



U.S. Department of Justice

Civil Division

---

Washington, DC 20530

May 31, 2012

Ginger McCall, Esq.  
Marc Rotenberg, Esq.  
John Verdi, Esq.  
Electronic Privacy Information Center (EPIC)  
1718 Connecticut Ave NW  
Suite 200  
Washington, DC 20009

Re: **EPIC v. DHS**  
Civil Action #: 11-cv-02261 (JDB)

Dear Ms. McCall:

This is the third interim response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated April 12, 2011. Enclosed please find 213 pages of responsive documents, of which 56 pages are litigation materials relating to a relevant FOIA request made by the Electronic Frontier Foundation. These documents are from the United States Secret Service.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Jean-Michel Voltaire  
Trial Attorney  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
20 Massachusetts Avenue, NW  
Washington, DC 20530  
Tel.: 202-616-8211  
Fax: 202-616-8460  
Email: [jean.michel.voltaire@usdoj.gov](mailto:jean.michel.voltaire@usdoj.gov)

Enclosure(s):

cc: Donna Lewis  
DHS Attorney Advisor

# INTERNET USE POLICY

## General Information

### Purpose

This directive defines the responsibilities of Secret Service employees with respect to the appropriate use of the Internet and the services it provides.

### Scope

This directive applies to all Secret Service facilities and computer systems, regardless of location; and to all Secret Service personnel, including contract personnel employed by the Secret Service.

### Definition of Terms

**Firewall** - A combination of computer hardware and software that screens incoming data in order to guard against unauthorized system intrusion.

**Internet** - The Internet, or 'Nat,' is a public global network. Originally developed to link computer systems within the Department of Defense in the 1970s, the system was later expanded by the National Science Foundation to include colleges, research institutions and other U.S. Government agencies. In 1991, the development of the World Wide Web made the Internet easily accessible to the general public. Today, the Internet is a broad collection of networks mostly run by large telecommunications companies.

**Internet Service Provider (ISP)** - A vendor who provides direct access to the Internet, usually for a fee. An ISP normally provides its users a Web Browser and an e-mail account.

**Secret Service Computers** - For the purposes of this Directive, a Secret Service computer is defined as any computer owned or leased by the Secret Service (regardless of location), or any other computer being used for Secret Service business.

**Stand Alone Computer** - A computer that is not connected to any Secret Service information system and which would not require the transference of data from this computer to other Secret Service computers. For Internet use, the stand alone computer's data storage devices must be devoid of Secret Service data.

**Web Browser** - A Web browser/browser is a software tool used to locate and view data in a standardized graphical format on the WWW (e.g., Netscape Navigator).

**World Wide Web (WWW)** -The WWW or 'Web' is a portion of the information available on the Internet and consists of an electronic collection of documents stored on computers worldwide. The Web is noted for its graphics (photos, colors, etc.) and hyperlinks (allow users to jump quickly from one document to another).

## **Responsibilities**

**OFFICE OF PROTECTIVE RESEARCH** - Information Resources Management Division (IRM) - IRM controls connections to the Internet, and manages all services associated with the Internet.

**ASSISTANT DIRECTORS/CHIEF COUNSEL** - Assistant Directors or the Chief Counsel has ultimate authority to grant or deny employee access to the Internet.

**ASSISTANT DIRECTOR (INV, OPR)** - The appropriate Assistant Director (INV, OPR) will review and approve on a case by case basis all requests for Internet access/use to support ongoing investigations.

**OFFICE SUPERVISORS** - Office supervisors may limit or revoke the privilege for their employees to use Secret Service equipment to access the Internet for personal non-government usage.

**OFFICE SECURITY REPRESENTATIVE (OSR)** - The OSRs within each office are responsible for coordinating computer security issues with IRM Information Security (INFOSEC) personnel. OSRs are responsible for installing and updating anti-virus software on all computers connected to the Internet.

## **Authorization**

All Secret Service employees have access to the Internet through the Secret Service Network.

## **Internet Connectivity**

The Secret Service Network is equipped with safeguards, such as firewalls and intrusion detection systems, to minimize the possibility of computer virus exposure or intrusion by unauthorized personnel. Internet connectivity must be achieved via the Secret Service Network, unless specifically authorized in accordance with the Investigative Use section of this policy.

The Information Resources Management Division (IRM) controls the connections to the Internet. It is the only entity which may connect (or direct the connection of) Secret Service equipment to the Internet service. Only IRM approved "connectivity" software may be utilized.

Anti-virus software must be installed, updated and activated in any computer connected to the Internet, in accordance with policy in this manual regarding Baseline Security Controls for Personal Computer Virus Protection.

## Personal and Inappropriate Uses

Secret Service employees are permitted limited use of Secret Service equipment to access the Internet for personal needs.

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate.

Employees are expected to refer to directive Human Resources and Training Manual section PER-05(10), "Use of Government Systems," for information regarding personal use, no right to privacy, privilege, employee non-work time, inappropriate personal uses, and sanctions for misuse.

## Investigative Use

Criminal investigations that involve Internet technology currently fall into two broad categories:

- Threats against Secret Service protectees.
- Violations of Title 18 USC Section 1030 (Fraud and Related Activity in Connection with Computers), and related statutes. (See "section CFI-03, Computer Fraud Investigations Manual.")

Requests for Internet access/use to support ongoing investigations will be reviewed by the appropriate Assistant Director (INV, OPR), and approved on a case by case basis.

Personnel utilizing the Internet for investigative purposes are reminded that the access of an Internet site leaves an "electronic footprint," which can generally be used to identify the Internet address of the entity accessing the site. Therefore, all Internet accesses for investigative use will utilize 'stand-alone' computers that use anonymous accounts from an ISP.

The Electronic Crimes Special Agent Program (ECSAP) in Financial Crimes Division is available to assist field offices with their Internet investigations, as well as the seizure and forensic processing of computers encountered during investigations.

Many law enforcement organizations have established Home Pages, which allow for the exchange of investigative information via Internet e-mail. Internet e-mail is not secure. Due to the possibility of interception, sensitive investigative information or data should not be transmitted via Internet e-mail.

## Disclosure

Executive Branch employees do not have a right or expectation of privacy while using any government office equipment at any time, including accessing the Internet, using e-mail, or for limited personal use. To the extent that employees wish that their private activities remain private, they should avoid using an Agency's office equipment, such as their computer, the Internet, or e-mail "for personal use." By using government office equipment, executive branch employees imply their consent to disclosing the contents of any encrypted files.

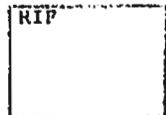
By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet, using e-mail, or for limited personal use. Any use of government communications resources is made with the understanding that such use is generally not secure and is not anonymous.

All e-mail messages (and other electronic database information) as defined in Federal Law, are government records. Electronic communications may be disclosed within an Agency to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access any electronic communications for work-related purposes. Electronic communications may only be disclosed externally in accordance with applicable law or regulations.

# USSS RECORDS DISPOSITION SCHEDULES ASSOCIATED WITH PROTECTIVE RESEARCH

This section includes the following disposition schedules:

- Appendix 1 Records Disposition Schedule for the Protective Intelligence and Assessment Division
- Appendix 2 Records Disposition Schedule for Land Mobile Radio (LMR) Transmissions Recording(s)



## Appendix 1: Records Disposition Schedule for the Protective Intelligence and Assessment Division

This schedule covers the records for the Protective Intelligence and Assessment Division maintained at the Service's Headquarters and the duplicate files maintained in the field.

### Protective Intelligence Case Files

#### ITEM NO.

##### 1. Criminal and Non-Criminal

Intelligence investigations of persons, groups or organizations that involve, or could involve, the use of threats, force, or violence to attempt assassination or otherwise harm protectees. Contains original investigative reports received from field offices of the Secret Service, correspondence with law enforcement and intelligence agencies. Includes photos, handwriting, personal history, statements of suspects, court documents, reports, completed forms, teletypes, and similar documents.

##### a. Sample Case Files Selected for Permanent Preservation

Unique or significant case files selected by Secret Service management for permanent preservation because of potential historical or archival value. Following are some examples of general criteria that will be used in selecting and earmarking such files for eventual offering to the National Archives:

- (1) The case established a precedent for significantly changing Secret Service policy or procedure.
- (2) The case was the subject of extensive litigation.
- (3) The case received widespread attention from the news media.
- (4) The case was reviewed at length in the publication of the agency such as the Annual Report to Congress of the Secretary of the Treasury.

##### Authorized Disposition:

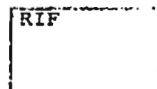
Permanent. Offer to the National Archives 20 years from the date of closing of the case.  
(NC1-87-88-1)

##### b. All Other Case Files

Judicial Cases.

##### Authorized Disposition:

Destroy 20 years from date of last action. (NC-1-87-76-3 #32)



**Non-Judicial Cases**

**Authorized Disposition:**

Destroy 5 years after case becomes inactive. (NC-1-87-76-3 #34)

Case files containing electronic surveillance records.

**Authorized Disposition:**

Destroy a minimum of 10 years after case is closed. (NC-1-87-76-3 #30, #31)

Field Office judicial and non-judicial cases.

**Authorized Disposition:**

Destroy 30 days from closing date of case. At discretion of SAIC files may be retained two years then destroyed. (NC-1-87-76-3 #33, #35).

Cases made for other districts.

**Authorized Disposition:**

Destroy 30 days from closing date. (NC-1-87-76-3 #28D)

PICS Computer file containing descriptive information of the subject and synopsis of the case.

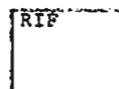
**Authorized Disposition:**

Delete record for each case three years following destruction of related paper case file. (NC-1-87-88-1)

**Secret Service Restriction for Access to Permanent Records.** Documents less than 50 years old will be made available only to authorized representatives of Government as a result of a written request and as authorized by the Assistant Director, Office of Protective Research, U. S. Secret Service. Such documents may not otherwise be published or Specified by the Director, U.S. Secret Service.

**2. Protective Intelligence Administrative Files**

**Protective Intelligence - General Files.** Documentation of administrative actions involving all phases of protective intelligence work such as mail consents, press index, intelligence reports received from other agencies for which no action is taken by the receiving office, internal protective intelligence investigative procedures, name check reports and similar records which clearly do not fit under item 1 and are not specified elsewhere. Consists of carbon copies as well as original materials.





**Protective Intelligence and Assessment Division**

**Authorized Disposition:**

Review and purge when SAIC determines material is no longer needed for administrative purposes.  
(N1-87-88-1)

Field Office

**Authorized Disposition:**

Cut off at the end of the month. Destroy 30 days after cut off. At the discretion of the SAIC, files may be retained two years, then destroyed. (N1-87-88-1)

3. **Protective Intelligence Summary File.** Contains internal teletypes providing summary information for particular intelligence situations.

Protective Intelligence and Assessment Division

**Authorized Disposition:**

Destroy After 10 years old. (N1-87-88-1)

Field Office

**Authorized Disposition:**

Cut off at the end of the calendar year then destroy. (N1-87-88-1)

4. **Protective Intelligence Research Files.** Consists of internal and external studies, proposals, and contracts pertaining to behavioral sciences research on assessments of dangerous prediction of violence and development of research models relating to the agency protective function. Reports are prepared by agency staff or by private organizations or individuals under contract to Secret Service. Reports are sensitive, some classified.

Research conducted directly by Secret Service.

**Authorized Disposition:**

Permanent. Transfer to Secret Service storage area five years after completion of research. When 20 years old, transfer to permanent custody of National Archives. (N1-87-88-1)

Research conducted by outside contractors.

**Destruction Not Authorized**

5. **Protective Intelligence Research Correspondence.** Files dealing with the administrative aspects of research. Documentation pertains to awarding of contracts, procurement of services, supplies, and professional issues related to research.



Research conducted directly by Secret Service.

**Authorized Disposition:**

Permanent. Transfer to Secret Service storage area five years after completion of research. When 20 years old, transfer to permanent custody of National Archives. (N1-87-88-1)

Research conducted by outside contractors.

