Fighting Cybercrime, Fighting for Integrity in Cyberspace

Geronimo L. Sy
Department of Justice
09 October 2012 Manila
Premises

- Emergence of cybercrime
- Substantial difference between physical and virtual worlds
- Reach, accessibility and convenience
- Permanence
- The need for law or regulation
Int’l Cybercrime Conference (2007)

Data Privacy Act

Cybercrime

Cybersecurity
- Twin computer forensics laboratories, 2001–2003
- 2004 – 1st cybercrime conviction (PNP–CIDG)
- 2006 – 2nd cybercrime conviction (NBI)
Revised Penal Code

Special Penal Laws

Revised Penal Code

Special Penal Laws

Revised Penal Code

Cybercrime

1932 → 1960s → 2000 → 2012

(E-Commerce Act)
REPUBLIC ACT NO. 10175

CYBERCRIME PREVENTION ACT OF 2012
SEC. 4(c)(4). *Libel*. — The 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.*
**EJUSDEM GENERIS**

Of the same kind

In the construction of laws, wills and other instruments, when certain things are enumerated, and then a phrase is used which might be construed to include other things, it is generally confined to things ejusdem generas.
Section 1. It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or dictaphone or walkie-talkie or tape recorder, or however otherwise described:

RA 4200: Anti-Wire Tapping Act of 1965
SEC. 5. Other Offenses. — The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. — Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

- Penalty is one (1) degree lower
SEC. 6. 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 this Act: Provided, 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.
Expressio unius est exclusio alterius

The expression of one thing is the exclusion of another
SEC. 4(c)(2). *Child Pornography.* — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti–Child Pornography Act of 2009, committed through a computer system. Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775.
Section 17. *Liability under the Revised Penal Code and other laws.* – Prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code or any other law.
SEC. 7. Liability under Other Laws. — 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.
“For instance, I told him, if a woman commits adultery using a computer, she would be guilty of a cybercrime and her penalty would be one degree higher.”

“To use my previous example of the case of the woman accused of adultery, because of Section 6, if a married woman’s e-mail to her lover were submitted as evidence, her penalty if convicted automatically becomes one degree higher.”

—from “The Cybercrime Law was brought to you by 7 senators & 12 congressmen,” an online article by journalist Raissa Robles
SEC. 12. *Real-Time Collection of Traffic Data.* — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

*Traffic data* or *non-content data* refers to any computer data other than the content of the communication including, but not limited to, the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.
SEC. 19. Restricting or Blocking Access to Computer Data. — 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.
transcendent, time critical, clear and present danger rule,
patently illegal acts
Luneta incident
How to make IED's creating panic or fear terrorism
mass suicide quarantine public health warrantless arrest checkpoint search HDO
*prima facie* versus probable cause

Not open-ended, 3 days

*ex parte*

Notification process

Attributable

Publication

Appeal
SEC. 20. Noncompliance. — Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of *prision correctional* in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.
Is there more?

We have too many laws.  
The problem is implementation.

But what is implementation?
How do we make implementation work?

Understand and assess needs.

Framework or approach.

Hard work.

Structure.

People.

Feedback.
**Cybersecurity** refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.
SEC. 4(a)(6)

Cyber-squatting. — The acquisition of domain name over the Internet in bad faith to profit, mislead, destroy reputation, and deprive others from the registering the same, if such a domain name is:
RA 10175

SEC. 4(c)(1). **Cybersex.** — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.
Special Laws

