

CYBERCRIME LAW:

INTERNATIONAL BEST PRACTICES

Craig J. Blakeley

Doha Information Security Conference

Doha, Qatar

June 10 - 11, 2008



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Cybercrime Law

- **Why do we need cybercrime law?**
- **What are the elements of cybercrime law?**
- **Some emerging issues in cybercrime law.**

The Role of Cybercrime Law

- **Cybercrime law is not by itself sufficient to deter or address cybercrime. However, it is a critical component in:**
 - **Developing a National Strategy for Cybersecurity**
 - **Deterring Cybercrime; and**
 - **Promoting a National Culture of Cybersecurity**

Why Do We Need Cybercrime Law?

- **Conventional/Traditional Law is not sufficient to cover cybercrime.**
- **Cybercrime can be very costly and can seriously weaken confidence in ICT, thus disrupting economic growth and development.**
- **Cybercrime is increasingly international in scope.**

Conventional/Traditional Law Is Not Sufficient to Cover Cybercrime

- **What do we mean when we say “cybercrime?”**
- **In its broadest sense, we mean any type of misconduct or crime that can be committed or assisted through the use of a computer or the Internet.**

Cybercrime: What is it?

- **Use of a computer/Internet to do something that would be a crime in any case.**

Analogy: Murder is the taking of a human life without justification whether done with a rock, a sword, a gun electricity, poison, etc. The crime is defined in terms of the end result -- not how that result was brought about.

- **Fraud (credit card or identity theft)**
- **Child Pornography**
- **Intellectual Property Violations**
- **Stalking**

Cybercrime: What is it?

- **Use of a computer/Internet to commit a “traditional” crime in a different way or to dramatically increase the impact of a “traditional” crime.**
 - **Fraud (credit card or identity theft)**
 - **“Phishing” -- obtaining identity information or credit card numbers by masquerading as a legitimate business representative (such as a Web site or through e-mail)**
 - **Child Pornography & Intellectual Property Violations**
 - **Internet can be used to distribute on a worldwide basis & can be used to hide geographic location of crime or to escape jurisdiction**

Cyber Crime: What is it?

- **Use of a computer/Internet to commit a “traditional” crime in a different way or to dramatically increase the impact of a “traditional” crime. (*cont.*)**
 - **Cyberstalking -- Use of e-mail or other electronic communication by computer to threaten, harass, or put an individual in fear of harm.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Cyber Crime: What is it?

- **Use of a computer/Internet to do something that we want to prohibit (i.e., make criminal) but which action (crime) would not be possible without a computer/Internet.**

Analogy: Drunk driving would not be a crime (i.e., would not be possible) without an automobile.

- **Computer viruses**
- **Spam**
- **Hacking**
- **Distributed Denial of Service Attacks**

A Cybercrime Law is Necessary Because Traditional Penal Laws Are Not Adequate.

- **Credit Card Fraud (for example):** Under existing law a fraudulent transaction does not lose its fraudulent (i.e., criminal) nature just because it takes place online rather than through a paper transaction. However, the impact may be significantly greater when it takes place online.
- **Hacking, Denial of Service Attacks, Viruses etc.:** Existing Laws are insufficient. There is not a physical entry or taking. And even if laws could be interpreted to cover such activity (a dubious proposition), the deterrence effect of a law of uncertain application would be very low.

Risks in the Absence of a Specific Law

- **Example: The Love Bug Virus**
 - **Originated with a student in the Philippines in 2000**
 - **Spread via e-mail with the subject of “I Love You” and an attachment reading “LOVE-LETTER-FOR-YOU”**
 - **The virus overwrote important files and sent a copy of the e-mail and virus to everyone in the computer’s e-mail address book**
 - **Net result was an estimated \$10 billion (U.S.) in economic damages worldwide**
 - **Perpetrator could not be prosecuted in the Philippines because there was no law that prohibited this conduct (e-commerce law was under consideration but had not yet been adopted)**

Cybercrime Has a High Cost and Disruptive/Destructive Consequences

- **Pervasive Nature and Growing Importance of the Internet and Computers**
- **Economic Importance of Computers & the Internet (Information & Communications Technology -- “ICT”)**
- **Cyber Crime Can Remove or Destroy Substantial Amounts of Economic Value from the Internet, Thus Increasing Costs, Consuming Resources, Discouraging New Investment, and Causing a Loss of Confidence in the Internet**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Cybercrime Is Increasingly International in Scope

- **Cybercrime is increasingly decentralized, spread across numerous countries. In this way, perpetrators can avoid better avoid detection and enforcement efforts.**
- **The ITU and others have indicated that there is evidence that cybercriminals tend to locate where relevant law is weakest or non-existent.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Cybercrime Is of Concern in the Middle East