**Destruction Not Authorized**

6. **Protective Intelligence and Assessment Division's Trip Files**

Contains internal reports pertaining to each trip/visit for each person protected by the Secret Service. Reports contain sensitive, some classified, operational and Intelligence Information such as notification teletypes to field offices, advance survey reports, instructions to agents, preliminary, interim and final intelligence reports. May include anonymous or vague allegations or threat information that warrant making inquiry but not of such a nature to justify case investigation. May also include intelligence data which may prove useful in future trips.

Trip files for domestic travel no longer needed for intelligence purposes.

**Authorized Disposition:**

Destroy when five years old. (N1-87-88-2)

Trip files for foreign travel no longer needed for intelligence purposes.

**Authorized Disposition:**

Destroy when 10 years old. (N1-87-88-2)

Trip files having long-term intelligence value.

**Authorized Disposition:**

Destroy when no longer needed for administrative purposes. (N1-87-88-2)

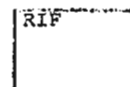
Field Office files.

**Authorized Disposition:**

Cut off at the end of each calendar year. Destroy when no longer needed for administrative and/or reference use, not to exceed five years. (N1-87-88-2)

7. **Freedom of Information Request/Appeal**

Electronic records and files that are the object of a request/appeal under the Freedom of Information Act (FOIA).



**Authorized Disposition:**

Maintain for six years from the date of release/denial of information. (GRS 14)

**Non-FOIA Lawsuits/Appeals**

All physical files and/or electronic records which are the object of a non-FOIA lawsuit/appeal naming the Secret Service as a defendant.

**Authorized Disposition:**

Maintain for six years from the date of completion of the legal process. (GRS 14)



## Appendix 2: Records Disposition Schedule for Land Mobile Radio (LMR) Transmissions Recording(s)

This schedule covers Land Mobile Radio (LMR) transmissions recordings of routine protective radio transmissions over multiple frequencies between the Command Post and agents, and support services such as local police during Presidential and Vice Presidential trips.

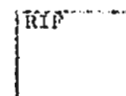
Item No.	Description of Record	Authorized Disposition
----------	-----------------------	------------------------

- |    |  |  |
|----|--|--|
| 1. | <p><b>Land Mobile Radio (LMR) Voice Transmission Recordings.</b> Recordings of routine protective radio transmissions over multiple frequencies between the Command Post and agents and support services such as local police during Presidential and Vice-Presidential trips. Media used to record these transmissions may be optical disk hard drives or equivalent hard drive technology, standard cassette tapes, magnetic tapes, compact disc (CDs), digital video disks (DVD) or other disposable electronic media. The Office of Protective Research, Information Resources Management Division (IRM), is responsible for the receipt of radio transmission data via the White House Communications Agency (WHCA) and/or the Communications Management and Control Activity (CMCA) under provisions of Public Law 94-524. The initial recording of radio transmissions by IRM is considered the official record copy.</p> | <p><b>TEMPORARY</b><br/>IRM will retain original transmission (official record copy) data recordings for 30 days; destroy by burning or by overwriting the storage media on the 31<sup>st</sup> day after the date of the recording. However, when a recording is affected by a particular case, significant event, pending or current litigation, or special requests, the recording should be disposed of in accordance with appropriate authorization.<br/>(N1-87-06-1)</p> |
|----|--|--|

**Note:** If a request is made for a copy of the digital file within the 30-day cycle, the following process will take place. If legally acceptable, an IRM technician will run a digital signature hashing program against each requested file. The copied file and documentation concerning the hash comparison will be stored in IRM in compliance with legal and MNO policies. This procedure safeguards against tampering with these recordings.

RIF

Item No.	Description of Record	Authorized Disposition
a.	<b>Unusual Incidents/Significant Events - Recordings related to significant events, which occurred in the course of protection travel.</b>	<b>PERMANENT</b> Retain as permanent and transfer to the National Archives and Records Administration with files according to applicable disposition instructions. (N1-87-06-1)
b.	<b>Pending or Current Litigation - Recordings affected by pending or current litigation.</b>	<b>TEMPORARY</b> Retain until litigation is resolved. (N1-87-06-1)
c.	<b>Special Requests - Recordings requested by the President, Congress, National Archives and Records Administration, or similar authority, and until otherwise directed.</b>	<b>TEMPORARY</b> Destroy when no longer needed for agency business. (N1-87-06-1)
d.	<b>Case Files - Recordings related to a case.</b>	<b>TEMPORARY</b> Retain according to the appropriate disposition authorization of that case. (N1-87-06-1)
e.	<b>All Other Offices - Requested copies of recordings. The business owner will notify IRM when recordings are affected by a particular case, significant event, pending or current litigation, and special requests.</b>	<b>TEMPORARY</b> IRM will retain official record copy of recordings. Destroy recordings 30 days from the date the transmission was originally recorded. On the 31 <sup>st</sup> day after the data was recorded, destroy by burning. However, when recordings are affected by a particular case, significant event, pending or current litigation, or special requests, the recordings should be disposed of in accordance with appropriate authorization. (N1-87-06-1)



United States Secret Service  
Directives System

Manual : Interception  
RO : ISD

Section : Chapter 1  
Date : 03/22/2006



---

**Subject:** Introduction

---

**To:** All Supervisors and All Manual Holders of the Interception and Recording of Wire, Oral and Electronic Communications Manual

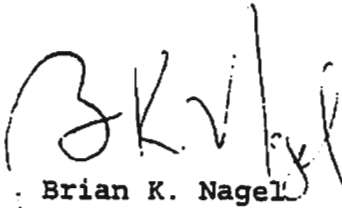
**Filing Instructions:**

- Remove and destroy pages 7 and 8 of Chapter 1, dated 03/01/2006, and replace with the attached revised pages.
- File this Policy Memorandum in front of this section.
- These materials are to be reproduced locally for all holders of the Interception and Recording of Wire, Oral and Electronic Communications Manual.
- This directive is in effect until superseded.

**Impact Statement:** This directive restores previously deleted material under the heading of "Security of Non-Telephone Consensual and Non-Consensual Intercept Equipment" with regards to the ledger book.

**Mandatory Review:** The Responsible Office will review all policy contained in this section in its entirety by or before March 2009.

Questions regarding this policy should be directed to the Investigative Support Division at 202-406-5773.

  
Brian K. Nagel  
AD - Investigations

DCP#: WIM 2006-3

RIF

## Introduction Table of Contents

	Page
Introduction .....	1
Overview of the Electronic Communications Privacy Act of 1986 (Public Law No. 999-508) ....	1
Definitions and Explanations .....	2
Exceptions .....	3
Title I - The Interception of Communications and Related Matters .....	4
Title II - Stored Wire and Electronic Communications and Transactional Records Access .....	4
Unlawful Access to Stored Communications .....	5
Disclosure of the Contents of a Stored Communication .....	5
Requirements for Governmental Access to Stored Communications .....	6
Procedures for Access to Transactional Information Including Telephone Records .....	6
Backup Preservation of Information in Storage .....	6
Delayed Notice .....	6
Title III - Pen Register and Trap and Trace Devices .....	6
Title I, II, and III (General) .....	7
Communications Assistance for Law Enforcement Act (CALEA) .....	7
Security of Non-Telephone Consensual and Non-Consensual Intercept Equipment .....	7
Reports to the Department of Justice .....	8



# INTRODUCTION

The purpose of this manual is to outline the legal and administrative procedures which must be followed when conducting either consensual or non-consensual interceptions of wire, oral, or electronic communications; or when utilizing pen registers, vehicle locator systems (VLS), telephone traps and traces; or when requesting governmental access to stored electronic communications.

In addition to the Fourth Amendment of the Constitution, there are a number of statutes and executive orders which govern the conduct of interceptions of wire, oral or electronic communications, both consensual and non-consensual.

The procedures used to conduct these interceptions are based upon procedures established by the Criminal Division of the Department of Justice pursuant to Title 18, United States Code, Sections 2510 to 2522; Title 18 Sections 2701 to 2712; Title 18 Sections 3121 to 3127 (Title I, II and III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (ECPA); the Communications Assistance for Law Enforcement Act of 1994 (CALEA), the Antiterrorism and Effective Death Penalty Act of 1996 (Antiterrorism Act)), the USA-Patriot Act of 2001, and The Homeland Security Act of 2002.

Although this Service may conduct interceptions pursuant to any of the aforementioned laws and regulations, the overwhelming majority of interceptions are conducted pursuant to the provisions of Title I, II, and III of the Electronic Communications Privacy Act of 1986. Since the other statutes are so diverse and so infrequently used by this Service, they are not addressed in this manual.

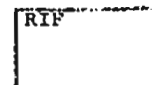
All requests for authorization of communication interceptions which are subject to provisions of statutes other than those incorporated in the Electronic Communications Privacy Act of 1986, should be directed to the Intelligence Division. The Intelligence Division, in conjunction with the Investigative Support Division, will coordinate the conduct of the interception and ensure all statistical and record keeping functions are accomplished.

All of the guidelines contained in this manual have been designed to assure strict adherence to the laws and rules that govern the use of these types of interceptions. It is the philosophy of the Secret Service that it is preferable to err on the side of caution rather than risk any inadvertent violation of law or established procedure when conducting such interceptions.

## Overview of the Electronic Communications Privacy Act of 1986 (Public Law No. 99-508)

This act is divided into three separate, but closely related titles: Title I - Interception of Communications and Related Matters; Title II - Stored Wire and Electronic Communications and Transactional Records Access; and Title III - Pen Registers and Trap and Trace Devices. The policies and procedures incorporated under this act became effective on January 20, 1987.

Since the act includes provisions for both civil and criminal penalties, all offices contemplating the use of investigative techniques covered under the act are cautioned to consult with the appropriate Office of the United States Attorney prior to implementation.





## Definitions and Explanations

**Department of Justice:** For the purpose of this manual, Department of Justice refers to the Office of Enforcement Operations, DOJ, Washington, D. C.

**Wire Communications:** The definition of "wire communication" means any "aural transfers" made in whole or in part through the use of facilities for the transmission of communication by the aid of wire, cable or other like connection between the point of origin and the point of reception as defined in 18 U.S.C. 2510 (1). Wire communications are specifically excluded from the definition of electronic communications, 18 U.S.C. 2510 (12) (A).

**Oral Communication:** 18 U.S.C. 2510 (2) defines oral communication as any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interceptions under circumstances justifying such expectation.

Oral communication, as defined, is specifically excluded from the definition of electronic communication.

**Intercept:** 18 U.S.C. 2510 (4) defines intercept as the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.

The "or other" was added to accommodate the non-aural acquisition of electronic communications.

**Electronic Communication:** 18 U.S.C. 2510 (12) defines "electronic communication" as any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or part by a wire, electromagnetic, photo electronic, or photo-optical system that affects interstate or foreign commerce.

"Electronic communication" is also specifically defined to exclude a wire or oral communication. The effect of the breadth of this definition is that any and all forms of electronic communications, unless specifically exempted, are now subject to statutory provision, just as wire and oral communications have been since 1968.

**Electronic, Mechanical or Other Device:** 18 U.S.C. 2510 (5) defines electronic, mechanical or other device as any device or apparatus which can be used to intercept wire or oral communication other than (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.

## Video Surveillance

Video surveillance or use of closed circuit television (CCTV) is not regulated by Title I, but it is frequently part of an application for electronic surveillance. When there is a reasonable expectation of privacy in the place to be videotaped, prior approval from an appropriate DOJ official and a court order is required before such video surveillance may be used in an investigation. A court order and prior DOJ approval is required unless the surveillance is used to record events in public places or places where the public has unrestricted access, and where the camera equipment can be installed in places to which investigators have lawful access.

If a court order is required, the pleadings are to be based on Rule 41 of the Federal Rules of Criminal Procedure and the All writs Act (28 U.S.C. Section 1651).

## Exceptions

Because the definition of electronic communication is so broad and all-inclusive, it became necessary to provide exceptions. The exceptions dealt with forms of electronic communications that either appeared patently not to be deserving of privacy protection or where a policy decision was made by the Congress not to include a specific form of electronic communication.

