti-cybercrime statute. If there is one thing that may be conclusively presumed by the passage of this act, it is that this government has finally acknowledged the perils of cybercrime and has committed to formulate ways to curb or eradicate it.

However, with all its flaws, adding to it the people's general negative reaction, government should never get discouraged in working towards perfecting a law that would sufficiently address this objective without however sacrificing constitutional guarantees. If government lags on this initiative it is a given that the economic effects would be perilous.

Now that the concept of cybercrime has already been embedded in the public consciousness, this therefore is the perfect time and opportunity for Congress to study and consider the enactment of a unified Computer and Cyber Code. This Code

should replace all the scattered laws relating to cybercrime and contain all provisions relating to the lawful conduct of computer and internet usage, the definition of cybercrimes and its penalties, and rules on its enforcement and implementation.

Nonetheless, in the drafting of this Code, government should learn from history and set non-negotiable standards: First, the law should be clear and devoid of vague and unequivocal provisions which may be subject to various legal interpretations or worse nullification for being against the void-for-vagueness doctrine, which essentially provides that "a law is facially invalid if men of common intelligence must necessarily guess at its meaning and differ as to its application." (Sps. Carlos S. Romualdez and Erlinda R. Romualdez vs. Commission On Elections And Dennis Garay (2008) (p. 12)); second, it should not, at all instances, contain provisions which may directly or indirectly cause violations of our basic freedoms; and third, the enforcement and implementation thereof should be reasonable and within the limits provided for in procedural law.

With a comprehensive but integrated law following the said principles, it is with fervent hope that this will harmoniously strike a balance between economic benefit, protection of constitutional rights, and of course, the total obliteration of that bane called cybercrime.

BIBLIOGRAPHY

1987 Constitution of the Republic of the Philippines

BPAP welcomes signing of Cybercrime Prevention Act into law. (2012). Retrieved from http://www.teamasia.com/newsroom/read-client-*news.aspx?id=356:bpap-welcomes s*igning-of-cybercrime-prevention-act-into-law.

Berland, E. (2013). *Norton cyber crime report of 2013*. Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

CNET News.com Staff. (1997). Net Founders Face Java Future. Retrieved from http://news.cnet.com/Net-founders-face-Java-future/2100-1001_3-278526.html.

Cybercrime. (n.d.) In Oxford English Dictionary online dictionary. Retrieved from http://dictionary.oed.com.

Department of Justice (DOJ). (2012). *Primer on cybercrime law*. Retrieved from http://www.doj.gov.ph/news.html?title=DOJ%20releases%20Primer%20on%20Cybercrime&newsid=141.

Disini, et.al. vs. Secretary of Justice, et al. (Supreme Court, G.R. Nos. 203335, 203299, 203306, 203359, 203378, 203391, 203407, 203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518. (2014 February 18)).

Internet Usage Statitistics, The Internet Big Picture, World Internet Users and Population Stats. (2012). Retrieved from www.internetworldstats.com.

Republic Act 10175, The Cybercrime Prevention Act of 2012

Republic Act 4200, The Anti-Wire Tapping Law (1965)

Republic Act 7394, The Consumer Act of the Philippines (1992)

Republic Act 8484, The Access Device Regulation Act of 1998

Republic Act 8792, The E-Commerce Act (2000)

Republic Act 9725 or the Anti-Child Pornography Act (2009)

Republic Act 9995 or the Anti-Photo and Voyeurism Act (2009)

Romero, P. (2012 October 10). The Road to the Cybercrime Prevention Act of 2012 infographic. Retrieved from http://www.rappler.com/rich-media/13901-the-road-to-the-cybercrime-prevention-act-of-2012.

Sps. Carlos S. *Romualdez* and Erlinda R. *Romualdez* vs. Commission On Elections and Dennis Garay, (Supreme Court G.R. No. 167011 (2008 April 30).