Legal Issues in Cybercrime Cases: Unauthorized Access

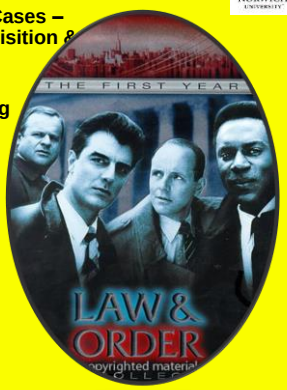
CJ341 – Cyberlaw & Cybercrime
Lecture #22

M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management

1

Introduction to §§22-25

- Legal Issues in Cybercrime Cases – review of laws affecting acquisition & presentation of electronic evidence at trial
- Serves as significant teaching tool to solidify knowledge of statues & procedure
- §§:
  - §22: Unauthorized Access
  - §23: Cyberfraud & Spam
  - §24: Intellectual Property
  - §25: Search & Seizure



2

Topics

- Defending Cases
  - Sixth Amendment to the US Constitution
- Defenses Defined
- Unauthorized Access
  - Computer Fraud & Abuse Act
- Electronic Communications Privacy Act
  - Wiretap Statute
  - Stored Wire & Electronic Communications Act

3

Defending Criminal Cases

- 6th Amendment of US Constitution:
  In all criminal prosecutions, the accused shall enjoy the right to a speedy & public trial, by an impartial jury of the State & district wherein the crime shall have been committed, which district shall have been previously ascertained by law, & to be informed of the nature & cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, & to have the Assistance of Counsel for his defence.
- Summary of Rights Guaranteed
  - Right to Speedy & Public trial
  - Right to Impartial jury
  - Right to be informed of charge
  - Right to confront witnesses
  - Right to put forth own witnesses
  - Right to Legal Counsel (next slide)

Think about which elements can be used by the defense & how to avoid being vulnerable to legitimate defense tactics.

4

Right to Legal Counsel

- Drafters of Constitution didn't explain scope of right
- Pre-1930s: two enacted statutory provisions suggested limitations on right to representation
- Post-1930s: evolution to absolute right to counsel
  - Gideon v. Wainwright – unanimous Supreme Court held "that in our adversary system of criminal justice, any person haled into court, who is too poor to hire a lawyer, cannot be assured a fair trial unless counsel is provided for him."
  - Right at federal & state levels
  - Recently defined as applicable to misdemeanors where imprisonment can be imposed
  - Also applies to felonies

5

Defense Counsel Responsibilities

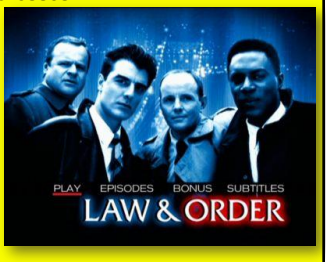
- "Effective Assistance of Counsel"
  - Explain criminal-justice process & stages
  - Advise defendant of his/her legal rights
- Check & balance to government power
  - Ensure no violation of accused's constitutional rights
  - E.g., role to see that government meets burden of proof
    - ✓Beyond reasonable doubt
    - ✓Otherwise risk of arbitrary punishment
    - ✓Rule of law depends on equitable application of documented & legal procedures

6

CJ341 Class Notes

Defense Counsel (cont'd)

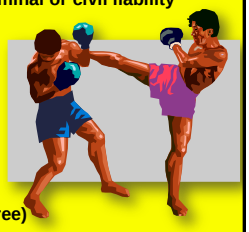
- Negotiation on behalf of defendant
- Handle matters from arraignment to sentencing
  - Inquiring/investigating into facts/evidence
  - Cross-examining of witnesses
  - Raising objections
    - ✓Improper evidence
    - ✓Improper process
    - ✓Improper questions
  - Preserving issues for appeal
  - Presenting legal defenses



7

Defenses

- Defenses may be alleged to avoid criminal or civil liability
  - Work to limit or excuse liability
- Types of criminal defenses
  - Innocence (i.e. didn't commit the crime)
  - Justification or excuse (i.e., did it, but…)
    - ✓e.g., self-defense, insanity
  - Procedural (e.g., evidence suppression / fruit of poisonous tree)
  - Innovative or creative (e.g., post-partum depression, involuntarily drugged, ate too many Twinkies™)
- Examples of civil defenses
  - Lack of jurisdiction
  - Failure to state a claim
  - Statute of Limitations



8

Unauthorized Access

- Types of Hackers/Crackers defined
  - Motivations
    - ✓Personal / intellectual interest / fun
    - ✓Profit
    - ✓Sabotage
    - ✓Destruction
    - ✓Political ideology
    - ✓Religious fervor
  - Criminal Intent – mens rea*

(Latin, "guilty mind")

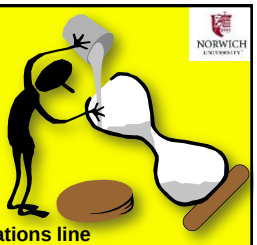
9

Computer Fraud & Abuse Act (CFAA, 18 USC §1030)