These exceptions appear in the legislation either as exceptions as defined in 18 U.S.C. 2510 or as exceptions to the section that penalizes certain activity as unlawful, 18 U.S.C. 2511. These exceptions are as follows:

1. **Tone only paging devices.** It has been the position of the Department of Justice that intercepting tone beeps or vibrations from a pager is not a search and, therefore, such interceptions raise no Fourth Amendment implications; the current statute endorses this policy. By contrast, digital display and voice paging devices are covered by the current statute (see Chapter IV of this manual).
2. **Communications from tracking devices (beepers) placed in automobiles or packages to trace their location.** 18 U.S.C. 2510 (12) (C). These are specifically excluded from this legislation because of the manner in which they function and the limited privacy implications related to their use. This area is being left to case law development.
3. **Pen registers, and trap and trace devices.** These investigative tools qualify as electronic communications as that term is broadly defined. Since the privacy interests involved are so limited with these techniques, they have been excluded from the coverage of Title I of the current statute.
4. 18 U.S.C. 2511 (2) (h) (i). However, Title III (Chapter 206, 18 U.S.C. 3121-3127, of the Federal Criminal Law Handbook) of the statute specifically regulates these techniques. By and large this Title, to be discussed in Chapter IV of this manual, merely codifies existing Department of Justice policy and practices on pen registers/trap and trace devices.
5. **Certain radio communications.** The definition of electronic communication is so broad that it sweeps in all forms of radio communications. Thus, it was necessary for the statute to specifically exclude various forms of radio communications that patently should not be subject to protection from interception such as electronic communications that are broadcast so as to be readily available to the public (AM and FM radio station broadcasts), ship to shore general public type communications, citizen band radio, general mobile radio services and the like. Reference is made to 18 U.S.C. 2511 (2) (g).

This subsection of the statute also contains other specific exceptions relating to interaction with the Federal Communications Act or where there is a necessity to service the system or locate interference. A review of Chapter 119 of the Federal Criminal Code and Rules is strongly recommended.

Reference is made to pertinent sections relating to the conduct of electronic surveillance to be found in the U.S. Attorney's Manual, Title 9, Chapter 7.



## **Title I - Interception of Communications and Related Matters**

The 1986 statute defines and regulates three types of communications: (1) wire; (2) oral; and (3) electronic communications. The last type, in essence, is any form of communication using electronics in which the human voice is not utilized.

It should be noted that the act mandates little change in the substantive or procedural requirements for obtaining an order to intercept a traditional wire or oral communication. In explaining the provisions of the act and the provisions set forth in the administrative guidelines which apply to interceptions not specifically provided for in the act (primarily Titles I and III), Title I of the current act largely replaces Title III under the old statute. Additional crimes have been added to the list of crimes enumerated in 18 U.S.C., Section 2516 for which a wire or oral interception order can be obtained. These additional crimes include the following, which may impact directly on this Service's operations:

18 U.S.C. 1203 (hostage taking);

18 U.S.C. 1029 (fraud and related activity in connection with access devices);

18 U.S.C. 115 (threatening or retaliating against a federal official) and;

18 U.S.C. 2511, 2512 (Interception and disclosure of certain communications and use of certain interception devices).

In addition, a subsection (18 U.S.C. 2516 (1) (I)) was added that authorizes interception to ascertain the location of any fugitive from justice from an offense described in 18 U.S.C. 2516 (1). Section 2518 of Title 18, which describes the procedure for intercepting wire, oral, and now electronic communications, remains substantially the same under this law.

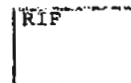
## **Title II - Stored Wire and Electronic Communications and Transactional Records Access**

Title II of the act is designed to protect the privacy of stored electronic communications, either before such a communication is transmitted to the recipient or, if a copy of the message is kept, after it is delivered.

In developing the legislation, electronic communications were divided into two categories: (a) communications during the transmission stage, and (b) communications in "storage."

Electronic Storage is defined in 18 U.S.C. 2510 (17) as both any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of backup protection of such communication. There was general recognition that the interception of communications during the transmission stage is more intrusive than of those in storage, and accordingly, those communications were given almost the same protection as that provided for wire and oral communications.

Stored communications were likened to regular mail being handled by the Post Office. Under present day standards, a search warrant would be required to intercept mail since it enjoys Fourth Amendment protection. Congress ultimately decided that electronic mail in storage incident to transmission should be accorded the



same protection. The same principle applies to "backup" copies made by the providers of electronic communications services.

Therefore, Fourth Amendment type protection will be accorded to the stored data for the first 180 days, requiring a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for government access. After the 180 day period expires, any records still retained would revert to the status of third party records and would be available by administrative or grand jury subpoena, a court order, or warrant. The most important provisions of Title II are the following:

## Unlawful Access to Stored Communications

18 U.S.C. 2701 makes it an offense to (a) intentionally access, without authorization, a facility through which an electronic communication service is provided; or (b) intentionally exceed the authorization of such facility; and as a result of this conduct, obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system.

This provision is intended to address the increasing problem of both unauthorized "computer hackers" and corporate spies who deliberately gain access to, and sometimes tamper with, electronic communications that are not available to the public. The provision is not intended to criminalize access to "electronic bulletin boards," which are generally open to the public so that interested persons may communicate on specific topics.

In addition, a communication will be found to be readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy.

## Disclosure of the Contents of a Stored Communication

18 U.S.C. 2702 (a) generally prohibits the provider of a wire or electronic communication service from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient of the communication. The originator, addressee, or intended recipient can give lawful consent to divulge the content of the communication.

18 U.S.C. 2702 (b) provides eight distinct exceptions that modify the general prohibitions against disclosure contained in 2702 (a). (See Chapter 5 for further explanation.) The eight exceptions allow disclosures to a law enforcement agency, if the contents were:

- (a) Inadvertently obtained by the service provider; and
- (b) Appear to pertain to the commission of a crime.

Similarly, 18 U.S.C. 2511 (3), as amended, prohibits such a provider from divulging the contents of a communication while it is in the transmission stage.

## **Requirements for Governmental Access to Stored Communications**

18 U.S.C. 2703 provides that a governmental entity may only obtain access to the contents of an electronic communication that has been in storage for 180 days or less pursuant to a search warrant. If the message has been stored for more than 180 days, the government can obtain the information by a variety of procedures including a search warrant, grand jury subpoena, administrative subpoena, or a court order, depending on the type of notification the government wishes to provide.

18 U.S.C. 2703 (b) relates specifically to records held in remote computing systems and such records that are not mentioned anywhere in 18 U.S.C. 2703 (a).

## **Procedures for Access to Transactional Information Including Telephone Records**

18 U.S.C. 2703 (c) sets forth the rules under which the government may obtain access to transactional records with or without the consent of the subscriber. These are records that pertain to the subscriber to, or customer of, an electronic communication service or remote computing service and which do not involve the contents of a communication. It should be noted that transactional records include toll records. The government will be able to obtain such transactional records by grand jury subpoena, administrative subpoena, search warrant, or court order based upon a finding of relevancy.

## **Backup Preservation of Information in Storage**

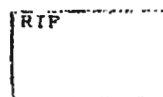
18 U.S.C. 2704 sets forth the procedures that apply to backup copy preservation. This is the provision that will permit law enforcement officials to have a copy made, in the nature of a picture of the records that exist on a given day, of records of illegal activities in which a computer storage or remote processing firm is utilized in the criminal activity.

## **Delayed Notice**

18 U.S.C. 2705 describes the circumstances under which the government may delay notification to the customer or subscriber.

## **Title III - Pen Register and Trap and Trace Devices**

Chapter 206 (18 U.S.C. Section 3121 to Section 3127) of the Federal Criminal Law Handbook covers Title III of the Electronic Communications Privacy Act of 1986. The Title begins with a general prohibition against the use of a pen register or a trap and trace device without first obtaining a court order pursuant to 18 U.S.C.



3123 or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.). This chapter, in essence, codifies the existing Department of Justice policy of obtaining a court order to authorize the installation of a pen register or a trap and trace device, and sets forth the procedure for seeking such an order.

NOTE: Under the provisions of the USA PATRIOT Act of 2001, the analysis remains unchanged with respect to the Fourth Amendment and the wiretap statute. However, substantial amendments to the definition of "Pen Register" and "Trap and Trace Device" alter the applicability of the pen/trap statute.

## **Title I, II and III (General)**

A review of Chapters 119, 121, and 206 of the Federal Criminal Law Handbook is strongly recommended. Further reference is made to pertinent sections relating to the conduct of electronic surveillance to be found in the U.S. Attorney's Manual, Title 9, Chapter 7.

## **Communications Assistance for Law Enforcement Act (CALEA)**

In October 1994, at the request of the nation's law enforcement community, Congress enacted the Communications Assistance for Law Enforcement Act, or CALEA. The CALEA clarified the scope of a telecommunications carrier's duty in effecting lawfully-authorized electronic surveillance and addressed previous deficiencies in the Electronic Communications Privacy Act. The CALEA requires telecommunications carriers to modify the design of their equipment, facilities, and services to ensure that lawfully-authorized electronic surveillance can actually be performed.

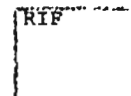
## **Security of Non-Telephone Consensual and Non-Consensual Intercept Equipment**

Due to the sensitivity of this type of equipment, it must be centrally located in one safe within each office or in a properly secured vault room within the office. In most cases, non-consensual equipment will be maintained within the Technical Security Division (TSD).

General access to the equipment should be limited to a minimum number of individuals, preferably supervisors, either by the squad supervisor, or in offices where assigned, the Physical Security Specialist, who are assigned to maintain, check out, check in, and secure the equipment. The record-keeping system controlling the use of the equipment must utilize a bound ledger book for this purpose.

The ledger book should be prepared with columns reflecting the following fields of information:

1. Date out - date that equipment is taken from storage.
2. Case Number - self-explanatory.



3. Equipment - description of item.
4. Serial and/or SS property number - self-explanatory.
5. Assigned to - last name of SA to whom equipment is being issued.
6. SA initials - Initials of SA to whom equipment is being issued.
7. Check out by - Initials of supervisor or other designee.
8. Date in - date item returned to storage.
9. Check in by - Initials of supervisor or other designee.

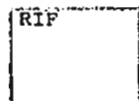
## Reports to the Department of Justice

### Non Consensual

The provisions of title 18 U.S.C. 2519 mandate that the Secret Service submit an annual report, due in January, to the Attorney General or the Assistant Attorney General of the United States regarding non-consensual intercepts. This report will cover each application for any non-consensual wire, oral, or electronic interception order made by this Service under provisions of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986.

### Consensual

There are no reporting requirements to the Attorney General for consensual monitoring. However, DOJ requires an agency to maintain the records of all consensual monitoring. Investigative Support Division (ISD) will maintain all the consensual monitors approved and conducted for three (3) years per General Records Schedule 23.



