Philippines Cyber Crime Protection Bill and its implications

February 10, 2012

Philippines recently tabled its Cyber crime Protection Bill which is supposed to propel the growth of the Philippines outsourcing industry.

The Philippines senate has passed the final reading of the Bill:2796, Cyber Crime Protection Bill of 2012. The declaration of the policy of the bill postulates in clear terms that the State recognises the indispensable role of Information and Communication industry which includes data processing, content production etc. and their role in the development of the economy. The bill also acknowledges the need to protect and safeguard the integrity of the computer and communication systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct.

Keeping in mind the aim of the bill which precisely matches with the business of outsourcing industry that basically deals with data processing ad computer systems, the bill holds influential implications for the booming Philippines Outsourcing Industry.

Kind of devices- access to which is protected

The bill protects computer data that refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system which is defined as device or a group of interconnected device which performs automatic processing of data.

Thus, electronic devices such as mobile phones, tablets, PCs and the data stored therein would squarely fit into the ambit of protected information.

Service Provider under the Bill

Service provider under the Bill is defined as any public or private entity that provides users of its service the ability to communicate by means of a computer system or any other entity that processes or stores computer data on behalf of such communication service or users of such service. Such service provider would be liable in case of any breach.

Subscriber's information protected under the Bill

This refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and which reveals subscriber's identity or any kind of personal information such as postal address, telephone no. etc.

Punishable acts under the Bill

Unlawful interference, the bill prohibits illegal access and interception with the computer system and the intentional and reckless alteration of computer data without permission.

The bill also prohibits use, production, sale, procurement, importation, distribution of a device, including a computer program for the purpose of committing any kind of cyber crime under this Act; or tampering with a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any Cybercrime.

However, no criminal liability shall attach when the use, production, sale, procurement, importation, distribution, or otherwise making available, or possession of computer devices/data referred to is for the authorized testing of a computer system.

Computer-related Forgery, that is the intentional input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, or the act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

Thus, the provision not only prohibits the Act of forgery but also the use of such forged data with the knowledge regarding it, making such crime a case of strict liability.

Computer-related Fraud, that is the intentional and unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby, with the intent of procuring an

economic benefit for one s e l f or for another person or for the perpetuation of a fraudulent or dishonest activity. However, if no damage has yet been caused, the penalty imposable shall be one degree lower.

Last but not the least, the Bill prohibits Unsolicited Commercial Communications, that is the transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless there is a prior affirmative consent from the recipient; or the following conditions are present:

i. 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;

ii. The commercial electronic communication does not purposely disguise the source of the electronic message; and
iii. 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
Under the Bill, not only the commission of such offenses but also the abatement or attempt to commit such crime is punishable.
All the offenses enumerated in the Act connotes that lawful interference with such computer system or data with due permission shall not come within the ambit of the cybercrime mentioned in the Act. This gives the BPO service provider to freely deal with the computer system.
However, at the same time it leaves open an option to the employees of the BPO service provider to indulge in offense proscribed in the bill under the garb of permission. In case of such act, under the provision of corporate liability given in Section 8 of the Bill, the judicial person incharge shall be held liable. This provision carries the potential to make the corporate organization more prudent in carrying out their business so as to avoid liability under the Cyber Crime Bill that would be enacted soon.
The Cyber Crime bill is heralded as the revelation of new era in the Philippines outsourcing industry. Business Processing Association of the Philippines (BPAP) believes the bill will be a big boost to the industry's goals as they aim to provide 4 million jobs to Filipinos and $25 billion in export revenues by 2016. As said by Benedict Hernandez, CEO, BPAP, the bill will be one of the keys in providing Philippines investors and customers with a sound business environment.

Ref.: http://outsourceportfolio.com/philippines-cyber-crime-protection-bill-and-its-implications/

Look also www.cybercrime.aboutphilippines.ph