ELECTRONIC FRONTIER FOUNDATION eff.org

Computer Crimes: An American Case Study

Eddan Katz

International Affairs Director

Electronic Frontier Foundation

Thai Netizen Network Digital Rights Workshop

July 26, 2009

Cybercrime Legal Regime

- Child Pornography Statutes
- Computer Fraud and Abuse Act
- CAN-SPAM Act
- Criminal Copyright
- Anti-Circumvention Provisions
- Electronic Communications Privacy Act
- Identity Theft

Defining Computer Crime

- US Dep. of Justice: “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.”
  - Applying Criminal Laws to actions taken with a computer
    - crimes present primarily technical problems in prosecution
  - Criminal acts as the use of and access to a computer system not connected to taking money or tangible items from a 3rd person.
    - Unauthorized access to a computer
    - Unauthorized use of computer-processing services
    - Unauthorized tampering with data in a computer
    - Unauthorized taking (copying & reading) of information from a computer
    - Unauthorized acts that preclude access to a computer by other parties

Constitutional Issues

- First Amendment - Freedom of Speech
- Fourth Amendment - Search and Seizure
  - The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Free Speech Issues

- *Reno v. American Civil Liberties Union (ACLU)*
  - strict scrutiny for speech regulation Internet communications
  - struck down Communications Decency Act provisions prohibiting transmission of "indecent" and "patently offensive" as being constitutionally vague and overbroad
- CAN-SPAM Act
  - political and non-commercial speech
- Export Control Regulations
  - Code is Speech

Three Major Concepts

- Authorization
- Intent
- Expectation of Privacy

Unauthorized Access

- new criminal concept
  - define a computer system as a protected environment and make control of access to this environment a protected right
  - define severity in terms of amount taken
  - unclear in regards to intangible property

Authorization

- Interactive Communication on the Internet
- Security Research & Quality Assurance
- No “Obtaining Anything of Value”
- Fair Use
- Anti-Competitive Behavior

Intent

- Information Intermediaries
- to commit the act
- to commit the harm
- functionality of code

Computer as Subject of Crime

- Spam - unsolicited bulk email
- Viruses - modifies other computer programs
- Worms - viruses that self-replicate
- Trojan Horses - contain hidden malicious code
- Logic Bombs - activate at specific time
- Sniffers - network analyzers

Reasonable Expectation of Privacy

- public-private space distinction
- content of communications
- specificity of warrant

Cybercrime Convention & Intermediaries

- Art. 9 - “making available,” “distributing,” and “transmitting”
- Art. 11 - aiding and abetting commission of offenses
  - Explanatory Report Par. 119 - aided by another person *who also intends that the crime be committed*
  - no duty on an intermediary to monitor
- Art. 12 - acting under its authority
  - Par. 125 - customer, user. Not like an employee.

Computer Fraud and Abuse Act (CFAA)

- 1. Access computer files without authorization and to subsequently transmit classified government information if information can be used.
- 2. prohibits obtaining, without authorization, information from financial institutions, the United States, or private computers that are used in interstate commerce.
- 3. intentionally accessing US department or agency nonpublic computer without authorization
- 4. accessing a protected computer, without authorization, with the intent to defraud or obtain something of value

CFAA, continued

- 5. computer hacking
  - knowingly causing the transmission of a program, code, or command, that intentionally causes damage to a protected computer.
  - intentional access without authorization that results in damage but does not require intent
- 6. trafficking in passwords knowingly and with intent to defraud
- 7. illegal to transmit any threat to cause damage

Computer Fraud and Abuse Act Penalties

TABLE 1. SUMMARY OF CFAA PROVISIONS

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Compromising the Confidentiality of a Computer	(a)(2)	1 or 5
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Knowing Transmission and Intentional Damage	(a)(5)(A)(i)	10 (20 or life)
Intentional Access and Reckless Damage	(a)(5)(A)(ii)	5 (20)
Intentional Access and Damage	(a)(5)(A)(iii)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Threats to Damage Computer	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parenthesis.

Criminal Copyright

- No Electronic Theft (NET) Act (1998)
  - (i) existence of a valid copyright
  - (ii) that the defendant willfully
  - (iii) infringed
  - (iv) either (1) for commercial advantage or private financial gain
    - (2) by reproducing or distributing infringing copies with a retail value of over $1,000 over a 180-day period
    - by distributing a work being prepared for commercial distribution by making it available on a publicly-accessible network.

Digital Millennium Copyright Act (1998) §1201

- Act of Circumvention
  - to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.
- Circumvention Device Ban
  - No person may manufacture, import, offer to the public, provide, or otherwise traffic in a technology, product, service, or device that is used to circumvent such technological measures.
    - primarily designed or produced to circumvent
    - limited commercial use
    - marketed for use in circumventing

DMCA §1201 Exceptions

- non-profit library, archive, and educational institutions
- reverse engineering
- encryption research
- protection of minors
- personal privacy
- security testing

Electronic Communication Privacy Act (1986)

- updating existing federal prohibitions against intercepting wire and electronic communications
- curb hacking activities by fortifying privacy rights of computer users
- enabling law enforcement officers to employ electronic surveillance in the course of investigating crimes

Thank you.

- Eddan Katz
  - eddan@eff.org