## Consensual Interceptions Table of Contents

	Page
Introduction .....	1
Secret Service Policy .....	1
Delegation of Authority .....	1
Consensual Interceptions and/or Recordings of Telephonic and Non-Telephonic Communications ....	2
Department of Justice Policy .....	2
Cases Requiring Prior Written Department of Justice Approval.....	2
Exceptions .....	4
Cases Not Requiring Prior Department of Justice Approval.....	4
Authorization Procedures for All Consensual Telephonic and Non-Telephonic Interceptions .....	5
Examples of Consensual Non-Telephonic Interceptions and/or Recordings .....	6
Examples of Consensual Telephonic Interceptions and/or Recordings .....	6
Reporting of Consensual Non-Telephonic Interceptions .....	6
Sample Official Message for Reporting a Consensual Interception for a Non-Telephonic Communication.....	8
Incidental Non-Telephonic Consensual Interception .....	9
Sample Incidental Non-Telephonic Consensual Interception Official Message (Interception of Non-Target Individuals) .....	9
Special Requirement for Sting Operations .....	10
Sample "Sting" Operation Official Message .....	11
Reporting of Consensual Telephonic Interception.....	12
Sample Consensual Telephonic Interception Official Message .....	13
Additional Interceptions .....	14
Interceptions of "Name Unknown" Subjects and Identified Subjects Previously Using an Alias .....	14
Telephonic and Non-Telephonic Recordings .....	14
Electronic Communications Consensual Intercepts .....	14
Sample Official Message Reporting a Consensual Interception of Electronic Communication .....	16
Reports to the Department of Justice (DOJ) .....	17

RIF



United States Secret Service  
Directives System

Manual : Interception  
RO : ISD

Section : Chapter II  
Date : 08/06/2009



---

**Subject:** Consensual Interceptions

---

**To:** All Supervisors and All Manual Holders of the Interception and Recording of Wire, Oral, and Electronic Communications Manual

**Filing Instructions:**

- Remove and destroy the Chapter II Table of Contents (dated 03/01/2006), and replace with the attached revised Table of Contents.
- Remove and destroy Chapter II, Consensual Interceptions (dated 03/01/2006), in its entirety and replace with the attached revised chapter.
- File this Policy Memorandum in front of this section.
- This directive is in effect until superseded.

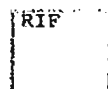
**Impact Statement:** This directive has been updated to remove language that could compromise ongoing investigations of additional subjects or criminal websites. More specifically, language has been removed from pages 15 and 16 that allowed "working copies" to be made of computer hard drives as they are not needed for continuing investigations.

**Mandatory Review:** The Responsible Office will review all policy contained in this section in its entirety by or before August 2012.

Questions regarding this policy should be directed to the Investigative Support Division at 202-406-5773.

  
Mr. Michael Merritt  
AD - Investigations

DCP#: WIM 2009-02



# CONSENSUAL INTERCEPTIONS

## Introduction

Pursuant to the provisions of Title 1, it is not necessary to obtain a court order in situations where one or more parties to a communication have given their prior consent to the interception or recording of their conversations. Title 18 U.S.C. 2511 (2)(c) states that "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."

The monitoring of conversations with the consent of one of the participants is a particularly effective and reliable investigative technique; and its use by the U.S. Secret Service (USSS) during a criminal investigation is encouraged where appropriate, and is expected where necessary. Nevertheless, although it is clear that such monitoring is constitutionally and statutorily permissible, it is appropriate that this investigative technique continue to be closely regulated.

For this reason, specific administrative guidelines and procedures have been established by the Department of Justice (DOJ) and the U.S. Secret Service. These guidelines and procedures address two categories of consensual interceptions; non telephonic to include electronic communications, and telephonic.

## Secret Service Policy

Reference is made to the Attorney General's memorandum dated May 30, 2002, entitled "Procedures for Lawful, Warrantless Monitoring of Verbal Communication." This memorandum allows the Director to delegate this authority to other supervisors within the USSS. Accordingly, the Director has issued a delegation of authority for the authorization of these interceptions. This delegation of authority is reproduced as follows:

### DELEGATION OF AUTHORITY

NO. 34 REVISION NO. 4

#### **INTERCEPTION OR RECORDING OF CONVERSATIONS WITH THE CONSENT OF ONE PARTY BY SECRET SERVICE PERSONNEL**

In accordance with the Department of Justice U.S. Attorneys' Manual, 9-7.301, Consensual Monitoring, the following officials of the U.S. Secret Service are hereby delegated the authority to approve and to implement the monitoring of private conversations with the consent of one party, in limited contexts as set forth in, and pursuant to, the guidelines promulgated by the Attorney General dated May 30, 2002:

### Non-telephonic and Telephonic Interceptions

Assistant Director – Office of Investigations  
Assistant Director – Office of Protective Research  
Assistant Director – Office of Professional Responsibility  
Deputy Assistant Director(s) – Office of Investigations  
Deputy Assistant Director(s) – Office of Protective Research  
Deputy Assistant Director(s) – Office of Professional Responsibility  
Special Agent in Charge – Office of Protective Intelligence and Assessment Division  
Special Agent in Charge – Office of Criminal Investigative Division  
Special Agent in Charge – Office of Investigative Support Division  
Special Agents in Charge – USSS Field Offices

This authority may be delegated to the Deputy Special Agent in Charge (DSAICs), Assistant Special Agent in Charge (ASAIcs), and Resident Agent (RAICs) acting in the capacity of the Special Agent in Charge (SAICs) enumerated above.

This delegation supersedes USSS Delegations of Authority No. 34, Revision No. 3, dated November 6, 2000.

## Consensual Interceptions and/or Recordings of Telephonic and Non-Telephonic Communications

### Department of Justice Policy

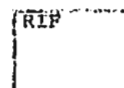
Department of Justice (DOJ) administrative guidelines and procedures governing the use of consensual non-telephonic interceptions are outlined specifically in the Attorney General's memorandum dated May 30, 2002, entitled "Procedures for Lawful, Warrantless Monitoring of Verbal Communication." This memorandum, hereinafter referred to as "the Attorney General's memorandum," is the basis for all USSS guidelines and procedures set forth in this chapter.

Specific authorization and reporting procedures have been established for use during all consensual interceptions of telephonic and non-telephonic communications. In most cases, these authorization procedures do not require prior written authorization from the DOJ, Office of Enforcement Operations (OEO). However, in a number of "sensitive" cases, prior written approval for the interception must be granted by the Director or Associate Director of the OEO, DOJ.

### Cases Requiring Prior Written Department of Justice Approval

In all but the most sensitive cases, the authority to approve requests for consensual surveillance is transferred to the departments and agencies.

There are six sensitive types of cases that require formal written approval from the DOJ. These sensitive cases require approval in writing by the Director or Associate Director of the Office of Enforcement Operation (OEO), Criminal Division, U.S. Department of Justice. These cases will be coordinated through the Investigative Support Division (ISD)



Prior to submitting a request for approval to the OEO, the investigator must first discuss with the Assistant United States Attorney (AUSA) the appropriateness and legality of the consensual monitoring. Upon concurrence from the AUSA, the investigator will make a formal request to the DOJ (OEO) with the approval of the Director or his designee. (See the Delegation of Authority on page 1 of this chapter.)

An emergency request may be made by telephone to the authorizing official and should later be memorialized in writing and submitted to the appropriate headquarters official as soon as practical after authorization has been obtained

If an emergency situation requires consensual monitoring and the approving official can not be reached, the authorization may be given by the Director or his/her authorized designee (Per Delegation of Authority). No later than three working days after the emergency authorization, this Service must notify, in writing, OEO, of the emergency monitoring.

The six "sensitive" case categories are as follows:

1. **High Federal Officials.** Investigations involving such sensitive investigative tools such as those utilized in consensual monitoring must be approached with extra care when the non-consenting party is a high Federal official. The officials delineated are: Members of Congress, Federal Judges, and any other Federal official holding a position of Executive Level IV or above, or a person who has served in this capacity within the last two years. This group includes Cabinet members, members of the White House staff, and most Presidential appointees. Investigations involving such officials must be supervised and coordinated at a central point, particularly since such investigations may raise issues involving the application of the Special Prosecutor provisions of the Ethics in Government Act of 1978. This category encompasses all of the major positions covered by that Act.
2. **Other Public Officials.** The Department of Justice has deemed it inappropriate to require central authorization in all cases in which other public servants, both Federal and State, are non-consenting parties because of the size and scope of the Federal and State work force and the wide variety of offenses that might be involved. However, certain offenses involving Federal or State public officials strike at the very integrity of Government. Thus, in cases in which a public official is the target of the investigation and the alleged offense involves **bribery, conflict of interest, or extortion** relating to the performance of official duties, centralized Department of Justice control will be retained.
3. **Members of the Diplomatic Corps.** Consensual surveillance of members of the diplomatic corps of a foreign country raises questions concerning the foreign relations of this country. To ensure appropriate coordination with the U.S Department of State in this sensitive area, formal written approval from the Department of Justice is required before consensual monitoring is utilized.
4. **Protected Witnesses.** It is vital to the integrity of the Witness Security Program that controls be maintained regarding the manner in which witnesses in the program, or those known to have been in the program, are properly utilized. For instance, use of a protected witness as an undercover informant can expose him/her to extreme danger, greater than that faced by other undercover informants. Centralized control is important in this area as well.

5. **Federal Prisoners.** The use of a monitoring device involving a person in the custody of either the Federal Bureau of Prisons or the United States Marshals Service raises particularly sensitive issues not the least of which concerns the Fifth Amendment right to counsel. It is also vital to prisoner security and safety that the Bureau of Prisons and the Marshals Service be informed whenever possible of consensual monitoring activities in their institutions or involving their charges; this is true whether the consenting person is or is not the prisoner. Authorization in such cases must be centralized in the Department of Justice. (Procedures on the use of Federal Prisoners are outlined in Investigative Manual, section ISD-08.)
6. **Where Otherwise Requested by the Department of Justice.** The final category consists of specific cases in which a written request from a United States Attorney or a higher Department of Justice official is deemed necessary for the proper progress of an investigation. This determination will be made by the United States Attorney(s) or officials of higher position within the Department of Justice.

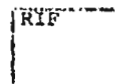
## Exceptions

Even if the interception falls within any of the six aforementioned categories, prior Department of Justice approval is not required for:

1. Extraterritorial interceptions;
2. Foreign Intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.);
3. Interceptions pursuant to the court-authorization procedures of Title I & III of the Omnibus Crime Control and Safe Streets Act of 1986 as amended (18 U.S.C. 2510, et seq.);
4. Routine Bureau of Prisons interceptions of verbal communications which are not attended by a justifiable expectation of privacy;
5. Interceptions of radio communications; and
6. Interceptions of telephonic communications.

## Cases Not Requiring Prior Department of Justice Approval

If an interception which is to be made does not fall within the six "sensitive" case situations, no prior written Department of Justice authorization is required.



## Authorization Procedures for All Consensual Telephonic and Non-Telephonic Interceptions

All interceptions must be authorized by the head of the department or agency or his/her authorized designee (See Delegation of Authority), on page 1 of this chapter). However, prior to receiving approval, a representative of the department or agency (usually, the case agent) must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation.

The requirement for approval is based on the Attorney General's memorandum titled "Procedures for Lawful, Warrantless Monitoring of Verbal Communications" dated May 30, 2002, which allows approval for the interception by the Director or his/her designee.

Whenever possible, authority to conduct an interception should be requested at least 48 hours prior to the interception.

If the interception falls within any of the six "sensitive" case situations requiring prior Department of Justice approval, the request for approval shall be made to the Department of Justice by the appropriate operational division, through the Investigative Support Division (ISD).

Additionally, the following guidelines, promulgated by the U.S. Department of Justice, will apply to inmate telephone conversations monitored by the Federal Bureau of Prisons:

1. Prison officials can monitor inmate telephone conversations for the purposes of maintaining prison security and prison administration. Attorney/client calls, however, are obviously excluded.
2. Law enforcement authorities outside of the Bureau of Prisons are not allowed random access to inmate monitored telephone conversations, past, present or future.
3. Requests by outside law enforcement agencies to disclose transcripts of the general telephone conversations of inmates that have been monitored in the past, in connection with a criminal investigation relating to activities outside the confines of the prison and concerning specified individuals, will be complied with only pursuant to a proper legal authorization, (e.g., grand jury subpoena, search warrant, or subpoena issued by the court).
4. Requests by outside law enforcement agencies to monitor and disclose the future telephone conversations of specified inmates in connection with a criminal investigation being conducted, relating to activities outside the confines of the prison that do not affect prison security or administration, will be complied with only where an interception order has been procured under the authority of Federal statutes pertaining to electronic surveillance, 18 U.S.C. 2510 et seq.

In addition, it should be noted that inmate/attorney telephone monitoring requires a court order, absent a clear showing that there is no attorney client privilege involved. Also, in cases of consensual telephone monitoring involving prisoner use requests (see Investigative Manual, section ISD-08), permission for telephone monitoring may be appended upon request, in the initial communication requesting the use of the prisoner.