- **The Casablanca Conference on Cybercrime (June, 2007)**
 - **“Laid focus on the issue of law reform in the Arab countries, and the role of cooperation in initiating laws, on the national and regional levels, that conform to the international standards of criminalization and prevention,” and “urged the establishment of a legal framework of cooperation between the Arab and foreign public prosecution offices or the assisting apparatuses in order to curb the grown and development of these crimes.”**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Cybercrime Is of Concern in the Middle East *(cont.)*

- **The Cairo Conference on Cybercrime (Nov. 2007)**
 - **“Participants note with appreciation the efforts underway in Egypt and other countries of the Arab region with regard to the strengthening of cybercrime legislation. These efforts should be given high priority and completed as soon as possible in order to protect the region from the threat of cybercrime.”**
 - **“The Budapest Convention (2001) on Cybercrime is recognized as the global guideline for the development of cybercrime legislation. Countries of the Arab region are encouraged to make use of this model . . .”**

Cybercrime Is of Concern in the Middle East *(cont.)*

- **The Doha Conference on Cybercrime (Feb. 2008) focused on elements of the ITU Cybersecurity Framework including:**
 - **Developing a National Strategy for Cybersecurity**
 - **Establishing a National Government-Industry Collaboration**
 - **Deterring Cybercrime**
 - **Creating National Incident Management Capabilities; and**
 - **Promoting a National Culture of Cybersecurity**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Evolution of Cybercrime

- **Cybercrime is:**
 - **Sophisticated**
 - **Financially Lucrative**
 - **International**
 - **Cybercrime operations move to countries lacking an appropriate legal structure**
 - **Using a distributed command structure capable of easily spreading to computers in multiple countries**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Evolution of Cybercrime

- **Cybercrime is:**
 - **Sophisticated**
 - **Financially Lucrative**
 - **International**
 - **Cybercrime operations move to countries lacking an appropriate legal structure**
 - **Using a distributed command structure capable of easily spreading to computers in multiple countries**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

What Kind of Cybercrime Law is Needed?

- **Cybercrime law is needed in each country, which contains:**
 - **uniform and flexible definitions of illegal activity**
 - **procedures to allow the detection of cybercrimes and capture/preservation of relevant evidence**
 - **method for effective international collaboration**

Convention on Cybercrime (Also known as the Budapest Convention on Cybercrime)

- **Opened for signature on Nov. 23, 2001**
- **Entered into force on Jan. 7, 2004**
- **Signed by 44 countries**
- **Ratified/acceded to by 23 countries
including Canada, Costa Rica, Japan,
Mexico, South Africa, and U.S.**

Convention on Cybercrime

(cont.)

- **The first international treaty focused on crimes committed on the Internet and using other computer networks**
- **Generally accepted as the international standard for cybercrime laws/legislation**
- **Aimed at fostering a common criminal policy against cybercrime, across multiple countries, and encouraging international co-operation against cybercrime**

Convention on Cybercrime

(cont.)

The Convention has three aims that are set forth in three chapters:

- **Harmonizing national substantive laws dealing with cybercrime**
- **Providing necessary power for the investigation and prosecution of cybercrime offenses**
- **Creating an effective means of international cooperation**

Convention on Cybercrime: Substantive Criminal Law Provisions

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense to:

- **Illegal access.** (Chap. II, Sect. 1, Art. 2)
Intentionally access the whole or part of a computer system without legal right to do so
- **Illegal Interception.** (Chap. II, Sect. 1, Art. 3)
Intentionally intercept without right non-public transmissions of data to, from, or within a computer system
- **Data Interference.** (Chap. II, Sect. 1, Art. 4)
Intentionally damage, delete, deteriorate, alter, or suppress computer data without right



ALLIANCE
LAW GROUP_{LLC}

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

- **System Interference.** (Chap. II, Section 1, Art. 5)
Intentionally seriously hinder without right the functioning of a computer system by inputting transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
- **Misuse of Devices.** (Chap. II, Sec. 1, Art. 6)
Intentionally and without right, produce, sell, procure for use, import, distribute, or otherwise make available:
 - a device designed or adapted for the purposes of committing any of the offenses specified in Articles 1 to 5 or



ALLIANCE
LAW GROUP_{LLC}

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

- a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed
- **Computer-related forgery.**
(Chap. II, Sec. 1, Art. 7).
Intentionally and without right, input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether the data is directly readable and intelligible

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

- **Computer-related fraud.**

(Chap. II, Sec. 1, Art. 8)

