DLSU
BUSINESS
NOTES AND BRIEFINGS
ISSN (Print): 2345-8216 | ISSN (Online): 2350-6814
Volume 2 | Number 2 February 2014
Ramon V. del Rosario College of Business
CBRD
Center for Business Research & Development

Boon or bane: Business and the anti-cybercrime law

Written by:

ATTY. JAMES KEITH C. HEFFRON
Ramon V. del Rosario
College of Business
De La Salle University

Introduction

"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 Schmidt, Executive Chairman, Google.**

When it comes to information technology or colloquially - IT, there has not been an evolution of such great magnitude as the progress that we have seen for the past decade. On February 4, 2014, we celebrated the tenth birthday of one of the driving forces of this evolution – the social media giant Facebook. Indeed, ten years ago, one cannot imagine being able to interact with his grade school classmate, co-worker, mother and gym instructor all in one online platform, or having to leave the house in order to do ordinary chores, engage in business transactions, get entertained or even earn money.

The internet, without any doubt, has already gained a stature of power. Arguably, as of now, even 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 that some people will 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 internet based or related businesses, have been coined as "cybercrimes."

Cybercrime

The Oxford English Dictionary defines a cybercrime as a *"crime committed using computers or the Internet.*" In the Philippines, the word has no express definition under the law but according to the Department of Justice (DOJ) Primer on Cybercrime Law,[1] 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 confined to felonies committed with the aid of computers or the Internet.

According to the Norton Cyber Crime Report of 2013, 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 Primer cited a 2010 report of security software Symantec, which stated, *"87% of Filipino internet users were identified as victims of crimes and malicious activities committed online."* It continues to state *"(t)he 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."*

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

Current protection

As of now, there are several laws that 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 through the use of an access device, with intent to defraud or with intent to gain and fleeing thereafter."* 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)."* 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."* Pursuant to this declaration of policy, this law, among others, punished the following acts: hacking or unauthorized access into a computer system or server, the introduction of computer viruses, which shall result to destruction, or theft of electronic data, intellectual piracy and even violations of the Consumer Act via the use of electronic messages. In 2009, Congress, recognizing the fact that information technology may be used to proliferate sexually related crimes especially those that involve minors, enacted Republic Act 9725 or the Anti-Child Pornography Act and Republic Act 9995 or the Anti-Photo and Voyeurism Act.

Although these laws penalized acts that supposedly may fall within its characterization, there are sectors clamoring that a law should be finally enacted that will specifically and clearly define acts that should constitute a cybercrime. Although this clamor supposedly started back in 2000 when Filipino student Onel de Guzman created the infamous I LOVE YOU virus which 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.[2]

Cybercrime Prevention Act of 2012

Section 4 of the Cybercrime Prevention Act lists down the acts that constitute a cybercrime and these offenses are essentially categorized in 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 cybercrime and providing for its penalties, the law further laid down the provisions for its enforcement and implementation. Section 10 mandated the National Bureau of Investigation (NBI) and Philippine National Police (PNP) to create units within their respective organizations, which are to be manned by special investigators trained and tasked to only handle cybercrime cases. Section 12 authorizes these law enforcement units to collect or record real-time electronic traffic data that 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."* However, it continues to add, *"All other data to be collected or seized or disclosed will require a court warrant."* 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 can be prosecuted as long as "*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."*

Reaction to the law

Many argue that the Cybercrime Prevention Act is a boon to business, specifically those related to information technology, communications, business process outsourcing, and intellectual property. As piracy, fraud and intellectual theft are arguably the greatest profit-killers of these industries; the implementation of this law will definitely limit or even eradicate these blights. Further, since it provided for clear and specific provisions on enforcement and implementation, this law patently has more teeth compared to the other cybercrime-related laws mentioned earlier. This without a doubt will help safeguard our information technology infrastructures as much of our industries today rely heavily on computer 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 therefore that several business groups have at least expressed support for the law or at the 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 expressly praised the passage of the law stating therein that the 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."* According to BPAP CEO Benedict Hernandez, *"(t)he 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."*

However, with all its perceived economic benefits, many likewise contend that the law is teeming with constitutional defects. For instance, Section 6 of the statute states, *"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, *"(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 one may be separately charged for a violation of the said law and other separate criminal laws for the very same felonious act. This provision is a clear violation of one's right against double jeopardy, a right that is tightly guarded by Section 7, Article III of the 1987 Constitution or the Bill of Rights, following the horrors of Martial Law.

Another is Section 19, 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 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."* One cannot deny that therefore that this provision is reminiscent of the notorious Arrest, Search and Seizure Orders (ASSO) by law enforcement agencies prevalent during the dark days of Martial Law.

Then we have the provision on internet libel, a last minute insertion by the Senate, which states, *"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."*[3] 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 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. Many have not even minced words in going to the extent in calling it a form of E-Martial Law.

In late 2012, a total of fifteen petitions have been filed before the Supreme Court, some respectively seeking the nullity of

certain questionable provisions and the others praying for the revocation of the entire law itself. At present, the law's implementation was suspended due to an indefinite Temporary Restraining Order issued by the Supreme Court in October 9, 2012.

Balancing economic benefit versus safeguard of constitutional rights

Though the Cybercrime Prevention Act was praised mostly by the business community because of the stern protection it guarantees, the next question is: are we willing to sacrifice our constitutional securities in the name of progress?

There is no doubt that the spirit and intent of the Cybercrime Prevention Act is noble, with many saying that the passage of the law is long overdue. It is worthy to note that it took almost twelve years and several bills filed in Congress by countless lawmakers before a real and more comprehensive anti-cybercrime statute has been finally enacted. The passage of this act is a testament to the fact that this government has finally acknowledged the perils of cybercrime especially in business and has committed to formulate ways to curb or eradicate it. However, with all its flaws, adding to it the people's reaction thereto, government still should never get discouraged in perfecting a law that would sufficiently address this objective. If government lags on this initiative it is a given that the economic effects will be perilous.

To obviate objections from most sectors of society, the author therefore suggests a better alternative. Now that the concept of cybercrime has already been embedded in the public consciousness, this is the perfect time and opportunity that the drafting of a unified Computer and Internet Code should seriously be considered. This Code will finally 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 provisions which may be subject to various interpretations; 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 law following the said standards, all can hope that this will finally strike a balance between economic benefit, protection of constitutional rights, and of course, the total obliteration of that bane called cybercrime.

This is an expanded version of an article of the same title published in the January 22, 2013 issue of the Manila Times under the opinion column Managing for Society.

Footnotes

[1] See http://doj.gov.ph
[2] See *"The Road to the Cybercrime Prevention Act of 2012"* infographic by Purple S. Romero posted in 10/09/12 in www.rappler.com
[3] See Section 4 thereof.

DLSU BUSINESS NOTES AND BRIEFINGS
ISSN (Print): 2345-8216 | ISSN (Online): 2350-6814

Published by the De La Salle University Ramon V. del Rosario - College of Business, Center for Business Research and Development (CBRD).
Volume 2 No. 2 February 2014.