28 C.F.R. 540.102, directs the warden of a Federal correctional institution to give notice to the prisoners of the potential for monitoring their conversations.

## Examples of Consensual Non-Telephonic Interceptions and/or Recordings

1. The use of a transmitter or recorder secreted on the person of an agent or informant while engaged in conversations with a suspect or suspects.
2. The installation of a transmitter or recorder in a fixed location, without trespass, where an agent or informant is engaged in conversation with a suspect or suspects. (Unless an agent or person is acting pursuant to court order that authorizes entry and/or trespass.)

(NOTE: Should the consenting party leave the location where the transmitter or recorder is installed, the interception and/or recording of further conversation between the non-consenting parties must terminate immediately. Continued interception would require a court order under Title I.)

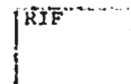
3. Electronic Communication intercepted over a modem or network connection. Additional information is available on page 14 of this policy under the section entitled "Electronic Communications Consensual Intercepts."

## Examples of Consensual Telephonic Interceptions and/or Recordings

1. Phone call to or from a consenting person, agent or otherwise, to a suspect while a second agent listens on an extension telephone.
2. Phone call to or from a consenting person, agent or otherwise, to a suspect while a second agent overhears the conversation on speaker-type phone equipment.
3. Phone call to or from a consenting person, agent or otherwise, to a suspect while a stenographer records the conversation in shorthand while overhearing the conversation.
4. Phone call to or from a consenting person, agent or otherwise, to a suspect which is recorded. This example is considered to be included within the above guidelines even though the conversation is not listened to by a third party until the conversation has been concluded, i.e., by playing the recording. As in non-telephonic intercepts, tape cassettes or disks used in recording consensual telephonic intercepts should be properly labeled. All evidence should be handled in accordance with evidence handling procedures which can be found in the "Reference Guide for "Evid"/Evidence System," located under the Resources Section of the Forensic Services Division (FSD) Homepage.

## Reporting of Consensual Non-Telephonic Interceptions

Within two (2) days following any interception, an official message must be forwarded to the appropriate operational division, appropriate Assistant Director's Office, and the Investigative Support Division (ISD). This official message should be submitted under the case number of the investigation in which the interception has been conducted. If a local field office case number has been assigned, it must be designated Special ("S"). This official message will be part of the case file maintained at the field office and at the appropriate operational division. (See the section entitled "Electronic Communications Consensual Intercepts" on page 14 of this policy for electronic communication intercept reporting requirements.)



This official message shall comment on the following factors:

- Name of the United States Attorney, Assistant United States Attorney or Organized Crime Strike Force attorney who provided advice as to the legality of the consensual interception, date of advice, and the judicial district to which he/she is assigned;
- Reason for the interception;
- Whether or not the target of the interception falls within any of the six "sensitive" case situations. If yes, explain (see the six "sensitive" case categories listed in this chapter);
- Type of equipment used;
- Equipment serial and/or USSS property number;
- Whether or not a recording was made (if no, state reason why, i.e., equipment failure, etc.);
- Method of installation;
- Location where equipment was used (include judicial district);
- Name(s) of all person(s) intercepted, include all aliases, dates of birth, and Social Security numbers if available, or "unknown subject." (The name(s) of the person intercepted for which permission to intercept as a target was obtained should be listed first, and should be denoted as a target);
- Name of consenting party;
- Date of interception;
- Duration of interception;
- Investigative benefits derived (Be specific if no benefits were derived); and
- Is continued use expected? Yes or No.

When any authorization is granted, it applies to only those target individuals who were identified in the initial request. If additional individuals become targets of a consensual interception and/or recording in the same investigation, a separate authorization must be obtained for these new targets.

The following pages have sample official message formats reporting a consensual interception of a non-telephonic communication.



## Sample Official Message for Reporting a Consensual Interception for a Non-Telephonic Communication

<b>FROM:</b>	<b>SAIC-FIELD OFFICE</b>	<b>CASE NUMBER:</b>
		<b>CASE TITLE:</b>
<b>TO:</b>	<b>SAIC-APPROPRIATE OPERATIONAL DIVISION</b>	
<b>INFO:</b>	<b>AD - APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC - INVESTIGATIVE SUPPORT DIVISION</b>	
<b>SUBJECT:</b>	<b>CONSENSUAL INTERCEPTION AND/OR RECORDING OF NON-TELEPHONIC COMMUNICATION</b>	
<b>AUTHORIZATION:</b>	(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)	
<b>ADVISING AUSA:</b>	(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO HAS GIVEN ADVICE ON THE LEGALITY OF THE INTERCEPTION, DATE OF ADVICE, AND THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED)	
<b>REASON FOR INTERCEPTION:</b>	(TO OBTAIN INCRIMINATING STATEMENTS, CORROBORATE INFORMATION, ETC.)	
<b>SENSITIVE SITUATION:</b>	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER.)	
<b>TYPE OF EQUIPMENT USED:</b>	(AUDIO/RF TRANSMITTER, RECEIVER, OR RECORDING DEVICES, ETC.)	
<b>EQUIPMENT SERIAL AND/OR USSS PROPERTY NUMBER:</b>		
<b>WHETHER OR NOT A RECORDING WAS MADE:</b>	(YES OR NO. IF NO, STATE REASON WHY, I.E., EQUIPMENT FAILURE, ETC.)	
<b>METHOD OF INSTALLATION:</b>	(ON BODY OF AGENT, ON BODY OF INFORMANT, IN GOVERNMENT VEHICLE, ETC.)	
<b>LOCATION WHERE EQUIPMENT WAS USED:</b>	(EXACT STREET ADDRESS, CITY, STATE, JUDICIAL DISTRICT)	
<b>NAME OF PERSON(S) INTERCEPTED:</b>	(IDENTIFY PERSON(S) INTERCEPTED, INCLUDE ALL ALIASES, DATES OF BIRTH AND SOCIAL SECURITY NUMBER IF AVAILABLE, OR "UNKNOWN SUBJECT." LIST AUTHORIZED TARGET FIRST, THEN ENTER INCIDENTAL INTERCEPTIONS. LIST EACH SUBJECT BY NUMBER, I.E., 1, 2, ETC.)	
<b>NAME OF CONSENTING PARTY:</b>		
<b>DATE OF INTERCEPTION:</b>		
<b>DURATION OF INTERCEPTION:</b>	(STARTING TIME TO ENDING TIME OF THE INTERCEPTION FOR EACH INDIVIDUAL. LIST THE DURATION FOR EACH SUBJECT BY NUMBER AS ABOVE.)	
<b>INVESTIGATIVE BENEFITS DERIVED:</b>	(BRIEF SYNOPSIS)	
<b>EXPECTED CONTINUED USE:</b>	(YES OR NO).	
<b>FIELD OFFICE</b>	<b>CASE SA/SUPERVISOR/SAIC</b>	

## Incidental Non-Telephonic Consensual Interception

When a subject other than the target is intercepted, an official message must be sent in the above previously mentioned format or in the following format (see sample below). The message should indicate the authorized target of the interception.

### Sample Incidental Non-Telephonic Consensual Interception Official Message (Interception of Non-Target Individuals)

FROM:	SAIC-FIELD OFFICE	CASE NUMBER:	
		CASE TITLE:	
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION		
INFO:	AD - APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC - INVESTIGATIVE SUPPORT DIVISION		
SUBJECT:	CONSENSUAL INTERCEPTION AND OR RECORDING OF NON-TELEPHONIC COMMUNICATION (INCIDENTAL INTERCEPTION)		
ON (DATE), _____ SAIC OF (FIELD OFFICE) AUTHORIZED INTERCEPTION AND RECORDING OF (SUBJECT) PURSUANT TO A COUNTERFEIT INVESTIGATION IN ABOVE CASE NUMBER.			
DURING AN ATTEMPT TO LOCATE AND INTERVIEW THE TARGET (NAME), THE FOLLOWING PERSON(S) WAS/WERE INTERCEPTED.			
NAME OF PERSON(S) INTERCEPTED:	(IDENTIFY PERSON (S) IF KNOWN. INCLUDE ALL ALIASES, AND IDENTIFIERS, OR UNKNOWN SUBJECT)		
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES)		
TYPE OF EQUIPMENT USED:	(AUDIO/RF TRANSMITTER, RECEIVER, OR RECORDING DEVICES, ETC.)		
EQUIPMENT SERIAL AND OR USSS PROPERTY NUMBER:			
WHETHER OR NOT RECORDING MADE:	(YES OR NO. IF NO, STATE REASON WHY, I.E., EQUIPMENT FAILURE, ETC.)		
METHOD OF INSTALLATION:	(ON BODY OF AGENT, ON BODY OF INFORMANT, ETC.)		
LOCATION WHERE EQUIPMENT WAS USED:	(EXACT STREET ADDRESS, CITY, STATE)		
NAME OF CONSENTING PARTY:			
DATE OF INTERCEPTION:			
DURATION OF INTERCEPTION:	(START TIME TO END TIME)		
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS)		
EXPECTED CONTINUED USE:	(YES OR NO. IF YES, NOTE HERE IF ADDITIONAL AUTHORIZATION HAS BEEN OR WILL BE REQUESTED)		
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC		

## Special Requirements for Sting Operations

"Sting" operation procedures are designed for operations where it is expected that most of the persons to be intercepted would be of the "walk-in" variety, such as in store front operations under conditions where the target is unknown before he is intercepted. However, if the "sting" operation is the type where it is known prior to an interception, who is to be intercepted, these blanket authorization procedures do not apply. The normal procedures for obtaining authorization for each target apply.

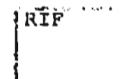
The reporting requirements for non-telephonic consensual interceptions during a "sting" operation is unique. As in "non-sting" type cases, the field office will provide in advance of the intercept to the appropriate operational division the following information:

1. **Case File Number** (Note: all intercept cases are to be designated as "S" Cases except case classification code 704 "Sting" Operations. Code 704 requires Headquarters distribution of memorandum reports.);
2. **Date of intended use;**
3. **Target to be intercepted;**
4. **Type of violation (CFT/Financial Crimes/etc.);**
5. **Statute violated;**
6. **Office and person making request;**
7. **If sensitive situation (what type?), and**
8. **Name and district of Assistant United States Attorney (AUSA).**

All targets intercepted under this "Blanket Worksheet" will be immediately reported via official message (as in "Non-Sting" cases). Each new target will be assigned a separate case suffix number (first suffix field). Each target can then be intercepted for a sixty day period beginning on the date of the first intercept of that target, without requesting an additional authorization.

