

# Cyber Security - the laws that protect your systems and govern incident response

Joel Michael Schwarz

Department of Justice

Computer Crime and Intellectual Property Section

Criminal Division

(202) 353-4253 / [Joel.Schwarz@usdoj.gov](mailto:Joel.Schwarz@usdoj.gov)

<http://www.cybercrime.gov>

# Today's goals:

1. An introduction to DOJ's Computer Crime & Intellectual Property Section
2. Applying the Computer Fraud and Abuse Act to Security Breaches of Your Systems (18 U.S.C. 1030)
3. Incident Response – Monitoring Communications and Traffic Data During an Incident
4. Disclosing Stored Communications and Documents (“ECPA”)

# 1. U.S. Department of Justice's Computer Crime & Intellectual Property Section ("CCIPS")

## CCIPS attorneys:

**approximately 40 attorneys**

**many have received degrees in computer science, engineering, or other technical fields (many are former prosecutors)**

**advise federal prosecutors and law enforcement agents**

**investigate and litigate cases**

**primary prosecutors in cyber-crime cases (ex. hacking)**

**assist AUSAs in real-world crime investigations (ex. securing content of E-mail account to trace a kidnapper)**

**offer comments/advise on legislation & policy pertaining to technical/legal issues, computer crime and CIP**

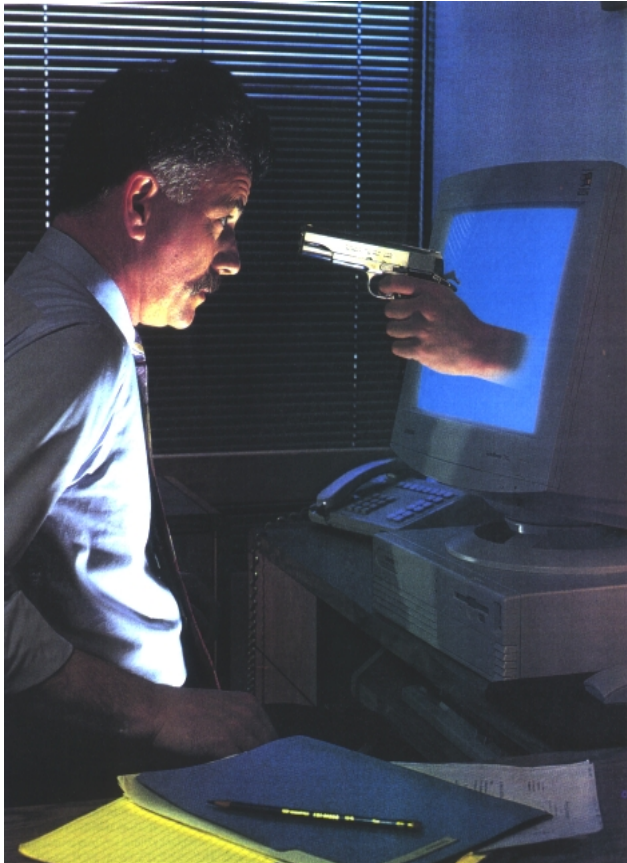
**train law enforcement on cyber-investigation and other technical issues**

# Today's goals:

1. An introduction to DOJ's Computer Crime & Intellectual Property Section
2. Applying the Computer Fraud and Abuse Act to Security Breaches of Your Systems (18 U.S.C. 1030)
3. Incident Response – Monitoring Communications and Traffic Data During an Incident
4. Disclosing Stored Communications and Documents (“ECPA”)

## 2. Applying the Computer Fraud and Abuse Act

“There’s a &#x26;#x24;%# intruder in my system!”



## 2a. The Frantic Call from the Head of IT Security Management

“The head of your IT Security Management received an anonymous call this morning from someone claiming to have broken into your system, copied 500 customer account numbers and passwords, and uploaded a virus to cover his tracks. He is now threatening to post the account numbers and passwords on the Internet, as well as the backdoor that he used to get into your system, unless you give him \$500,000.”

Subsequent investigation confirms this story

## 2b. What Laws Could He Have Broken?

### Major network crimes (18 USC)

- Confidentiality: 1030(a)(2)
- + Fraud: 1030(a)(4) and 1343
- Damage (data or systems): 1030(a)(5)
- Password trafficking: 1030(a)(6), 1029
- Extortion: 1030(a)(7), 871 et seq.
- Attempt: 1030(b) covers all of 1030(a)

## 2c. Obtains Information From Your System: 1030(a)(2)

- Intentionally accessing computer w/o or in excess of authorization
- And thereby obtaining information
  - (A) in a financial record or a credit report
  - (B) from a federal agency or
  - (C) from a “protected computer” if conduct involved an interstate communication
- Even if merely reading/browsing the info.  
United States v. Czubinski, 106 F.3d 1069 (1997)

