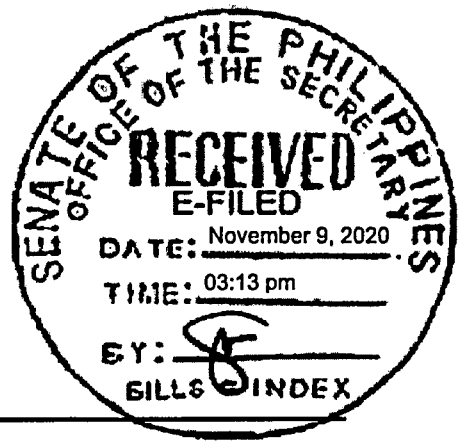
EIGHTEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
Second Regular Session)



SENATE
S.B. No. **1905**

Introduced by **SENATOR IMEE R. MARCOS**

AN ACT AMENDING REPUBLIC ACT NO. 10175 OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012," AND FOR OTHER PURPOSES

EXPLANATORY NOTE

Article XIV, Section 10 of the 1987 Philippine Constitution recognizes science and technology as "essential for national development and progress." This is perhaps most exemplified in the unprecedented advancements in the field of Information Communication Technologies (ICTs), which has permeated all facets of everyday life.

For the most part, advancements in ICTs and the advent of new technologies has changed our society for the better. After all, the inherent nature of the internet as a borderless medium encourages the exchange of ideas, facilitates instantaneous transactions, and keeps people connected, wherever they are in the world. Consequently, commercial dealings, businesses, banking, and even romantic relationships are moving, and flourishing, online.

However, the increased online presence and pervasive use of computers in everyday life – especially during this time in which the country has been placed under a state of public health emergency due to the COVID-19 pandemic – has also given rise to various new schemes and crimes which have left existing legislation insufficient or lacking. Advancements in the field of ICT have brought with them new, more insidious types of criminals, as ICT opens more opportunities for and facilitates the commission of crimes, leading to an unprecedented growth in the crime rate globally and in the Philippines.

Locally, the Philippine Department of Justice – Office of Cybercrime (DOJ-OOC) reports an alarming spike in illegal online activities in 2020 as compared to previous years. Specifically, they note the rise of various schemes and modus operandi such as online "love scams", elaborate bank heists, online estafa, and other cybercrimes which all have one thing in common – the use and abuse of ICT and the Internet. These scams are commonly committed by foreigners in the Philippines, while the victims are local Filipinos or overseas Filipino workers. In 2019 eleven (11) such cases were

reported by the DOJ-OOC. While for 2020 year to date alone, there have been a reported 46 cases of such scams and the number is increasing daily.

The Bangko Sentral ng Pilipinas (BSP) stated that based on the Reports on Crimes and Losses filed by banks during the ECQ period, from March 15 to May 18, 2020, 98.4% of all criminal incidents reported were classified as cyber or online in nature, amounting to P60.6 million or 54.5% of all total bank losses during the two-month period. And, 80.5% of all cyber incidents reported were credit card and internet banking-related, accounting for 79% of total losses.

Due to the ephemeral nature of computer data, and the anonymity which the internet allows, the perpetrators of such crimes have been able to operate freely and undetected. In light of the above, there has been a growing demand to give law enforcement more teeth in order to battle cybercrimes and other similar offenses.

This issue was sought to be addressed originally by Section 12 of Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act Of 2012," which sought to give law enforcement the authority to conduct real-time collection and recording of traffic data. However, in the case Disini v. The Secretary of Justice (G.R. No. 203335, 11 February 2014), this provision was declared unconstitutional for giving law enforcement authorities power which is "too sweeping and lacks restraint".

Nevertheless, the Supreme Court itself recognized in Disini that "[t]here are many ways the cyber criminals can quickly erase their tracks," and as such, "it is only real-time traffic data collection or recording and a subsequent recourse to court-issued search and seizure warrant that can succeed in ferreting them out." The law, however, should be "written with specificity and definiteness as to ensure respect for the rights that the Constitution guarantees."

Undoubtedly, as the Supreme Court held in Disini, the State has a compelling interest in enforcing the "Cybercrime Prevention Act Of 2012" as there is a dire need to put order to the tremendous activities in cyberspace for public good.