### Sample "Sting" Operation Official Message

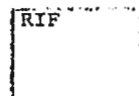
FROM:	SAIC-FIELD OFFICE	CASE NUMBER:	
		CASE TITLE:	
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION		
INFO:	AD - APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC - INVESTIGATIVE SUPPORT DIVISION		
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF NON-TELEPHONIC COMMUNICATION - OPERATION (NAME)		
AUTHORIZATION:	(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)		
ADVISING AUSA:	(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO HAS GIVEN ADVICE ON LEGALITY OF THE INTERCEPTION, DATE OF ADVICE, AND THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED)		
REASON FOR INTERCEPTION:	(TO OBTAIN INCRIMINATING STATEMENTS, CORROBORATE INFORMATION, ETC.)		
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER.)		
TYPE OF EQUIPMENT USED:	(AUDIO/RF TRANSMITTER, RECEIVER, OR RECORDING DEVICES, ETC.)		
EQUIPMENT SERIAL AND/OR USSS PROPERTY NUMBER:			
WHETHER OR NOT RECORDING WAS MADE:	(YES OR NO. IF NO, STATE REASON WHY. I.E., EQUIPMENT FAILURE, ETC.)		
METHOD OF INSTALLATION:	(ON BODY OF AGENT, ON BODY OF INFORMANT, IN GOVERNMENT VEHICLE, ETC.)		
LOCATION WHERE EQUIPMENT WAS USED:	(EXACT STREET ADDRESS, CITY, STATE, JUDICIAL DISTRICT)		
NAME OF PERSON(S) INTERCEPTED:	(IDENTIFY PERSON(S) INTERCEPTED, INCLUDE ALL ALIASES, DATES OF BIRTH AND SOCIAL SECURITY NUMBERS IF AVAILABLE OR "UNKNOWN SUBJECT." LIST AUTHORIZED TARGET FIRST, and THEN ENTER INCIDENTAL INTERCEPTIONS. LIST EACH SUBJECT BY NUMBER, I.E., 1, 2, ETC.)		
NAME OF CONSENTING PARTY:			
DATE OF INTERCEPTION:			
DURATION OF INTERCEPTION:	(STARTING TIME TO ENDING TIME OF THE INTERCEPTION FOR EACH INDIVIDUAL. LIST THE DURATION FOR EACH SUBJECT BY NUMBER AS ABOVE.)		
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS)		
EXPECTED CONTINUED USE:	YES OR NO		
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC		



## Reporting of Consensual Telephonic Interception

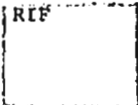
As with the consensual non-telephonic interception, when conducting a consensual telephonic intercept, an official message must be forwarded to the appropriate operational division with distribution to the appropriate Assistant Director's Office and the Investigative Support Division (ISD). This Official Message should be submitted under the case number of the investigation in which the interception has been conducted. It must be designated special (S) in all cases involving consensual interceptions. The official message should comment on the following factors:

- Name of USSS authorizing official and date of authorization;
- Name of the United States Attorney, Assistant United States Attorney or Organized Crime Strike Force attorney who provided advice as to the legality of the consensual interception, date of advice, and the judicial district to which he/she is assigned;
- Reason for the interception;
- Whether or not the target of the interception falls within any of the six "sensitive" case situations. If yes, explain. (See the six "sensitive" case categories listed in this chapter.);
- Type of equipment used;
- Equipment serial and/or USSS property number;
- Whether or not a recording was made (if no, state reason why, i.e., equipment failure, etc.);
- Method of installation;
- Location where equipment was used (include judicial district);
- Name(s) of all person(s) intercepted, include all aliases, dates of birth, and Social Security numbers if available, or "unknown subject." (The name(s) of the person(s) intercepted for which permission to intercept as a target was obtained should be listed first, and should be denoted as a target);
- Name of consenting party;
- Telephone number to which the call was placed. (If the call was incoming to consenting party, note this in the official message.);
- Telephone number, to include area code from which the call was placed;
- Date of interception;
- Duration of interception;
- Investigative benefits derived. (Be specific if no benefits were derived); and
- Is continued use expected? Yes or No.



## Sample Consensual Telephonic Interception Official Message

FROM:	SAIC-FIELD OFFICE	CASE NUMBER:
		CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD - APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC - INVESTIGATIVE SUPPORT DIVISION	
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF TELEPHONIC COMMUNICATION	
AUTHORIZATION:	(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)	
ADVISING AUSA:	(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO PROVIDED ADVICE ON LEGALITY OF THE INTERCEPTION. DATE THE ADVICE WAS GIVEN, THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED.)	
REASON FOR INTERCEPTION:	(TO OBTAIN INCRIMINATING STATEMENTS, TO CORROBORATE INFORMATION, ETC.)	
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER)	
TYPE OF EQUIPMENT USED:	(SONY TC-110A TAPE RECORDER, ETC.)	
EQUIPMENT SERIAL AND/OR USSS PROPERTY NUMBER:		
WHETHER OR NOT RECORDING WAS MADE:	(YES OR NO)	
METHOD OF INSTALLATION:	(INDUCTION COIL, ETC.)	
LOCATION WHERE EQUIPMENT WAS USED:	(NAME OF FIELD OFFICE, EXACT STREET ADDRESS, STATE, JUDICIAL DISTRICT)	
NAME OF SUBJECT(S) INTERCEPTED:	TARGET(S), (INCLUDE ALL ALIASES, DOB'S, SSN'S, AVAILABLE OR "UNKNOWN")	
NAME OF CONSENTING PARTY:	(AGENT NAME, INFORMANT NUMBER, ETC.)	
TELEPHONE NUMBER TO WHICH CALL PLACED:	(IF CALL WAS INCOMING TO CONSENTING PARTY, NOTE)	
TELEPHONE NUMBER CALL MADE FROM:		
DATE OF INTERCEPTION:		
DURATION OF INTERCEPTION:	(STARTING TIME TO ENDING TIME OF THE INTERCEPTION)	
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS)	
EXPECTED CONTINUED INTERCEPTION:	YES OR NO	
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC	



## **Additional Interceptions**

A separate official message must be submitted for each and every telephonic and non-telephonic interception.

## **Interceptions of "Name Unknown" Subjects and Identified Subjects Previously Using an Alias**

No additional official messages are necessary when identification is made on subjects using an alias or "unknown subjects." However, the identification will be indicated in the memorandum report referencing the official message which previously reported the target as unknown or subject using an alias.

## **Telephonic and Non-Telephonic Recordings**

Once a recording is made using any type of audio, video, and/or electronic storage device, it must be properly labeled to identify the recording of all consensual interceptions of wire and oral communications. The label must contain the case number, date and time of interception, name of case agent, and person intercepting the communication.

All consensual recordings (audio, video, and/or electronic) will be inventoried on an SSF 1544, Certified Inventory of Evidence, and will be maintained in a secure location. All evidence should be handled in accordance to evidence handling procedures which can be found in the "Reference Guide for "Evid"/Evidence System," located under the Forensic Services Division (FSD) Homepage, Resources Section.

At the time a non-judicial case is closed, with the approval of the appropriate Headquarters operational division, consensual recordings may be physically destroyed locally. Judicial cases also require permission from the appropriate operational division and consultation with the U.S. Attorney's Office, prior to destruction. **SSF 1544 clearance procedures must be followed when physically destroying consensual recordings. THE AUDIO, VIDEO, AND/OR ELECTRONIC STORAGE DEVICES (TAPES/ DISKS) SHOULD NEVER BE RE-USED FOR THE RECORDING OF EVIDENCE.**

## **Electronic Communications Consensual Intercepts**

As previously stated in this manual, "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronics, or photo-optical system that affects interstate or foreign commerce. Additional reference to this definition and related topics may be found under Title 18 U.S.C. 2510.

Generally speaking, consensual interception of electronic communications over public phone lines or network connection will be handled in the same manner as the interception of telephonic and non-telephonic communication, with the local field office SAIC authorizing the intercept. Prior to the intercept, advice must be obtained from the AUSA as to the legality of the proposed consensual interception.

Examples of consensual computer data transmissions (electronic communications) are as follows:

- Party A communicates with Party B via computer attached by a modem or network connection.
- Party A and Party B communicate with each other directly in what is called the "chat" mode. Typically via an instant messenger program such as ICQ, MSN, AOL, etc.

When two individuals (one consenting-Special Agent/Informant) are communicating over phone lines or network connection using computers, as in the above examples, and the conversation is being recorded, printed or viewed by a third party, a consensual intercept is being made. In these cases an official message must be sent to the appropriate operational division.

**NOTE: The private area of an electronic bulletin board is one that does not have general access. An "elite" bulletin board, where there is no general access, is treated the same as the private area of a general access bulletin board. This area, for example, has a special password, not known to the general public. Caution must be exercised when using computer bulletin boards. This type of consensual interception should be thoroughly discussed with the local U.S. Attorney's Office. Prior to an interception, Secret Service personnel may not "hack" onto a bulletin board gaining access by breaking security systems, etc. This would be considered a non-consensual interception and would require a court order.**

As in the case of consensual telephonic intercepts, authorization for this type of intercept, conducted over telephone lines or a network connection, should emanate from the SAIC of the investigating field office. The authorization to intercept the electronic communication will be obtained in the beginning of the interception and will be valid for the duration of the investigation. Once an authorization has been given, an official message must be sent every 30 days from the date of initial interception to the appropriate operational division, appropriate AD's office and ISD.

Notification of such intercepts will be made in much the same manner as consensual telephonic intercepts. However, modifications to the official message are necessary. These modifications will include the type of computer equipment used in the intercept in addition to, the property or serial number of the computer equipment.

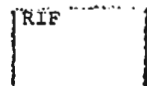
The intercepted communication must be converted to a hardcopy printout and/or stored to a technologically appropriate storage device. The printouts and or communication stored on a storage device must be treated as evidence and handled in accordance to evidence handling procedures which can be found in the "Reference Guide for "Evid"/Evidence System," located under the Forensic Services Division (FSD) Homepage, Resources Section.

The following page has a sample official message reporting a consensual interception of electronic communication:



## Sample Official Message Reporting a Consensual Interception of Electronic Communication

FROM:	SAIC-FIELD OFFICE	CASE NUMBER:
		CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD - APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC - INVESTIGATIVE SUPPORT DIVISION	
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF ELECTRONICS COMMUNICATION	
AUTHORIZATION:	(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)	
ADVISING AUSA:	(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO HAS GIVEN ADVICE ON LEGALTY OF THE INTERCEPTION, DATE OF ADVICE, AND THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED)	
REASON FOR INTERCEPTION:	(TO OBTAIN INCRIMINATING STATEMENTS, CORROBORATE INFORMATION, ETC.)	
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER)	
COMPUTER EQUIPMENT USED:	(WITH SERIAL OR USSS PROPERTY #)	
WHETHER OR NOT A COPY WAS MADE:	(YES OR NO. IF NO, STATE REASON WHY, I.E., EQUIPMENT FAILURE, ETC.)	
TYPE OF EQUIPMENT USED TO MAKE COPY:	(WITH SERIAL OR USSS PROPERTY #)	
METHOD OF MAKING COPY:		
NAME OF CONSENTING PARTY:		
NAME OF PERSON BEING INTERCEPTED:	(TARGET UNIQUE NETWORK IDENTIFIERS TO INCLUDE TRUE NAME, USERNAME, MAC ADDRESS, NETWORK COMPUTER NAME, PHONE NUMBER, EMAIL ADDRESS, IP ADDRESS, ICQ NUMBER, AIM NUMBER, ETC; LIST THE TARGETS IF THERE IS MORE THAN ONE TARGETS)	
DURATION OF INTERCEPTION:	(MM/DD/CCYY, HH/MM - MM/DD/CCYY, HH/MM)	
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS OF THE INTERCEPTION RESULT)	
EXPECTED CONTINUED INTERCEPTION:	YES OR NO	
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC	



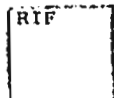
## Reports to the Department of Justice (DOJ)

There are no reporting requirements to the Attorney General for consensual monitoring. However, the Department of Justice requires an agency to maintain the records of all consensual monitoring. The Investigative Support Division will maintain all the consensual monitors approved and conducted for three (3) years, per General Records Schedule 23.

