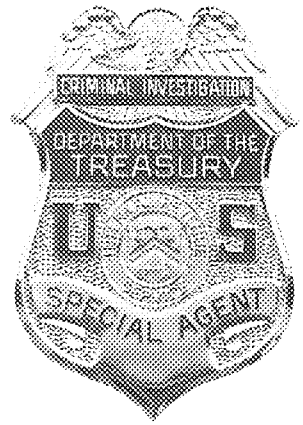
Internet Surveillance & Tracking Electronic Data

CPE 2008



CI Mission

Criminal Investigation serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.

Objectives

- List investigative techniques used in Internet investigations.
- Present an overview of the Patriot Act and the Electronic Communications Privacy Act (ECPA) of 1986.

Objectives

- Recognize classes of information under ECPA.
- Describe the judicial process for obtaining stored communications.
- Review the Online Investigative Principles.

Introduction

- In the last decade, computers and the Internet have entered the mainstream of American life. Millions of Americans spend several hours every day in front of computers, where they send and receive e-mail, surf the web, maintain databases, and participate in other online activities.

CI Search Warrant

- “[Target] is a ‘Cyber organization’ revolving around a web site. It has no physical address; its principals operate and conduct business over the Internet using laptop computers.”

Internet Investigations and Electronic Surveillance

- Tools and techniques to gather information about someone's Internet usage that has evidentiary value.
- Requires early CIS participation.

Investigative Methods and Early Involvement of CIS

- Install wiretaps and pen/traps.
- Trace machines to physical location.
- Identify owners of web sites.
- Preserve and analyze evidence.
- Reporting of evidence.

The USA PATRIOT Act

- The Patriot Act clarified and updated the Electronic Communications Privacy Act (ECPA) in light of modern technologies, and eased restrictions on law enforcement access to stored electronic communications.

Electronic Communications Privacy Act (ECPA) of 1986

- Overview of ECPA.
- Stored electronic communications.
- Classes of information.
- Judicial process.

Electronic Communications Privacy Act (ECPA) of 1986

- ECPA regulates how the Government can obtain stored account information from network service providers such as Internet Service Providers (ISPs).

Electronic Communications Privacy Act (ECPA) of 1986

- Whenever agents or prosecutors seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with ECPA.

Electronic Communications Privacy Act (ECPA) of 1986

- Extends Government restrictions on telephone wiretaps to include electronic transmissions from computers.
- Prevents unauthorized Government access to private electronic communications.

Obtaining Stored Electronic Communications

- 18 USC § 2703 specifies the methods to obtain access to stored electronic communications.
- 18 USC § 2703 prohibits service providers from voluntary disclosures.
- Mandates use of a search warrant, court order, or subpoena.

Classes of Information Pursuant to 18 USC § 2703

- Unopened e-mail.
- Records stored with a remote computing service in off-site archives.
- Basic subscriber information (such as - name, address, and telephone).
- Internet Protocol (IP) address.

Classes of Information Pursuant to 18 USC § 2703

- Length of service.
- Type of service.
- Transactional information.

Judicial Process for Obtaining Stored Communications

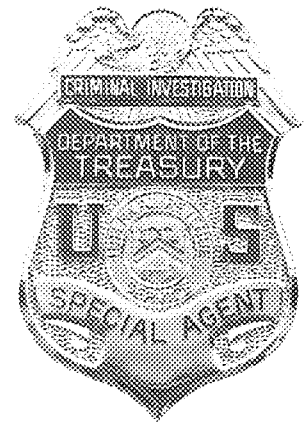
- Search Warrant for unopened e-mail stored for 180 days or less.
- For opened e-mail or e-mail stored for more than 180 days, a § 2703(d) court order, grand jury subpoena, or administrative summons is needed.