Intentionally and without right, and with the fraudulent intent of procuring without right an economic benefit for oneself or for another person, cause a loss of property to any other person by:

- **any input, alteration, deletion or suppression of computer data or**

- **any interference with the functioning of a computer system**



www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Child Pornography (Chap. II, Sec. 1, Art. 9)

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense with respect to child pornography to:

- Produce it for the purpose of distributing it through a computer system**
- Offer or make it available through a computer system**
- Distribute or transmit it through a computer system**
- Procure it through a computer system**


**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Child Pornography *(cont.)*

- **Possess it in a computer system or on a computer data storage medium**

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Infringement of copyright & related rights

Chap. II, Sec. 1, Art. 10

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense to violate the Agreement on Trade-Related Aspects of Intellectual Property Rights (“TRIPS”), the WIPO Copyright and Performances and Phonograms Treaties, and related international agreements (the Bern & Rome Conventions) where such acts “are committed willfully, on a commercial scale, and by means of a computer system.”

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Attempt & Aiding and Abetting

Chap. II, Sec. 1, Art. 11

The Convention requires parties to adopt domestic laws and other measures that will make it a criminal offense to intentionally aid, abet, or attempt, the commission of any of the offenses, established under Articles 2 - 10 of the Convention.



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Corporate Liability

Chap. II, Sec. 1, Art. 12

The Convention requires parties to adopt domestic laws and other measures to ensure that legal persons can be held liable in appropriate instances when actions prohibited by laws under the Convention are taken by natural persons on their behalf.



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: Substantive Criminal Law Provisions

(cont.)

Penalties

Chap. II, Sec. 1, Art. 13

The Convention requires parties to adopt domestic laws and other measures to ensure that violations by natural persons of offenses established in accordance with the Convention’s substantive provisions are punishable by “effective, proportionate, and dissuasive sanctions,” including imprisonment.

Similar requirements are imposed with respect to legal persons (i.e. corporations), except that imprisonment is not specified.

Convention on Cybercrime: Procedural Provisions

Section 2 of the Convention specifies procedural requirements to be applied to:

- **The criminal offenses established pursuant to the Convention**
- **Other criminal offenses committed by means of a computer system**
- **The collection of evidence in electronic form concerning a criminal offense**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Why Are Procedural Issues Important?

- **The Internet makes cybercrime activity possible anywhere in the world, directed at any area of the world**
- **Cybercriminals often mask their location and their activity by using “third party” computers that they control without the owner’s knowledge or consent**
- **Digital evidence is ephemeral and can quickly disappear or be erased. Thus, it is critical to detect and capture it very quickly.**

Convention on Cybercrime: Procedural Provisions

Parties must adopt domestic law and other provisions necessary to require:

- Expeditious preservation of data stored on a computer system**
- Submission of specified computer data under a person's control and subscriber information within the possession or control of a service provider**
- Search of a computer system and the data on it and seizure of relevant data**
- Collection or recording of real-time traffic data (including compelling a service provider to do so)**

Convention on Cybercrime: Procedural Provisions (*cont.*)

- **Collection or recording of real-time communications content (including compelling service providers to do so or to assist)**

Convention on Cybercrime: Jurisdictional Provisions

The Convention requires that parties adopt domestic law and other measures necessary to establish jurisdiction over any substantive offense under the Convention and that occurs in:

- The Party's territory**
- On board a ship flying the flag of the Party**
- On board an aircraft registered under the laws of that Party or**
- In a State where the offense was committed by a Party's nationals and is punishable by criminal law in that State or if the offense is committed by one of that Party's nationals in an area outside the territorial jurisdiction of any State**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Why is Jurisdiction Important?

- **Cybercriminals try to avoid detection and prosecution by operating outside of the territory that they are targeting.**
- **Thus, it is important that the targeted country have broad jurisdiction to pursue them.**
- **In order to do this effectively, international cooperation and coordination is critical.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation

Chapter III of the Convention establishes the general principle that parties shall cooperate with each other “to the widest extent possible” to conduct investigations or proceedings concerning criminal offenses related to computer systems and data and for the collection of evidence in electronic form of criminal offenses under laws established pursuant to the Convention.