## Non – Consensual Interception Table of Contents

	Page
Introduction .....	1
Types of Non-Consensual Interceptions .....	1
Preparing for a Non-Consensual Interception .....	2
Headquarters Notification on Submission of Application to Department of Justice (Notification Message) .....	2
Sample Headquarters Notification Official Message Reporting Submission of an Application to the Department of Justice .....	3
Types of Cases in Which Authorization May Be Granted .....	4
Overview of the Title I Application Process .....	4
Roving Interceptions .....	4
Applying for a Non-Consensual Interception .....	5
Exception .....	5
1) Affidavit .....	5
Details Relating to the Affiant .....	6
Details Relating to the Target Telephone Number(s) .....	6
Details Relating to Previous Application (ELSUR Check) .....	7
Details Relating to the Investigation .....	7
Details Relating to the Goals of the Investigation .....	8
Details Relating to Investigative Methods Already Utilized .....	8
Time Period for Interception .....	8
Privileged Communications .....	9
Interception of Foreign Language and/or Code(s) .....	9
2) Application .....	9
Details Relating to the Applicant .....	10
Details Relative to Previous Application (ELSUR Check) .....	10
Details of Any Requests for Extensions .....	10
Covert Entry .....	11
Persons Under Indictment or on Trial .....	11
Public Telephone Interceptions .....	11
Toll and Subscriber Information .....	11
3) Court Order .....	11
Authority to Issue a Court Order .....	12
Required Information .....	13
Dates of Implementation and Termination .....	13
Minimization .....	14
Covert Entry .....	14
Persons Under Indictment or on Trial .....	14
Interception of Foreign Language and/or Codes .....	14
Details Relating to the Target Telephone Numbers(s) .....	15
Public Telephone Interceptions .....	15
Toll and Subscriber Information .....	15
Periodic Reports by the Supervising Attorney .....	15
4) Authorization Request Letter From the Director or Designee .....	16
Department of Justice Approval .....	19
Headquarters Team Assistance .....	19
Application to the Court .....	20

Sealing of Documents .....	20
Procedures if the Application for an Interception Order is Denied .....	20
Emergency Interceptions .....	21
Preparing to Conduct the Interception .....	21
Staffing Requirements .....	22
Supervising Agent .....	22
Wire Room Shift Leader .....	23
Monitoring/Minimization Personnel .....	23
Technical Security Division (TSD) Personnel .....	24
Criminal Research Specialists (CRS) and Data Analysis .....	24
Transcribing Personnel .....	25
Surveillance Personnel .....	25
Other Investigative Tactics .....	25
Field Office Wire Room .....	26
Outside Wire Room .....	26
Conducting the Interception .....	27
Monitoring and Recording .....	27
Minimization .....	27
Extrinsic Minimization .....	28
Intrinsic Minimization (Spot Monitoring) .....	28
After-the-Fact Minimization .....	29
Foreign Languages .....	29
Public Telephones .....	29
Evidence of Other Crimes .....	29
New Targets .....	30
Privileged Communications .....	30
Minimization Memorandum .....	31
Sample of Minimization Memorandum .....	31
Disclosure of Intercepted Communications .....	36
Preliminary Meeting Held by Supervising Attorney (AUSA) .....	36
Posting the Court Order .....	37
Installation of the Interception Equipment .....	37
Pen Register .....	37
Personnel Access .....	38
Headquarters Notification After Interception is Initiated (Initiation Message) .....	38
Sample Official Message Reporting Initiation of a Non-Consensual Interception .....	39
Preparation and Logging of Recording of Intercepted Communication .....	40
Recording of Intercepted Communication .....	40
Procedure When No Recording Can Be Made .....	41
Disk Control Log .....	41
Consecutive Call Log .....	41
Interception of Electronic Communication .....	42
Transcripts .....	43
Termination of the Interception .....	44
Application for Extension of Interception .....	45
Final Headquarter Notification (Termination Message) .....	46
Sample Headquarters Notification Official Message for Reporting the Termination of a Non-Consensual Interception .....	47
Sealing and Custody of the Evidence Upon Termination of Interception .....	48
Inventory - Disclosure of the Wire Tap .....	48
Postponing of the Inventory - Disclosure of the Wiretap .....	48
Preparing the Inventory List for Disclosure of the Wiretap .....	49



Manual : Interception  
RO : ISD

Section : Chapter III  
Date : 03/01/2006

Record Retention .....	50
Indexing of the Targets in MCI .....	50
Reports to Department of Justice .....	50



# NON-CONSENSUAL INTERCEPTIONS

## Introduction

This chapter is intended to serve as an operational guide for all agent and technical personnel who engage in the conduct of non-consensual wire or oral communication interceptions. Although most of the non-consensual interceptions which are conducted by this Service are conducted pursuant to the provisions of Titles I and/or III of the Electronic Communications Privacy Act of 1986, as amended (18 U.S.C. 2510, et seq.), this Service may, on occasion, conduct non-consensual interceptions pursuant to the provisions of other statutes or executive orders which have a bearing on our protective responsibilities such as the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.) or Executive Order 12333.

Each of these other statutes or executive orders contains specific provisions for the conduct of communication interceptions. Because the intercept guidelines contained within these other statutes and executive orders are so diverse and so infrequently used by this Service, they are not addressed in this manual. All requests for authorization of communications intercepts which are subject to provisions of statutes or executive orders, other than Titles I and/or III, should be directed to the Intelligence Division. The Intelligence Division will contact the Investigative Support Division (ISD) in these cases to coordinate the conduct of these interceptions and to ensure statistical and record keeping functions.

Prior to preparing for any non-consensual interception, this chapter should be read in its entirety by all agents and supervisory agents who are to be responsible for preparation of the required documentation or who will directly oversee the actual interception operation. Because of the extremely sensitive nature of this type of interception, each employee is cautioned that any deviation from the policy and procedure set forth in this chapter may subject the employee to disciplinary action, to include dismissal, and may also expose the employee to criminal and/or civil liability.

## Types of Non-Consensual Interceptions

With the continual advancement of technology, non-consensual interceptions are no longer limited to standard hardwire telephones. They also apply to interceptions of cellular telephone communications, electronics communications (to include e-mail, faxes, internet and digital display pagers), and interception of dialed numbers using trap/trace devices and pen registers. These interceptions remain governed by all the laws, policies, and procedures set forth in this chapter.

## Preparing for a Non-Consensual Interception

Liaison with the Technical Security Division (TSD) and the Investigative Support Division (ISD) will be established as soon as the decision has been made to apply for a non-consensual interception. TSD will make all necessary coordination with the telephone service providers for the interception of both hard lines and cellular telephone systems. TSD will also determine what equipment will be required and acquire all equipment necessary to conduct the interception. The most up to date telecommunication interception equipment available and capable of intercepting oral communication and call data will be installed on all anticipated target telephone lines. Early installation of the interception equipment will also facilitate the initiation of the interception once it is authorized by the court. ISD will coordinate with the Electronic Surveillance Unit of the Department of Justice (DOJ) and assist the case agent with required ELSUR checks and preparation of Directorate authorization letter. ISD will also maintain a record of electronic interception.

In addition, liaison must be established with the Assistant United States Attorney (AUSA) who will supervise the interception. It is the responsibility of this Assistant United States Attorney to provide guidance in the composition and submission of the required affidavit, application, and court order; and to later provide supervision in the overall conduct of the interception.

## Headquarters Notification of Submission of Application to Department of Justice (Notification Message)

Once a decision is made to apply for a nonconsensual interception (to include interception over digital display pagers), telephone notification should be made to the Technical Security Division (TSD), appropriate operational division, and the Investigative Support Division (ISD). Upon submission of the application to the Department of Justice, an official message will be submitted to Headquarters under the case number of the investigation for which the interception is to be conducted.

The distribution of this official message will include the appropriate operational division, appropriate Assistant Directors office, Technical Security Division (TSD), and Investigative Support Division (ISD). The official message will reference the previous telephone communications between the case agent and Headquarters officials, notifying of the intent to submit an affidavit in support of a non-consensual interception. The following page has a sample official message for reporting the notification.

## Sample Headquarters Notification Official Message Reporting Submission of an Application to the Department of Justice

FROM: SAIC-FIELD OFFICE

CASE NUMBER:

CASE TITLE:

TO: SAIC-APPROPRIATE OPERATIONAL DIVISION

INFO: AD-APPROPRIATE ASSISTANT DIRECTORS OFFICE  
SAIC-INVESTIGATIVE SUPPORT DIVISION  
SAIC-TECHNICAL SECURITY DIVISION

SUBJECT: NOTIFICATION OF APPLICATION FOR A NON-CONSENSUAL INTERCEPTION

REFERENCE IS MADE THE TELEPHONE CONVERSATIONS BETWEEN SA \_\_\_\_\_ (APPROPRIATE FIELD OFFICE), AND SA \_\_\_\_\_ (APPROPRIATE OPERATIONAL DIVISION), AND SA \_\_\_\_\_ (ISD), AND SA (PSS) \_\_\_\_\_ (TSD), REGARDING THE INTENTION TO APPLY FOR A COURT ORDER TO CONDUCT A NON-CONSENSUAL INTERCEPTION.

THIS OFFICIAL MESSAGE IS TO SERVE AS NOTIFICATION THAT AN APPLICATION FOR A NON-CONSENSUAL INTERCEPTION HAS BEEN FORMALLY SUBMITTED TO THE DEPARTMENT OF JUSTICE, AS OF \_\_\_\_\_ (DATE OF SUBMISSION).

TECHNICAL SECURITY DIVISION IS REQUESTED TO PROVIDE EQUIPMENT AND NECESSARY TECHNICAL ASSISTANCE IN THE TITLE INVESTIGATION.

FIELD OFFICE

CASE SA/SUPERVISOR/SAIC



## Types of Cases in Which Authorization May Be Granted

Judicial authorization for a non-consensual interception may be granted if probable cause has been shown in the application and accompanying affidavit(s) that any of the offenses enumerated in 18 U.S.C. 2516 have been, are being, or will be committed.

It should be noted that the applicant's Federal agency must have responsibility for the investigation of the offense for which the application is made as outlined in Title 18, U.S.C., 2516 (1). Offenses not specifically assigned in legislation to another agency may be applied for by the U. S. Secret Service under the provisions of Title 18 U.S.C., Section 3056 (c) (1) (C). For example, this means that the U.S. Secret Service would not be allowed to apply for an interception for a violation of Section 831 pertaining to the prohibited transactions involving nuclear materials since we are not responsible for the investigation of those crimes.

## Overview of the Title I Application Process

The Title I application process begins with an affidavit prepared by the case agent. The affidavit will be reviewed by the AUSA and, based on the affidavit, the AUSA prepares an application for the court order (herein after "application") and a draft court order. The affidavit, application, and draft court order is forwarded to OEO/DOJ for review and approval by the AUSA handling the case. Once the affidavit, application, and draft court order is approved by OEO, ISD will submit a letter in support of the Title I, signed by the Assistant Director. OEO will then submit the documents to the attorney general or his/her designee with the recommendation for approval. Once the attorney general or his/her designee authorizes the Title I interception, OEO will forward the signed authorization to the AUSA in charge of the case. The case agent then will have the court order signed by a judge in the district where the Title I interception will take place.

"Spin off" applications on other subjects or facilities or telephone numbers are handled as separate requests and the process is the same as the initial request.

## Roving Interceptions

18 U.S.C. 2518 (11), (12) established the roving provisions under Title I of Electronic Crimes Privacy Act. These provisions permit the interception of oral, wire, or electronic communications of named subjects without requiring that a specific facility or premises be identified in advance of the authorization.

In the case of a roving oral interception, the application must establish, and the order must specifically find, that probable cause exists that a particular subject is committing a Title I offense at a location that is not practical to specify.

In the case of a roving wire or electronic interception, 18 U.S.C. 2518 (11) (b) (ii) requires probable cause showing that the actions of a named subject could have the effect of thwarting the reception from a specified facility. While the statute does not address the jurisdictional restrictions of roving interceptions, DOJ ruled that a roving interception is not trans-jurisdictional. An order must be obtained in each jurisdiction in which roving interceptions are to be conducted. The exception to this is in the case of mobile cellular telephones or vehicles that cross jurisdictional lines. Title 18, U.S.C. 2518 (3) permits extra-jurisdictional orders and interception. Consultation with an AUSA is advised when a roving interception is considered.

## Applying for a Non-Consensual Interception

There are several steps that must be followed in applying for an interception. Except for emergency authorizations, all of the following documentation must be completed and submitted to the Department of Justice, Office of Enforcement Operations, Electronic Surveillance Unit, through ISD, for review and approval prior to being presented to the presiding judge for approval and issuance of the court order:

- 1) Affidavit,
- 2) Application,
- 3) Court Order,
- 4) Authorization Request Letter from the Director or his/her designee.

Except for item 4, the Assistant United States Attorney who will supervise the interception should assist the case agent in the composition and submission of these documents.

For the sake of brevity, no sample affidavits, applications, or court orders are included in this manual. Copies of these may be obtained from ISD.