	Voluntary Disclosure Allowed?		Mechanisms to Compel Disclosure	
	Public Provider	**Non-Public Provider**	**Public Provider**	**Non-Public Provider**
Basic subscriber, session, and billing information	Not to government, unless 2702(c) exception applies [2702(a)(3)]	Yes [2702(a)(3)]	Subpoena; 2703(d) order; or search warrant [2703(c)(2)]	Subpoena; 2703(d) order; or search warrant [2703(c)(2)]
Other transactional and account records	Not to government, unless 2702(c) exception applies [2702(a)(3)]	Yes [2702(a)(3)]	2703(d) order or search warrant [2703(c)(1)]	2703(d) order or search warrant [2703(c)(1)]
Accessed communications (opened e-mail and voice mail) left with provider and other stored files	No, unless 2702(b) exception applies [2702(a)(2)]	Yes [2702(a)(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [2703(b)]	Subpoena; ECPA doesn't apply [2711(2)]
Unretrieved communication, including e-mail and voice mail (in electronic storage more than 180 days)	No, unless 2702(b) exception applies [2702(a)(1)]	Yes [2702(a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [2703(a,b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [2703(a,b)]
Unretrieved communication, including e-mail and voice mail (in electronic storage 180 days or less)	No, unless 2702(b) exception applies [2702(a)(1)]	Yes [2702(a)(1)]	Search warrant [2703(a)]	Search warrant [2703(a)]

Electronic Surveillance in Communications Networks

Wiretaps

Pen/Traps



"Real Time" Electronic Surveillance

- Wiretap statute, 18 USC §§ 2510-2522, generally known as "Title III".
- Pen Registers and Trap and Trace Devices, 18 USC §§ 3121-3127.

Non-Consensual Monitoring

- 18 USC § 2510 governs the “real time” interception of wire, oral, and electronic communications.
- 18 USC § 2516(3) authorizes the “real time” interception of electronic communications.

The "real time" … transmission of electronic mail, computer-to-computer transmissions, facsimile transmissions, and private video transmissions (but not video surveillance) are all covered by the wiretap statute.

Pen Registers & Trap and Trace Device Orders

- The USA PATRIOT Act amended 18 USC §§ 3121, 3123, 3124, and 3127.
- Authorizes use of pen register and trap and trace device orders to trace communications on the Internet and other computer networks.

Pen/Trap Device Orders

- Easy to obtain.
- Internet equivalent of mail cover.
- Requires authorization and approval from SAC on Form 9170.
- Requires CIS and AUSA involvement.

Pen/Trap Device Order Requirements

- AUSA is a “Government attorney.”
- Information likely to be obtained is relevant to an ongoing investigation.
- Electronic communications have been or continue to be used to further the offense under investigation.

Preservation of Evidence and Preventing Disclosure

- ECPA contains two provisions to aid law enforcement officials when working with ISPs.
- Two provisions include:
  - Preservation of Evidence
  - Orders Not to Disclose

ISP Preservation Letters

- Pursuant to 18 USC § 2703(f), Internet Service Providers (ISPs) will preserve information related to a subscriber or customer for 90 days, which may be extended by a second request for an additional 90 days.

Orders Not to Disclose

- Pursuant to 18 USC § 2705(b), agents can apply for a court order directing network service providers not to disclose the existence of compelled process whenever the Government itself has no legal duty to notify the customer of the process.

Online Principles for Federal Criminal Investigations

- Developed by inter-agency working group.
- Adopted by AG on 11/22/99, and Under Secretary for Enforcement at Treasury.
- Also in use at DoD, USPS, and IG offices.

Online Principles

- Static sources.
- User/network identifying information.
- Acquiring “real time” communications.
- Restricted sources.
- Communicating online.
- Undercover operations.

Online Principles

- Online undercover facilities.
- Appropriating identity with consent.
- Appropriating identity without consent.
- Off-duty use of the Internet.
- International considerations.

Summary

- The Internet provides a wealth of information that may have relevance to CI investigations.
- Internet communications and/or transactions may be important evidence to investigators.

- There are many tools which exist to help criminal investigators gather evidence related to the subjects' presence on the Internet.
- "Real time" intercepts is another investigative approach to consider.

- Pen registers and trap and trace devices may be appropriate investigative steps.
- Generally, the policies that govern investigations in the physical world also apply to cyberspace.