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation *(cont.)*

Chapter III of the Convention also sets forth general principles on:

- **Extradition (i.e., the removal of a person from one country to another in order to be subject to prosecution for one of the criminal offenses established in accordance with the Convention) and**
- **Mutual assistance between parties**

Convention on Cybercrime: International Cooperation *(cont.)*

Chapter III of the Convention provides specific provisions on certain aspects of mutual assistance requests, where the data is within the territory of another party including:

- **Expedited preservation of stored computer data**
- **Expedited disclosure of traffic data**
- **Accessing stored computer data**
- **Real-time collection of traffic data**
- **Interception of communications content data**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

Convention on Cybercrime: International Cooperation *(cont.)*

Finally, Title 3 of Chapter III of the Convention specifies that each party shall designate a point of contact available on a 24 hour by 7 day a week basis to assist in investigations or proceedings concerning criminal offenses related to computer systems and data. Such assistance shall include facilitation or performance of the following functions:

- Technical assistance**
- Preservation of data**
- Collection of evidence**
- Coordination and communication on an expedited basis with another Party's designated contact**

Continuing Issues

- **Need for national cybercrime laws**
- **Need for increased international coordination and cooperation**
 - **For example, the ITU, through its Global Security Agenda (GSA), and the High-Level Experts Group (HLEG) operating as part of the GSA, is actively working to elaborate “strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.”**

New Types of Cybercrime or Misconduct

Identity Theft

- **The use of another person’s identity by which the perpetrator fraudulently obtains and uses that person’s identity**
- **The identification information can be obtained through various means, including “phishing” (providing a link to a fraudulent web site designed to collect personal information) and hacking (penetrating a computer database to obtain confidential identifying information).**

New Issues

Identity Theft (*cont.*)

- **An increasing problem:**
 - **In 2006, over 8 million Americans were victims of identity theft with an estimated cost of \$56 billion. The result is bad credit reports, inability to obtain credit cards and loans.**
 - **In the UK, the cost of identity theft was calculated at 1.3 billion British Pounds per year.**
 - **In Australia, estimates of the cost of identity theft range from \$1 billion to \$3 billion (U.S.) per year.**

New Issues

Identity Theft (*cont.*)

- **The Issue: How to Deal With It as a Legal Matter?**
 - **The Convention on Cybercrime protects against certain acts involved in identity theft for example, hacking into a computer system or database in order to obtain identify information. However, the information itself is not protected.**
 - **The U.S. protects the data itself (i.e. the personal information) but also the means that may be used (such as hacking) to obtain that information.**

New Issues

Identity Theft (*cont.*)

- **The Issue: How to Deal With It as a Legal Matter?**
 - **The Council of Europe is considering various means that would focus on the information itself, including closing gaps in the Cybercrime Convention and adopting specific national laws focusing on protection of the information**
 - **The U.S. is considering additional identity-theft protections (“The Identity Theft Enforcement and Restitution Act of 2007”). This would expand enforcement powers, expand crimes (e.g., cyber extortion) and allow victims of identity theft to sue for damages.**



**ALLIANCE
LAW GROUP_{LLC}**

www.AllianceLawGroup.com

New Issues

Cyber Bullying

- **What is it?**
 - **One definition is: “when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones.”**
 - **This became an issue in the U.S. when a 13-year old girl killed herself allegedly because of insulting Internet communication she received from someone she believed to be a 16-year old boy.**

New Issues

Cyber Bullying

- It later developed that the communication was, in fact, from a woman who was the mother of a former friend of the girl.
- Is cyber bullying criminal (*should it be*)?
 - Missouri declined to file criminal charges because its state law was not broad enough to cover the conduct
 - U.S. government charged that the mother's access to the social networking site violated terms of use and thus was unauthorized access in violation of law



ALLIANCE
LAW GROUP_{LLC}

www.AllianceLawGroup.com

On-Line Resources

- Council of Europe Convention on Cybercrime
(http://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp)
- ITU Global Security Agenda
<http://www.itu.int/osg/csd/cybersecurity/gca/>
- Regional Conference on Cybercrime
Activities & Recommendations
Casablanca, Morocco (June 18 - 20, 2007)
<http://www.arab-niaba.org/english/events/pubsbyactivity.asp?aid=122>

On-Line Resources (cont.)

- Regional Conference on Cybercrime
Cairo, Egypt (Nov. 26 - 27, 2007)
http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/6_Cybercrime/Cairo_DeclarationAgainstCC2007_EN.pdf
- ITU Regional Cybersecurity Forum 2008
Doha, Qatar (February 18 - 20, 2008)
<http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf>
- Computer Crime and Intellectual Property Section
U.S. Department of Justice
<http://www.cybercrime.gov/>

On-Line Resources *(cont.)*

- News summaries concerning cybercrime laws and regulation and links to many national laws concerning cybercrime
<http://www.cybercrimelaw.net/>

THANK YOU!



www.AllianceLawGroup.com

Craig J. Blakeley
Alliance Law Group LLC
7700 Leesburg Pike, Suite 410
Tysons Corner, VA 22043-2618
+1 703 848.8336
cblakeley@alliancelawgroup.com