## 2d. “Protected Computer”

Key term #1: “Protected computer”

[defined in 1030(e)(2)]

- (A) exclusively for use by financial institution or U.S. Govt. (or non-exclusive use, but conduct affects that use)
- (B) used in “Interstate or foreign commerce or communication” (even computer located outside U.S. that is used in a manner that affects commerce)

# 2e. Punishment for violating 1030(a)(2)

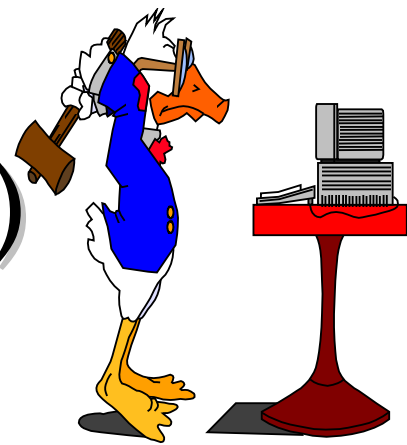
- Misdemeanor if no aggravating factors (and no previous offense)
- 5 year felony if:
  - for commercial gain
  - committed in furtherance of a criminal or tortious purpose
  - or value of information > \$5,000

## 2f. Fraud: 1030(a)(4)

- Prohibits knowingly and with intent to defraud:
    - accessing a protected computer (without, or in excess of, authorization), and because of such conduct:
      - furthers the intended fraud (must have another action in addition to the access itself – ex. copying information which he will ransom); and
      - obtains anything of value
- Object of fraud and thing of value obtained cannot be only the use of the computer itself, when that use is less than \$5000 in a one year period.
- Up to five year felony (unless previous offense)

# 2g. Damaging Computers

*Intentionally*: 1030(a)(5)(A)(i)



- Prohibits knowingly causing the transmission of a “program, information, code, or command” and as a result of such conduct, intentionally causing “damage” (without authorization) to a “protected computer”
- Applies to insiders or outsiders
- Applies to viruses, even w/o “access”
- Up to ten year felony (unless previous offense)

# 2h. “Damage” to a Protected Computer

Key term #2: “Damage”

- Defined as “any impairment to the integrity or availability of data, a program, a system, or information” causing:
  - a **loss** of at least \$5,000 within the period of a year; or
  - modification or impairment of medical records/data; or
  - physical injury to a person; or
  - threatening public health or safety; or
  - damaging system used in admin of justice, national security, or national defense

“Loss” includes cost of

## 2i. Homeland Security Act – Enhanced Penalties

1030(a)(5)(A)(i) - knowingly causing the transmission of a “program, information, code, or command” that results in serious injury or death

If the actor cause or attempts to cause serious bodily injury the penalty can be up to 20 years

If the actor cause or attempts to cause death the penalty can be up to life in prison

## 2j. Damaging Computers: 1030(a)(5)(A)(ii)

- Prohibits intentionally accessing a protected computer without authorization and “recklessly” causing damage
- Applies only to outsiders
- Up to five year felony (unless previous offense)

## Damaging Computers: 1030(a)(5)(A)(iii)

- computer without authorization and as a result, causing damage [i.e. negligently causing damage]
- Applies only to outsiders
- Up to one year (unless previous offense)

# 2k. Might Have A Violation Of 1030(a)(7)

## Threats to Damage a Computer

- Prohibits transmitting a threat to cause damage to a protected computer w/intent to extort any thing of value
- Up to 5 year felony (unless previous offenses)
- Query: Is threatening to post an unauthorized backdoor into your system a threat to “cause damage to a protected computer”?
- Consider – you might at least have: 18 USC 875(d) - Extortionate threats to injure the property of another

# 2l. Civil Restitution – 18 USC 1030(g)

Civil restitution if:

- (i) loss of at least \$5000 during a 1 year period (if civil action is based only upon loss under this section - limited to economic damages);
- (ii) modification or impairment of medical exam, diagnosis, treatment or care (potential or actual)
- (iii) physical injury
- (iv) threat to public health or safety
- (v) damage affecting government computer system (relating to admin of justice, national security or defense)

# Today's goals:

1. An introduction to DOJ's Computer Crime & Intellectual Property Section
2. Applying the Computer Fraud and Abuse Act to Security Breaches of Your Systems (18 U.S.C. 1030)
3. Incident Response – Monitoring Communications and Traffic Data During an Incident
4. Disclosing Stored Communications and Documents (“ECPA”)

# 3. Incident Response – Monitoring Communications During an Incident

## *Part I.*

*Contents of  
communications*

Wiretap Act  
(18 USC §§2510-22)

*Real-time  
interception*

## *Part II.*

*Metadata, logs, and  
other information*

Pen Register  
Statute  
(18 USC §§3121-27)