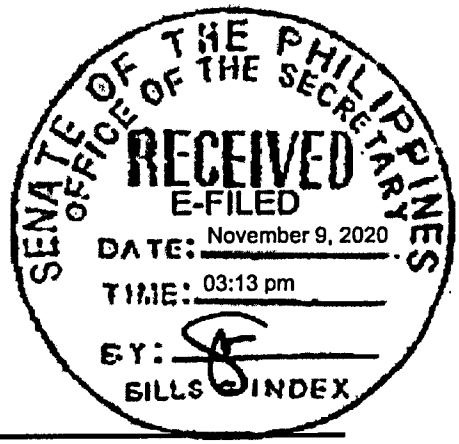
Therefore, this bill seeks to amend Republic Act No. 10175 otherwise known as the "Cybercrime Prevention Act of 2012," first, to specifically define and punish as a cybercrime cyber-estafa, or estafa committed by means of computer system. Second, this bill seeks to give law enforcement authorities the authority to conduct real-time collection and recording of traffic data, subject to the restraints and safeguards which the Constitution requires.

Given the abovementioned circumstances, the immediate passage of this bill is earnestly sought.

Imee R. Marcos

IMEE R. MARCOS

EIGHTEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
Second Regular Session)



SENATE
S.B. No. **1905**

Introduced by **SENATOR IMEE R. MARCOS**

AN ACT AMENDING REPUBLIC ACT NO. 10175 OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012," AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

SECTION 1. Section 4 of Republic Act No. 10175 otherwise known as the *"Cybercrime Prevention Act of 2012"* is hereby amended to read, as follows:

"Section 4. Cybercrime Offenses. – The following acts constitute the offense of cybercrime punishable under this Act:

XXX XXX XXX

(b) Computer-related Offenses.

(1) Computer-related Forgery. –

(i) The 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 regardless whether or not the data is directly readable and intelligible; or

(ii) 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.

(2) Computer-related Fraud. – The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided,* That if not damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(3) COMPUTER-RELATED ESTAFA. – THE UNLAWFUL OR PROHIBITED ACTS OF SWINDLING (ESTAFA) AND OTHER DECEITS AS DEFINED IN

ARTICLES 315, 316, 317 and 318 OF THE REVISED PENAL CODE, AS AMENDED, COMMITTED THROUGH OR BY MEANS OF A COMPUTER SYSTEM, WHETHER PARTIALLY OR IN ITS ENTIRETY, OR ANY OTHER SIMILAR MEANS WHICH MAY BE DEVISED IN THE FUTURE: PROVIDED, THAT IF NO DAMAGE HAS YET BEEN CAUSED, THE PENALTY IMPOSABLE SHALL BE ONE (1) DEGREE LOWER.

[(3)] (4) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided,* That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

xxx xxx xxx

SEC. 2. Section 12 of Republic Act No. 10175 otherwise known as the *"Cybercrime Prevention Act of 2012"* is hereby reinstated and amended to read, as follows:

"SECTION 12. *REAL-TIME COLLECTION OF TRAFFIC DATA FOR CERTAIN OFFENSES.* — THE SECRETARY OF JUSTICE OR THE DOJ – OFFICE OF THE CYBERCRIME, UPON DUE EVALUATION OF A VERIFIED COMPLAINT FILED BY ANY PEACE OFFICER, LAW ENFORCEMENT AGENT, OR PERSON DAMAGED OR LIABLE TO BE DAMAGED BY ANY OF THE CYBERCRIMES DEFINED IN THIS ACT, AND OFFICIALLY DOCKETED AND ASSIGNED FOR INVESTIGATION, MAY ISSUE AN ORDER DIRECTING LAW ENFORCEMENT AUTHORITIES TO COLLECT OR RECORD BY TECHNICAL OR ELECTRONIC MEANS TRAFFIC DATA IN REAL-TIME ASSOCIATED WITH COMMUNICATIONS TRANSMITTED BY MEANS OF A COMPUTER SYSTEM, WHICH COMMUNICATIONS ARE DULY SPECIFIED AND ALLEGED IN THE VERIFIED COMPLAINT, *PROVIDED* THE SECRETARY OF JUSTICE OR THE DOJ – OFFICE OF THE CYBERCRIME FINDS JUST REASON AND DUE CAUSE TO BELIEVE THE PROBABLE COMMISSION OF ANY OF THE CYBERCRIMES IN THE FOLLOWING CASES:

