HACKING AND THE E-COMMERCE ACT

Atty. AL. S. VITANGCOL III, CHFI, CEI
Managing Lawyer, AVALaw
President & CSO, i-technoLAWgy SYSTEMS SOLUTIONS INC.

Philippine Hackers Convention
October 23, 2010
Overview of E-Commerce
Background of RA 8792
ILOVEYOU Virus

- A computer virus that hit numerous computers in 2000, when it was sent as an attachment to an email message.
- The virus arrived in e-mail boxes on May 4, 2000.
- Email has a subject of "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs".
Effects of ILOVEYOU Virus

• The virus began in the Philippines on May 4, 2000, and spread across the world in one day (traveling from Hong-Kong to Europe to the United States).
• It infected 10 percent of all computers connected to the Internet and causing about $5.5 billion in damage.
• By 13 May 2000, 50 million infections had been reported. Most of the "damage" was the labor of getting rid of the virus.
• The Pentagon, CIA, and the British Parliament had to shut down their e-mail systems to get rid of the virus, as did most large corporations.
Legislative Aftermath

- The authors of the virus were Filipinos - siblings Irene and Onel de Guzman, Reomel Lamores, and Michael Buenafe.
- Onel de Guzman denied writing the virus, although he said he may have inadvertently been responsible for its release.
- As there were no laws in the Philippines against virus-writing at the time, they were released and the prosecutors dropped all charges against them.
- The original charges brought up against de Guzman dealt with the violation of RA8484, *Access Devices Regulation Act of 1998*. 
Philippine E-Commerce Act

ELECTRONIC COMMERCE ACT OF 2000
[Republic Act No. 8792]
AN ACT PROVIDING FOR THE RECOGNITION AND USE
OF ELECTRONIC COMMERCIAL AND NON-
COMMERCIAL TRANSACTIONS AND DOCUMENTS,
PENALTIES FOR UNLAWFUL USE THEREOF AND FOR
OTHER PURPOSES

Signed into law on June 14, 2000.
• Consolidation of Senate Bill No. 1902 and House Bill No. 9971.

• Both bills were primarily based upon the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce

• Final form has 42 sections/provisions.
Rationale

• Government’s attempt at a comprehensive verification and authentication of electronic documents.
• Designed to aid in the adoption of the Internet and other electronic media as a legitimate channel for domestic and international transactions.
• Recognizes electronic documents and signatures as valid legal transactions.
• Requires the government to computerize front-line transactions, within two years from the effectivity of the law, or specifically by July 2002.
Government Websites Hacked

- LTO, PRC
- 12/28/09. DOH
- 12/30/09. NDCC
- 01/04/10. DSWD
- 01/07/10. DOLE
- 01/10/10. TESDA
- 01/25/10. TESDA
- 05/10/10. COMELEC?
HAPPY NEW YEAR!!!

DON'T USE FIRECRACKERS!!!!

USE PENIS
What Cybercrimes are penalized under the Philippine Ecommerce Act?
Computer Hacking

• **Computer hacking** originally means the rapid development of new programs or the reverse engineering of already existing software to make the code better and more efficient.

• **Hacker** - a person who enjoys learning the details of computer systems and stretches their capabilities.
Computer Cracker

• **Cracker** - refers to a person who uses his hacking skills for offensive purposes; malicious hacker; a.k.a black hat hacker

• The term ‘**hacking**’ has over time gained negative meaning and had been associated with destructive or undesirable activities.

• The term ‘**hacker**’ is now synonymous with ‘**cracker**’.
(a) **Hacking** or cracking which refers to **unauthorized access** into or interference in a computer system/server or information and communication system; **or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices**, without the knowledge and consent of the owner of the computer or information and communications system, **including the introduction of computer viruses and the like**, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years.
Two Types of Hacking:

1. Unauthorized access into or interference in a computer system/server or information and communication system.

(a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, or introducing computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document.

2. Any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document.

Section 33(a) of E-Commerce Act of 2000

Any act that is committed in the course of or in connection with the commission of any of the acts described in the preceding paragraph shall be an act committed in the course of or in connection with the commission of an offense under this section and shall be punishable by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years.
Computer Hacking as a Crime

Two Types of Hacking:

1. Unauthorized access into or interference in a computer system/server or information and communication system.

   (a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document.

Elements of the Crime (2nd Type):

1. Any access using a computer or other similar information and communication devices;

2. Done in order to corrupt, alter, steal, or destroy, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document.

3. Without the knowledge and consent of the owner of the computer or information and communications system;

4. Resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document.
Computer Piracy as a Crime

Elements of the Crime:

Section 23(b) of the E-Commerce Act of 2000 - (b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature, or copyrighted work, including legally protected sound recording or phonogram or information material on telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years.
Criminal Case No. 419672-CR
MTC-Branch 14, Manila

Facts of the Case:
• JJ Maria Giner penetrated government websites of National Economic and Development Authority, National Book Development Board, the Philippine Navy, and the web servers or computer systems hosting websites of local Internet service provider Bitstop in Dagupan City and University of the Philippines.
• Giner also launched attacks on the websites of the Office of the Presidential Management Staff in Malacañang, the Task Force on Security of Critical Infrastructure, the PRC, the DOLE, and TESDA.
• Giner sent an e-mail to NEDA, informing the agency about the vulnerability of its website to hackers.
Outcome of the Case:

- The DoJ resolution said Giner had clearly violated section 33a of the E-commerce Law (RA8792) because he was not authorized to access government websites. "Intention is not essential in this mode as mere unauthorized access is a violation of the law," the resolution said.

- On September 28, 2005, JJ Maria Giner was convicted for violation of Section 33 (a) of the E-Commerce law which involved the act of hacking the government portal "gov.ph" and other government websites.

- Judge Rosalyn Mislos-Loja, sentenced Giner to one to two years of imprisonment and to pay a fine of 100,000 pesos. However, Giner immediately applied for probation, which was eventually granted by the court.
Contact information

📞 AVALaw, (02)9082588
✉️ asvitangcol@gmail.com
📞 i-technoLAWgy Systems Solutions Inc.
  (02)7299752
📞 (0917)5025336
🌐 www.AttyALSVitangcoliiii.com