# 3a. Monitoring During an Incident; Law Enforcement's Role

**enforcement in conducting investigations, securing evidence and tracking criminals**

**These laws are set up using a type of hierarchy**

**requiring different types of approvals depending upon the intrusiveness of the information being sought**

**for example reading the content of someone's E-mail is more invasive than merely looking at the path the E-mail took to be delivered to that person**

**therefore securing the right to read E-mail content requires greater legal process, and a higher burden of proof on the part of a prosecutor, than securing t**

# 3b. Monitoring Communications During an Incident; The Tools

## Part I. Obtaining Content of Communications - Wiretap

ives reading the content of communications in real-time

**Phone** – install a device to listen in on the line

- Ex. listen in on a phone conversation planning a bank job

**Computer** – install a sniffer

- Ex. read E-mail and IM of a kidnapper to learn where he is at the moment and what his plans are

If law enforcement wishes to do this

Must secure a court order – this is a choice of last resort  
high burden of proof

# 3c. Monitoring Communications During an Incident; Generally

- Without a court order - cannot intercept contents unless an exception applies; it's a wiretap.
- Three key exceptions (no REP):
  - Provider Exception, 18 U.S.C. § 2511(2)(a)(i)
    - To protect the rights and property of the system under attack
  - Consent, 18 U.S.C. § 2511(2)(c)
    - Consent from one of the parties to the communication
  - Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i)
    - Trespasser – accesses computer w/o authorization
    - Can intercept information “transmitted to, through or from the protected computer”

# 3d. Monitoring Communications During an Incident; Provider Exception

- Allows system administrator to conduct reasonable monitoring:
  - To protect provider's "rights or property";
    - *Must be "substantial nexus" between the monitoring and the threat* – cannot indiscriminately monitor (w/o consent)
  - When done in normal course of employment, while engaged in any activity which is a "necessary incident to the rendition of . . . service" by provider
- Is a limited exception. Not a criminal investigator's privilege (cannot delegate to LE).
  - Provider may monitor the network to protect rights, and then disclose to law enforcement

# 3e. Monitoring Communications During an Incident; Consent Exception

- Banner the network
  - You have no reasonable expectation of privacy on this network.**
  - your activities are monitored;
  - results of monitoring may be disclosed to law enforcement; and
  - your continued use of the network consents to such monitoring and disclosure
- Obtain the written consent of authorized users.
  - through a click-through terms and conditions agreement or some type of written agreement (consult legal counsel)

# 3f. Monitoring Communications During an Incident; Trespasser Exception

- Allows law enforcement to intercept communications to or from “computer trespassers” 18 U.S.C. 2510(21)
  - Pre-PATRIOT ACT, system owners could monitor systems to “protect property,”
    - was unclear whether they could use/disclose information to LE
    - would be as counterintuitive as requiring a warrant to assist a burglary victim
  - PATRIOT Act created the trespasser exception
- Even if trespasser is using system as a pass-through to other downstream victims
- A “computer trespasser”
  - Is a person who accesses network “without authorization” and “thus has no reasonable expectation of privacy...”
  - Excludes a person known by the provider to have an existing contractual relationship with the provider for use of the system (even if contract is to access a different part of the system)

# 3g. Monitoring Communications During an Incident; Trespasser Exception (2)

- Conditions:
  - The provider must authorize the interception.
  - The person intercepting is acting under color of law.
  - The communications are relevant to an ongoing investigation and
  - No communications other than those sent to or received by the trespasser are intercepted.
- Provider immunity under 18 U.S.C. 2520(d)(1)
  - *Good-faith* reliance on court order, warrant, legislative or statutory authorization is a complete defense (civil and criminal)
- May combine this authority with other exceptions, such as consent.

# 3h. Tracing Traffic Data During an Incident; The Tools

## Part II. Tracing Source/Destination of Communications Pen/Trap

The Pen Register, Trap and Trace Statute governs real-time monitoring of traffic data (e.g. most e-mail header information, source and destination IP address and port)

Pen Register: outgoing connection data

Trap and Trace: incoming connection data

Does not include content of communications (e.g. e-mail subject line or content of a downloaded file).