(1) WHEN THE CYBERCRIME IS COMMITTED OR TO BE COMMITTED BY A SYNDICATE. A CYBERCRIME IS DEEMED COMMITTED BY A SYNDICATE IF CARRIED OUT BY A GROUP OF THREE (3) OR MORE PERSONS CONSPIRING OR CONFEDERATING WITH ONE ANOTHER;

(2) WHEN THE CYBERCRIME IS COMMITTED OR TO BE COMMITTED IN LARGE SCALE. IT IS DEEMED COMMITTED IN LARGE SCALE IF (A) COMMITTED AGAINST THREE (3) OR MORE PERSONS, INDIVIDUALLY OR AS A GROUP OR (B) IF THE CYBERCRIME INVOLVES CASH, MONEY, PROPERTY OR ANYTHING OF VALUE, AMOUNTING TO AT LEAST TEN MILLION PESOS (P10,000,000); OR

(3) WHEN THE CYBERCRIME IS COMMITTED OR TO BE COMMITTED AGAINST VULNERABLE PERSONS OR GROUPS, WHICH SHALL INCLUDE, BUT ARE NOT LIMITED TO, MINORS, OVERSEAS FILIPINO WORKERS (OFWS), PERSONS WITH DISABILITY (PWD), AND SENIOR CITIZENS, AS THESE ARE RESPECTIVELY DEFINED UNDER APPLICABLE LAWS;

PROVIDED FURTHER, **THAT SUCH LAW ENFORCEMENT AUTHORITIES WHO IMPLEMENTED AND/OR ENFORCED SUCH ORDER, MUST WITHIN A PERIOD NOT EXCEEDING TEN (10) DAYS OF SUCH COLLECTION AND/OR RECORDING, THEREAFTER EITHER (I) APPLY FOR A COURT SEARCH AND SEIZURE WARRANT FOR THE SEIZURE, COLLECTION OR DISCLOSURE OF OTHER NON-TRAFFIC DATA OR (II) FILE A CRIMINAL COMPLAINT WITH THE PROPER COURT OR TRIBUNAL;** ***PROVIDED, FINALLY,*** **THAT UPON THE EXPIRATION OF THE SAID TEN (10) DAY PERIOD WITHOUT AN APPLICATION FOR SEARCH AND SEIZURE WARRANT OR COMPLAINT BEING FILED, ANY TRAFFIC DATA COLLECTED AND/OR RECORDED UNDER THIS SECTION MUST BE DELETED AND RETURNED, AND MAY NOT BE USED AS EVIDENCE AGAINST ANY PERSON IN ANY PROCEEDING.**

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. 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; ***PROVIDED, THAT*** **FOR PURPOSES OF THIS SECTION, SERVICE PROVIDERS DIRECTED BY LAW ENFORCEMENT AUTHORITIES TO COOPERATE AND ASSIST IN THE COLLECTION OR RECORDING OF THE ABOVE-STATED INFORMATION WILL BE EXEMPT FROM THE PROVISIONS OF REPUBLIC ACT NO. 10173, OTHERWISE KNOWN AS THE DATA PRIVACY ACT OF 2012, REPUBLIC ACT NO. 1405, OTHERWISE KNOWN AS THE SECRECY OF BANK DEPOSITS LAW, REPUBLIC ACT NO. 6426, OTHERWISE KNOWN AS THE FOREIGN CURRENCY DEPOSIT ACT OF THE PHILIPPINES, AND OTHER SIMILAR OR RELATED PRIVACY AND/OR CONFIDENTIALITY LAWS AND REGULATIONS."**

Sec. 3. *Repealing Clause.* – All laws, decrees, orders, rules and regulations or other issuances or parts thereof inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

Sec. 4. *Separability Clause.* – If any portion or provision of this Act is declared unconstitutional, the remainder of this Act or any provision not affected thereby shall remain in force and effect.

Sec. 5. *Effectivity.* – This Act shall take effect after fifteen (15) days following the completion of its publication either in the Official Gazette or in a newspaper of general circulation in the Philippines.

Approved,