

# **CYBERCRIME: THE U.S. APPROACH**

*The Middle East Cybercrime Forum  
Beirut, Lebanon  
February 23 - 24, 2006*

**Craig J. Blakeley**



# Cybercrime

- **What is it?**
- **Why should it be of concern to the Middle East?**
- **Are existing penal laws adequate to deal with it?  
(Is there something unique or different about  
cyber crime that requires new laws to specifically  
address these issues?)**
- **U.S. laws**
- **Lessons for the Middle East**

# 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**

# 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.**

# 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**
- **Denial of Service Attacks**

# **Cybercrime: Why Should It Be Of Concern in the Middle East?**

- **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, or causing a loss of confidence in the Internet**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# **Cybercrime: Why Should It Be Of Concern in the Middle East? *(cont.)***

- **Cyber-criminals will locate in areas with weak or no laws concerning cybercrime (e.g., the Middle East)**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Are Traditional Penal Laws 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 Law in the U.S.

- **U.S. has a “federal” system with both a national government and 50 state governments, as well as the District of Columbia**
- **Criminal law (in the noncomputer context) is a mixture of federal and state law**
- **The same is true with respect to laws addressing Cybercrime**

# **Cybercrime Law in the U.S.**

- **U.S. Computer Fraud and Abuse Act**
- **CAN-Spam Act**
- **Electronic Communications Privacy Act of 1986**
- **No Electronic Theft Act**
- **Identity Theft and Assumption Deterrence Act**
- **FTC Act**
- **State Laws**

# Federal Law

- **U.S. Computer Fraud and Abuse Act**

- **Addressed to Crimes Against Computers**

- **Applies to “protected computers”**

- **Computers used by financial institutions or the U.S. Government and**
- **Computers used in “interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States”**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Federal Law

- **U.S. Computer Fraud and Abuse Act (*cont.*)**

- **Prohibits:**

- **Intentionally accessing a computer without authorization to obtain information contained in a financial record of a financial institution or credited care company or contained in the file of a consumer reporting agency on a consumer; from any department or agency of the U.S. Government; or from any “protected computer” if the conduct involves interstate or foreign communication**
- **“Knowingly and with intent to defraud,” accessing a protected computer without authorization, and through such conduct furthering the intended fraud (unless the purpose of the fraud and what is obtained is**

# Federal Law

- **U.S. Computer Fraud and Abuse Act (*Prohibitions cont.*)**
  - only the use of the computer and the value of what is obtained is not more than \$5,000 in any one-year period)
  - Knowingly cause transmission of a program, information, code or command (*i.e., a virus or or other malware*) and, as a result, intentionally cause damage to a protected computer or intentionally access a protected computer and cause damage to it if such damage includes a loss by one or more persons aggregating at least \$5,000 in any one year, physical injury to any person, any threat to public health or safety (*or certain other specified harms*)

# Federal Law

- **U.S. Computer Fraud and Abuse Act (*Prohibitions cont.*)**
  - **Knowingly and with intent to defraud, traffic in any password or similar information through which a computer may be accessed without authorization if such trafficking affects interstate or foreign commerce or the computer is used by or for the U.S. Government**
  - **Transmit in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer with intent to extort from any person any money or other thing of value**
  - **Also prohibits accessing without authorization certain U.S. Government computers and obtaining certain “classified information”**

# Federal Law

- **U.S. Computer Fraud and Abuse Act**

- **Penalties**

- **Fines of up to \$250,000 and imprisonment of up to 20 years (up to a life term if death results)**
    - **Injured persons have a “private right of action” to bring lawsuits for damages and equitable relief (e.g, injunctions)**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Federal Law

- **CAN-Spam Act**

- **Approved in 2003; took effect on January 1, 2004**
- **Designed to prevent proposed California law from taking effect**
  - **Calif. Law would have required affirmative consumer consent -- “opt-in” -- prior to receiving Spam**
- **Permits sending of Spam to consumers unless they “opt out”**
- **Prohibits state laws dealing with Spam, except those that prohibit false or deceptive e-mail**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Federal Law

- **CAN-Spam Act; Specific Provisions**
  - Covers e-mail whose primary purpose is advertising or promoting a commercial product or service
  - E-mail that facilitates an agreed-upon transaction or updates a customer in an existing business relationship is not covered by the law (except with respect to accuracy of header information)

# Federal Law

- **CAN-Spam Act; Specific Provisions (*cont.*)**
  - All commercial e-mail and “transactional or relationship e-mail” must have accurate header information (“From,” “To,” and routing information)
  - Commercial e-mail must contain:
    - Accurate subject lines
    - Sender’s valid physical postal address
    - Identification as advertisement
    - Opt-out method (using e-mail address or other internet-based mechanism for recipients that must be valid for 30 days after the e-mail is sent; opt-out requests must be honored within 10 business days after receipt)

# Federal Law

- **CAN-Spam Act; Specific Provisions (*cont.*)**
  - **Other practices of commercial e-mailers are prohibited:**
    - **“Harvesting” e-mail addresses**
    - **Generating e-mail addresses using a “dictionary” attack**
    - **Using scripts other automated ways of registering for multiple e-mail or user accounts to send commercial e-mail**
    - **Relaying e-mails through a computer or network without permission**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Federal Law