- Originally referred to "federal-interest computers"
- Defined as federal / state / municipal government equipment
- Or used by agencies or contractors for such governments

10

CFAA Revisions



- 1996: Congress expanded scope of CFAA
  - Replaced 'federal-interest computer" with "protected computer"
  - Includes every computer linked to interstate communications line
    - ✓Encompasses Internet
    - ✓Covers access to private computer
    - ✓Note: If private computer connected to Internet & access occurs in same state, CFAA still implicated
- 2001: U.S.A.P.A.T.R.I.O.T. expansion of definition
  - Includes access to foreign computers that affect US interstate commerce or communications

11

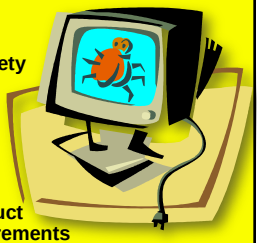
18 USC §1030(a)(5)

- Primary anti-hacking provision of CFAA
- Crime to intentionally damage a protected computer through transmission of a program, code or command
  - Damage: impairment to integrity or availability of data, program or information
- Must act without, or in excess of, authorization
- Must cause, or would have caused if successful, loss to 1 or more persons during a 1 year period of at least $5,000
  - Loss: any reasonable cost to any victim, including loss of revenue

12

18 USC §1030(a)(5) [cont'd]

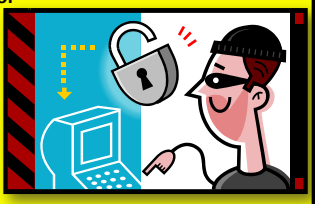
- May also be liable if causes damage that
  - Potentially or actually modified or impaired medical treatment
  - Causes physical injury
  - Threatens public health or safety
  - Damages a computer used by or for national security
- 1996: Amendments tried to limit available defenses
- 2001: USA PATRIOT Act tried to broaden scope of culpable conduct & eliminate selected intent requirements
  - Goal: easier prosecutions



13

18 USC §1030(a)(5) [cont'd]: INTENT

- If intent to access is found (even if no intent to damage) – can be convicted of misdemeanor
- I.e., no defense to CFAA charge to claim "I didn't mean to cause resulting damage" if intentionally accessed computer
- Before amendments: whether intent element went to access or resulting damage was ambiguous
  - U.S. v. Morris: Robert T. Morris* launched destructive program Nov 2, 1988, but didn't intend to cause damage, only wanted to show vulnerabilities;
  - Court convicted Morris of felony, concluding that "intent" element applied to access



*NOT JR!

14

18 USC §1030(a)(5) [cont'd]: LACK OF DAMAGE

- Section 1030(e)(8): damage = "any impairment to the integrity or availability of data, a program, a system, or information" that causes a loss of at least $5000 in a one-year period."
- 2001: loss defined to include any reasonable loss; e.g., damage assessment, repair, lost profit, among other losses
- Does damage caused rise to requisite level?

15

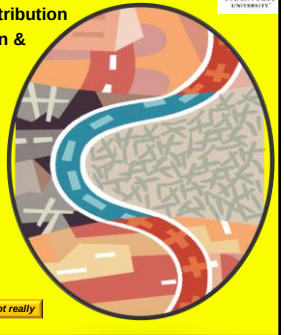
18 USC §1030(a)(5) [cont'd]: Penalties

- Federal Sentencing Guidelines: violation of 1030(a)(5) = 4-10 months sentence
- Increased penalty for knowingly or intentionally causing damage
  - 12-18 months sentence
  - 51-63 months sentence for disruption to critical infrastructure (next slide)
  - Prior conviction under 1030(a) or state offense involving unauthorized access

16

Critical Infrastructure

- Agriculture, food production & distribution
- Electricity generation, transmission & distribution
- Financial services
- Gas production, transport & distribution
- Heating
- Monty-Python skit suppliers*
- Oil & oil products production, transport & distribution
- Public health
- Security services
- Telecommunication
- Transportation systems



*OK, not really

See Moteff, J. & P. Parfomak (2004). "Critical Infrastructure and Key Assets: Definition and Identification." Congressional Research Service, Library of Congress. Order Code RL32631. < http://www.fas.org/sgp/crs/RL32631.pdf >

18 USC §1030(a)(5) [cont'd]: US v. Heim (2006)

- Oct. 2006: California defendant, Jay Heim (47 yrs old), sentenced in federal Court for violating §1030(a)(5), for recklessly damaging a protected computer
- Heim was founding partner & employee of Facility Automation Systems (FAS)
- Left company in March 2005
- In Jan 2006, used FAS' assigned username & password for its Internet domain & redirected all FAS Internet traffic, including e-mail to a server at his new employer
- He knew redirection of traffic would make Web site & e-mail services inaccessible
- Cost to FAS: productivity & service restoration >$6K
- Heim sentenced to 2 yrs probation + $500 fine & restitution to FAS ($6,050)