If law enforcement wishes to get a court order – the burden of proof is lower than for reading content

# 3i. Tracing Traffic Data During an Incident; Header Information

Old: Pre-1986 there was arguably no process necessary to trace source and destination of phone calls

Passed statute in 1986 to require court process

Still only applied to telephones

Used terms like “number dialed” and “telephone line”

Internet uses IP Addresses and T1 lines

New (PATRIOT Act): Updated for the Internet – statute is technology neutral

Permits tracing of Internet communications

also expands protection of individual rights under the statute

explicitly requires a court order

criminal penalty for misuse

# 3j. Tracing Traffic Data During an Incident; Header Information (2)

- Akin to the Wiretap Act, Pen/Trap also grants providers exceptions to the general restrictions on intercepting header info.
- Exceptions:
  - Provider exception is broad:
    - can intercept if “relating to the “operation, maintenance, and testing,” of the service, or to protect the rights or property of the provider, or to protect users of that service from abuse of service or unlawful use of service
  - Consent of user
  - to record the fact that a wire or electronic communication was initiated or completed

# 3k. Tracing Traffic Data During an Incident

In emergency situations, law enforcement may intercept header information without a court order (emergency authorization lasts 48 hours - after which order is needed)

Emergencies under this provision include:

- an immediate danger of death or serious bodily injury;
- conspiratorial acts of organized crime;

New sections under Homeland Security Act:

- an immediate threat to a national security interest;
- an ongoing attack on a “protected computer” that constitutes a crime punishable by a term of imprisonment of more than a year

# Today's goals:

1. An introduction to DOJ's Computer Crime & Intellectual Property Section
2. Applying the Computer Fraud and Abuse Act to Security Breaches of Your Systems (18 U.S.C. 1030)
3. Incident Response – Monitoring Communications and Traffic Data During an Incident
4. **Disclosing Stored Communications and Documents (“ECPA”)**

# 4a. Disclosing Stored Communications and Documents

## Part III. Access To/Disclosure of Stored Communications

ECPA (18 U.S.C 2701-11) governs access to and disclosure of stored files.

Provider/Customer/Government roles

Cannot necessarily share stored files with others, including government

Three main categories are covered

Communications/content (e.g., e-mail, voicemail, other files)

Transactional Data (e.g., logs reflecting with whom users communicated)

Subscriber/Session Information

# 4b. Disclosing Stored Communications and Documents

- What stored communications records can network operators voluntarily disclose?
- First ask whether provider offers communications services to the public generally, or if it is a private provider
  - public provider - if services may be accessed by *any* user who complies with required procedure and pays any fees
  - If not a public provider – ECPA doesn't apply to preclude from voluntarily disclosing to law enforcement or others
- Examples:
  - AOL is a public provider,
  - A company that provides e-mail and voice mail services to employees is a private provider

# 4c. Disclosing Stored Communications and Documents

- When providing E-mail services, or other stored communication services (such as letting a student store files, web pages, etc.) what records can network operators voluntarily disclose?
- If you are a private provider (i.e. non-public) may voluntarily disclose all without violating ECPA (ECPA doesn't apply)
  - Content (e.g., the stored e-mail or voice mail)
  - Transactional data
  - User information
- Private providers may voluntarily disclose to government and non-government alike

# 4d. Disclosing Stored Communications and Documents

- A public provider must look to statutory exceptions before disclosing a user's content or non-content to government
- Public provider may voluntarily disclose the content of communications when:
  - Consent to do so exists (e.g., via banner or TOS)
  - Necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service
  - Contents inadvertently obtained & pertain to commission of a crime (to law enforcement)
  - Provider has “good faith” belief that an emergency involving immediate danger of death or serious physical injury requires disclosure (to governmental entity)

# 4e. Disclosing Stored Communications and Documents

*Provider has “good faith” belief that an emergency involving immediate danger of death or serious physical injury requires disclosure (may disclose to a governmental entity)*

previously, the standard was “reasonable” (as opposed to “good faith”), which potentially allowed courts to second guess an ISP’s reasonableness

previously an ISP could only disclose to law enforcement agencies; now they can disclose to any government entity

# 4f. Disclosing Stored Communications and Documents

- Public provider may voluntarily disclose non-content records concerning a customer or subscriber (i.e. transactional or subscriber information):
  - When consent to do so exists (e.g., via banner or TOS)
  - To protect provider's rights and property
  - To the government if provider reasonably believes an emergency involving immediate danger of death or serious physical injury requires disclosure
  - To any person other than a governmental entity

# 4g. Disclosing Stored Communications and Documents

What stored communications records can non-public providers be compelled to disclose to the government (and how can this be compelled)?

Content - unread E-mails (less than 180 days old)

search warrant

Content - unread E-mails (more than 180 days old)

subpoena (with notice to subscriber)

Content - read E-mails and other stored files

subpoena (ECPA doesn't apply)

# 4h. Disclosing Stored Communications and Documents

What stored communications records can network operators be compelled to disclose to the government - continued?

Transactional records

court order

Subscriber information

subpoena

NOTE: The process indicated in each of the above cases is the simplest form of process that may be used (ex. where a subpoena is required, a court order, a process with more procedural protections, will also satisfy

# 4i. Disclosing Stored Communications and Documents

## Immunity

A provider's good faith on legal process and statutory authorization in preserving and/or disclosing information confers complete immunity to any civil or criminal action against the provider.

# THE END



[joel.schwarz@usdoj.gov](mailto:joel.schwarz@usdoj.gov)