- **CAN-Spam Act**

- **Penalties** (*apply both to those who actually send the offending e-mails and to those who hire them*)

- **“Routine Violations”** -- **Fines of up to \$11,000 (U.S.) per violation** (*ban of false or misleading header information, prohibition of deceptive subject lines, provision of required opt-out mechanism, identification of commercial e-mails as advertisements and inclusion of sender’s valid physical postal address*)

- **Additional fines are imposed upon those who use harvesting, “dictionary” attacks, automated scripts to send commercial e-mail, relay e-mails through a computer or network without permission**



# Federal Law

- CAN-Spam Act

- Penalties (*cont.*)

**More egregious violations -- Imprisonment of 3 - 5 years, fines, and forfeiture of an property acquired from the proceeds of such misconduct**  
*(using third party computers without authorization to send multiple commercial e-mail messages (i.e. spam), using computers to relay or retransmit multiple spam messages with the intent to deceive or mislead as to the origin of the messages, falsification of header information in multiple spam messages, falsification of the identity of the actual registrant for five or more e-mail accounts*



# Federal Law

- CAN-Spam Act

- Penalties (*cont.*)

- or two or more domain names and the use of such accounts or names to send multiple commercial e-mail messages, falsification of the identity of five or more IP addresses and the use of such addresses to send commercial e-mail messages)*



ALLIANCE  
LAW GROUP<sub>LLC</sub>

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Federal Law

- **CAN-Spam Act**

- **Enforceable by:**

- **U.S. Federal Trade Commission and Department of Justice (criminal provisions)**
    - **State attorneys general and other relevant state agencies (for citizens of their states)**
    - **Internet Service Providers**
    - **Important Exception: Not enforceable by individual consumers or businesses**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Other Relevant Federal Laws

- **Electronic Communications Privacy Act of 1986**
  - Prohibits the interception, disclosure, and use of certain wire, oral and electronic communications affecting interstate (i.e., between more than one state in the U.S.) or foreign commerce
  - Fines and/or prison terms of up to five years may be imposed

# Other Relevant Federal Laws

- **No Electronic Theft Act**

- **Makes it a federal crime to reproduce, distribute, or share copies of electronic copyrighted works such as songs, movies, games, or software programs, even if the person copying or distributing the material acts without commercial purpose and/or receives no private financial gain**
- **Penalties of up to 5 years in prison and \$250,000 (U.S.) in fines may be imposed**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# Other Relevant Federal Laws

- **Identity Theft and Assumption Deterrence Act**
  - **Makes it a federal crime to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law**
  - **Penalties of up to 5 years in prison may be imposed**

# Other Relevant Federal Laws

- **FTC Act**

- **Prohibits renders unfair or deceptive acts or practices in or affecting commerce (including such actions on the Internet)**
- **FTC is empowered to adopt rules prohibiting such acts and to issue “cease and desist” orders**
- **Civil penalties of up to \$10,000 per violation may be imposed for violations of FTC rules concerning unfair or deceptive practices or or of “cease and desist” orders forbidding such practices**

# State Laws

- **In addition to federal laws, individual states have adopted laws that cover cybercrime in a number of ways. These include:**
  - **General computer crime statutes**
  - **Computer tampering**
  - **Computer trespass**
  - **Unauthorized use of a computer**
  - **Interruption of computer services**
  - **Computer fraud**
  - **Spam-related offenses (e.g., falsification of routing and heading information)**
  - **Unlawful use of encryption**
  - **Cyberstalking**
  - **Offenses against computer users**
  - **Theft of confidential data from computer systems**

# State Law Examples

- **Virginia Computer Crimes Act**

- **Prohibits:**

- **Use of computer for identity theft, harassment, invasion of privacy, transmit spam with false or misleading electronic mail transmission information or routing information**
- **Without authorization, altering, disabling, or erasing computer data, using computer to cause physical injury**

- **Enforcement**

- **Provides for criminal penalties and also permits lawsuits for damages by aggrieved parties**

# State Law Examples

- **Virginia Computer Crimes Act (*cont.*)**
  - **Broad jurisdictional provision. Law defines using a computer or computer network within Virginia as conferring jurisdiction in Virginia. Given that the bulk of U.S. (and perhaps the world's) Internet traffic passes through Virginia, this gives Virginia broad authority.**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# State Law Examples

- **California Database Protection Act**
  - **Applies to any person, agency, or company doing business in California**
    - **NOTE: “Doing business” may mean as little as marketing to California residents or having a contract with a California company**
  - **Requires disclosure to California residents of any security breaches where unencrypted personal information about them has been disclosed.**



**ALLIANCE  
LAW GROUP<sub>LLC</sub>**

[www.AllianceLawGroup.com](http://www.AllianceLawGroup.com)

# **LESSONS FROM THE U.S. EXPERIENCE**

- **Specific laws are required to address misconduct that are unique to computers or the Internet**
- **Laws of national application are, by themselves, insufficient to deal with cybercrime, which is international in scope**
- **Laws of extraterritorial application and/or international cooperation are required to deal with threats from outside a specific country**

***THANK YOU!***



[www.AllianceLawGroup.com](http://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](mailto:cblakeley@alliancelawgroup.com)**