http://www.cybercrime.gov/heimSent.htm

18

18 USC §1030(a)(2)

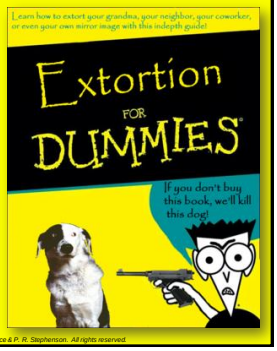
- Prohibits obtaining, without, or in excess of, authorization, information from a financial institution, the federal government, or a protected computer involved in interstate or foreign communication
  - "Reading"/viewing info suffices
  - Copying or alteration not required
- Penalties
  - Usually a misdemeanor: 0-6 months under sentencing guidelines (probation)
  - Felony if: in furtherance of commercial gain or other crime, or loss >$5,000
  - Up to 5 years prison

19

18 USC §1030(a)(7)

Define extortion

- Prohibits online extortion through use of protected computer
  - Conduct probably also triggers federal extortion-specific statute
- Felony
  - 27-33 months in prison
  - Increased penalty
    - ✓Depending on amount of money demanded or actual loss
    - ✓Damage to critical infrastructure or involving justice / security-related computer



20

21

Stored Wire & Electronic Communications Act (cont'd)

- Public provider can disclose info about users under certain conditions:
  - Consent of user
  - Necessary for provider to protect its own rights or property
  - Inadvertently-obtained info related to commission of crime
  - Reasonable belief of danger of death or serious injury
- Can also disclose transactional data
- Penalties
  - Fines, imprisonment < 1 year
  - Enhanced penalties for repeat offenders

22

18 USC §1030(a)(6)

- Prohibits trafficking in computer passwords used to access protected computer
  - Requires intent
    - ✓Knowingly
    - ✓Intent to defraud
- Possibly applicable in ID theft cases
- Penalties
  - 0-6 months jail
  - Increased sentence depending on loss

23

18 USC §1030(a)(4)

- Prohibits access with or without authority with intent to defraud or take anything of value (>$5,000)
- Defense:
  - Defendant can argue no value
- US v. Czubinski:
  - Defendant charged with 4 counts of fraud under 1030(a)(4) for unauthorized viewing of confidential taxpayer info;
  - Court found no violation, as viewing information does not equal taking something of value for statutory purposes
- But see US v. Ivanov: Court held defendant obtained something of value when obtained root access
- Penalties: 0-6 months, depending on loss & presence of aggravating factors

24

18 USC §1030(a)(3)

- Prohibits intentionally accessing a nonpublic computer of a US department or agency without authorization
- Penalties
  - 0-6 months,
  - More possible depending on loss & type of government computer
- Possible defenses
  - Lacked intent to access
  - Not US department or agency computer

25

18 USC §1030(a)(1)

- Prohibits knowing access of a computer, without authorization or in excess of authorization & subsequent transfer of classified government info
  - Info is protected if it could or has potential to injure US
  - Doesn't actually have to be used to injure the US
- Penalties
  - Depends on classification level of info involved & existence of any aggravating factors
  - 7-9 years if top secret info; less (4-5) if not

26

Wiretap Statute (18 USC §2511)

- Formulated 1968 & extended by ECPA 1986
- Prohibits interception & disclosure of wire, oral, or electronic communication* **Consent of one party sufficient*
  - Includes e-mail, voicemail, cell phones, satellite signals
  - Includes e-mail interception, tapping cell phones
    - ✓E.g., 2005: Paris Hilton's cell phone hacked**
  - Penalties
    - ✓Fine, 4-10 months sentence
    - ✓Increased penalty for commercial gain

** http://abcnews.go.com/Technology/WNT/story?id=545734&page=1

27

Wiretap Statute (cont'd)

- §2511 requires interception during transmission
  - Issue: determining "transit"
- US v. Councilman:
  - Defendant intercepted e-mails sent to amazon.com
  - Copied e-mails before they were received by amazon.com
  - Court dismissed indictment under Wiretap act,
    - ✓E-mails were in form of temporary storage
    - ✓As opposed to real-time interception

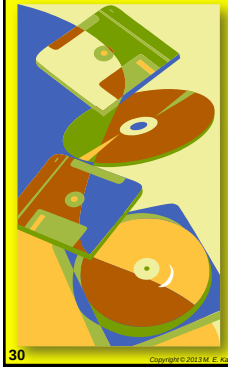
28

Electronic Communications Privacy Act (ECPA)

- 18 USC §2510-2521
- Review:
  - Enacted in 1986
  - Criminalizes unauthorized interception of electronic communications by private entities
  - Provides requirements for government access of electronic communications
  - Divided into 2 main chapters
    - ✓Wiretap statute
    - ✓Stored Wire & Electronic Communications & Transactional Records Act

29

Stored Wire & Electronic Communications Act



- §2701 prohibits access to electronic communications while in *storage*
- Exempts conduct that is authorized by
  - Entity providing the service or
  - By user (for own communications)
- E.g., *employer* who provides services to be used in employment is *not liable* for accessing employee communications

30