RA 10175 – Cybercrime Prevention Act of 2012

RA 9995 – Anti-Photo and Voyeurism Act of 2009

RA 9725 – Anti-Child Pornography Act of 2009

RA 9208 – Anti-Trafficking in Persons Act of 2003

RA 8792 – E-Commerce Act of 2000

RA 8484 – Access Device Regulation Act of 1998
<table>
<thead>
<tr>
<th>Offenses under Budapest Convention on Cybercrime</th>
<th>Offenses under RA 10175</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offenses against the confidentiality, integrity and availability of computer data and systems</td>
<td>Offenses against the confidentiality, integrity and availability of computer data and systems</td>
</tr>
<tr>
<td>a. Illegal Access</td>
<td>a. Illegal Access</td>
</tr>
<tr>
<td>b. Illegal Interception</td>
<td>b. Illegal Interception</td>
</tr>
<tr>
<td>c. Data Interference</td>
<td>c. Data Interference</td>
</tr>
<tr>
<td>d. System Interference</td>
<td>d. System Interference</td>
</tr>
<tr>
<td>e. Misuse of Devices</td>
<td>e. Misuse of Devices</td>
</tr>
<tr>
<td>f. Cyber-squatting</td>
<td></td>
</tr>
<tr>
<td>Computer–related Offenses</td>
<td>Computer–related Offenses</td>
</tr>
<tr>
<td>Content–related Offenses</td>
<td>Content–related Offenses</td>
</tr>
<tr>
<td>a. Offenses related to child pornography</td>
<td>a. Cybersex</td>
</tr>
<tr>
<td>c. Unsolicited Commercial Communications</td>
<td>c. Unsolicited Commercial Communications</td>
</tr>
<tr>
<td>d. Libel</td>
<td>d. Libel</td>
</tr>
<tr>
<td>Offenses related to infringements of copyright and related rights</td>
<td>Other Offenses</td>
</tr>
<tr>
<td>a. Offenses related to infringements of copyright and related rights</td>
<td>a. Aiding or Abetting in the Commission of Cybercrime</td>
</tr>
<tr>
<td>Ancillary liability and sanctions</td>
<td>b. Attempt in the Commission of Cybercrime</td>
</tr>
<tr>
<td>a. Attempt and aiding or abetting</td>
<td></td>
</tr>
<tr>
<td>All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of ICTs</td>
<td></td>
</tr>
<tr>
<td>Liability under Other Laws</td>
<td></td>
</tr>
</tbody>
</table>
Implementation – Criminal Justice Response

- Q and A Guide on Cybercrime
- Joint Investigation Manual for Law Enforcement and Prosecutors
- Electronic Evidence Guide (specialized forms)
- Accession to Convention on Cybercrime (COC)
- Build a network of monitors, investigators, prosecutors, public defenders, judges
Procedure for Detection and Filing of
Complaints

Sources of Detection
(No cut-and-dried approach)

- Private Complaints Directed thru System Audit or Use of Available Detection Tools/Systems
- By NBI/PNP Cybercrime Unit by Chance monitoring using Tools for Detection
- Digital Evidence/ Real Time Collection of Data

- 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. (Sec. 12)
- Request from other countries for mutual Assistance (Sec. 23)

Investigation Conducted by Cybercrime Unit PNP/NBI or Case Build Up Undertaken by a Joint Investigative Task Force Composed of Special Investigators & Designated Prosecutors and Cyber and Digital Forensic Experts

Investigation

Search and Seizure
- Secure warrant for search and seizure
- Secure and obtain copy of the computer system and computer data
- Conduct forensic analysis and examination (Sec. 15)

All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package (Sec. 16)

Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination. (Sec. 17)

Once the computer data preserved, transmitted, or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document of the investigators to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

Data Collection (Sec. 12). Secure for Court Warrant for Release of Data

Preservation of Data 6 mos. from transaction and may be extended for 6 mos. (Sec. 13)

Disclosure of Data Secure court warrant against service provider to disclose or submit subscriber’s information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order on the basis of valid complaint for investigation and disclosure

Search and Seizure
- Secure warrant for search and seizure
- Secure and obtain copy of the computer system and computer data
- Conduct forensic analysis or examinations

Offenses Covered by the Investigation (Secs. 4 - 6)
- Offenses against the confidentiality, integrity and availability of computer data and systems
- Computer-related Offenses
- Content-related Offenses
- Other Offenses: Aiding or Abetting in the Commission of Cybercrime, Attempt in the Commission of Cybercrime
- 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
Implementation – Societal response

Internet safety for children
Civility in cyberspace
Restorative justice
Crowd-sourcing
Accreditation
Leila M. De Lima <Imdelima.doj@gmail.com>

re: Sex videos and cybercrime law
1 message

Tue, Oct 2, 2012 at 10:57 PM

To: "Imdelima.doj@gmail.com" <Imdelima.doj@gmail.com>

Ginang De Lima,


Maraming Salamat po,
Way Forward

Collaboration with all stakeholders

Oversight on law enforcement agencies

Focus on syndicates and organized crime