Application for interception of electronic communication and Pen Register and Trap and Trace orders capable of collecting Uniform Resources Locators (URLs) should be forwarded by the AUSA handling the case to the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division, Department of Justice.

### Exception

Prior DOJ approval is required for most applications to conduct interception of electronic communications. An exception was made for electronic communications intercepted over digital display pagers; applications involving digital display pagers may be authorized by an Assistant United States Attorney.

#### 1) Affidavit

The most important document which is submitted in support of a non-consensual interception is the affidavit. The preparation of the affidavit must be supervised by the Assistant United States Attorney who will oversee the interception. Once the affidavit has been completed, it will be reviewed by the AUSA supervising the interception and the Department of Justice Computer Crimes and Intellectual Property Section (CCIPS) if it involves interception of electronics communications. The affidavit will then be forwarded by the CCIPS or the AUSA reviewing the affidavit to Electronics Surveillance Unit (ESU) of the Office of Enforcement Operation (OEO) for review and revision.

The affidavit becomes, in reality, an integral part of the application, outlining the probable cause that has been developed which supports the application for a non-consensual intercept. Although the probable cause standard for a non-consensual intercept affidavit is technically the same as other search and seizure situations, the non-consensual intercept "warrant" is a much more sensitive judicial issue. Therefore, as a



general rule, the highest degree of specificity, consistent with the information available at the time the application is being made should characterize the affidavit. (There should be no tendency to allege only the minimum necessary to establish probable cause.)

Often times, there is a tendency to assert conclusions rather than facts in the affidavit. Therefore, care must be taken to avoid unsupported statements of opinion and conclusions, particularly where they relate to key facts. The source for each item of information in the affidavit should be specified. It is important to set forth underlying circumstances and the factors which give intrinsic reliability to the basic facts established by the affidavit.

The probable cause outlined in the affidavit is expected to be as current as possible. Generally, the Department of Justice expects the basic probable cause to be no more than 15 days old at the time the affidavit, application, and court order are submitted for Department of Justice approval. As is the case in other search and seizure situations, appropriate effort should be made in safeguarding the identity of any intelligence sources which are used for developing probable cause. Particular care should be accorded when establishing the reliability of informants and the accuracy of the information which they provide.

In preparing the affidavit, there are a number of issues which must be addressed and a number of questions which must be answered with specificity. Some of these issues and questions are addressed as follows:

## Details Relating to the Affiant

The following questions must be addressed:

- Is the affiant properly identified? (For joint investigations or task force situations, under the direction of the AUSA, the affiant may be a Secret Service agent or another law enforcement member of the task force or joint investigation).
- Is the affiant's authority as the investigating agent clearly outlined?
- A brief explanation as to the agent's experience with the Secret Service (or other law enforcement member); more specifically, his/her experience with the type of investigation for which the interception is being sought should be included.

## Details Relating to the Target Telephone Number(s)

The paragraph quoted below should always be included in the affidavit in the event the target might change his/her telephone number during the course of a non-consensual intercept. It should be placed just below the paragraph describing the target telephone number in the affidavit.

The paragraph to be included in the affidavit, application, and, ultimately, in the court order should read as follows:

"The authority given is intended to apply not only to the target telephone number listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding post utilized by the target telephone within the 30 day authorization period."

If the interception involves electronic communications (facsimile, Internet or electronic mail), consult the AUSA for the appropriate wording for the affidavit. Once the affidavit has been completed, it will be reviewed by the AUSA supervising the interception and by the Department of Justice Computer Crimes and Intellectual Property Section (CCIPS).

## Details Relative to Previous Application (ELSUR CHECK)

In accordance with 18 U.S.C. 2518(1) (e), the affidavit must contain a full and complete statement of any prior electronic surveillance involving the persons, facilities or locations specified in the application. Electronic Surveillance (ELSUR) checks will be conducted by the Investigative Support Division (ISD), at the request of the case agent. The case agent should contact ISD and provide the names of the potential targets of the interception along with all identifiers available, and all addresses and phone numbers. In joint investigations all participating agencies' indices should be checked by the case agent via their counterpart.

## Details Relating to the Investigation

The following questions must be addressed in the affidavit:

- Are the violations under investigation (specific statute citations), the person (s) to be intercepted, and the facilities or location to be tapped or bugged, clearly identified?
- Have all of the details of the investigation which contribute to the establishment of probable cause been specified?
- Have all sources of information been specified?
- Does the affiant explain the reliability of informants referred to and how these informants obtained their information?
- Is there a "particular description" of the conversations to be intercepted?

18 U.S.C. 2518(1) (b) requires the following:

"a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;"

Note: If any of the persons described who are likely to be intercepted are under indictment or being tried, or if the telephone to be tapped is a public telephone, it should be noted in the affidavit. These circumstances will probably require the court to make certain modifications to the court order. Therefore, their inclusion in the affidavit will alert the court to these situations.

## Details Relating to the Goals of the Investigations

The affidavit must clearly state the goals of the investigation and what results are expected through the use of the interception.

## Details Relating to Investigative Methods Already Utilized

The following questions must be addressed:

- Does the affidavit state with specificity what other investigative methods have been tried and failed, or are too dangerous to try? Included are methods such as the use of standard surveillance techniques, use of undercover agents or informants, execution of search warrants, use of immunity, etc.

18 U.S.C. 2518(1) (c) requires the following:

**"a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;"**

## Time Period for Interception

The affidavit must specify the period of time requested for the interception. 18 U.S.C. 2518(1) (d) requires the following:

**"a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;"**

In any event, an initial request for an interception under Title I cannot exceed 30 days. This is specified in 18 U.S.C. 2518(5) as follows:

**"No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of an extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a**

**provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."**

## **Privileged Communications**

The following questions must be addressed:

- Does the affidavit outline any expectations that privileged communication will be intercepted?
- If so, does the affidavit, through probable cause, justify such interception?

18 U.S.C. 2517(4) provides that:

**"No otherwise privileged wire, oral or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."**

## **Interception of Foreign Languages and/or Code(s)**

Information should be provided in the affidavit relating to any use by the target(s) of any codes or foreign languages. If the target(s) of the interception occasionally speak in a foreign language or code, and none of the monitoring agents understand the language, the coded or foreign language portion of such conversations may be monitored and recorded. Later, when a translator or decoding information is available, the conversations can be minimized (after-the-fact minimization). However, if most of the conversation is in a foreign language or code, and the monitoring agent understands the language or code, the entire conversation is subject to the rules of minimization. Additional reference should be made to 18 U.S.C. 2518 (5).

Such information should also be addressed in the preparation of the application and court order.

## **2) Application**

After the affidavit has been reviewed and approved by the supervising Assistant United States Attorney, he/she is responsible for the composition of the application.

Although 18 U.S.C. 2510(7) defines the various investigative or law enforcement officers who may technically make application for the interception, it is the policy of the Department of Justice that all such applications be filed with the court by the Assistant United States Attorney who will supervise the interception.

The application is nothing more than an affidavit by the Assistant United States Attorney. It addresses all of the issues which are addressed in the affidavit, albeit in synopsis form. When information from the affidavit is repeated in the application, the same language should be used whenever appropriate, in order to avoid misinterpretation, grammatical error, etc.

The application should specifically reference each supporting affidavit and each affidavit should be made an attachment to the application with these documents attached. If a required statement is inadvertently omitted from the application, this would not necessarily cause the application to be later rejected as an evidentiary document during judicial proceedings. There are a number of issues which are not addressed in the affidavit which must be addressed in the application. They are explained as follows.

## Details Relating to the Applicant

The following questions must be addressed:

- Is the Assistant United States Attorney making the application properly identified?
- Is his/her authority as a law enforcement officer clearly defined?

18 U.S.C. 2518(1) (a) requires that each application include the following:

**"the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;"**

The Officer authorizing the application is the Attorney General of the United States or his/her designee.

## Details Relative to Previous Application (ELSUR Check)

In accordance with 18 U.S.C. 2518(1) (e) the affidavit must contain a full and complete statement of any prior electronic surveillance (ELSUR) involving the persons, facilities or locations specified in the application. This statement should include the date, jurisdiction, and disposition of any previous applications; as well as their relevance, if any, to the on-going investigation. In addition to any known prior applications, the agency conducting the investigation should conduct an ELSUR check of its own electronic surveillance indices, indices of any other agency participating in this investigation, and the indices of any agency which may have investigated the subjects in the past.

It is only necessary to notify the court of prior applications involving interceptees, premises or facilities named in the present affidavit; persons who have been intercepted on a previous wiretap, but who were not named as interceptees in any court order need not be identified. If such circumstances exist, however, the court should be notified by the AUSA handling the case to avoid a later appellate issue.

## Details of Any Requests for Extensions

Whenever an extension order is being applied for in the application, specific details about results already obtained must be included.

18 U.S.C. 2518(1) (f) requires the following:

**"where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results."**

## **Covert Entry**

If accomplishment of the proposed interception will require surreptitious or covert entry, the application should so advise the court. This notification will allow the court to modify the court order to allow for covert entry.

## **Persons Under Indictment or on Trial**

If a probable interceptee is under indictment or on trial, this fact should be noted in the application. This notification will allow the court to modify the court order to allow for interception of this interceptee within prescribed guidelines. These guidelines are described in the COURT ORDER section of this manual chapter.

## **Public Telephone Interceptions**

If the telephone to be intercepted is a public telephone, this fact should be noted in the application. This notification will allow the court to modify the court order to allow for this kind of interception, within prescribed guidelines. These guidelines are described in the COURT ORDER section of this manual chapter.

## **Toll and Subscriber Information**

In order to save time during the conduct of the interception, it is recommended that a request for these records be made a part of the application.

## **3) Court Order**

After the Assistant United States Attorney has reviewed and approved the affidavit and completed the application, he/she is responsible for the composition of the "warrant" or court order which will be signed by the judge, authorizing the non-consensual interception.

Since much of the information which will be contained in the interception order has been included in the application, the same language should be used whenever appropriate in order to avoid misinterpretation, grammatical error, etc.



## Authority to Issue a Court Order

The authority which allows a judge to authorize a non-consensual intercept order is derived from 18 U.S.C. 2518(3) as follows:

"Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that -

- (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;
- (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
- (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
- (d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire or oral, communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."

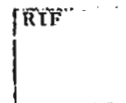
## Required Information

In preparing the court order, there are a number of issues which must be addressed and a number of questions which must be answered with specificity.

18 U.S.C. 2518(4) requires that the interception order contain the following information:

"Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify -

- (a) the identity of the person, if known, whose communications are to be intercepted;
- (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
- (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and



**(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained."**

18 U.S.C. 2518(4) also provides that, if needed, a court order can be issued compelling cooperation from communications common carriers, landlords, etc., ordering them to "...furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference...."

Pursuant to Title 18 U.S.C. 2522, an order may be issued to enforce the assistance capability and capacity requirement under the Communications Assistance for Law Enforcement Act (CALEA)

However, when this type of cooperation is provided for in the court order, efforts must be made to avoid possible breaches of security during the interception. The Department of Justice has concluded that there is no legal need for a communication common carrier, landlord, custodian or other person to be acquainted with the full details of the court order such as, the name(s) of the subject(s) to be intercepted, the violation(s) of law being investigated, etc., in order for them to furnish the necessary assistance. Therefore, in the interest of security, a separate abbreviated court order should be prepared and presented to the court in the applicable circumstances. A copy of this order may be left in the possession of the communication carrier.

## **Dates of Implementation and Termination**

Court Orders for interceptions are normally for thirty (30) days. Once the court order is signed, a ten (10) day grace period is allowed from the date the court order is signed until the actual interception begins. However, the interception should normally commence as soon as practical after the court order has been signed by the judge. For the actual thirty (30) day operational running time of the wire, and for reporting purposes, the start date is the date the actual interception begins, as long as it is within the ten (10) days after the order was signed.

As is mandated in 18 U.S.C. 2518(4) (e), the court order must contain the period of time for which the interception is authorized.

18 U.S.C. 2518(5) provides specific requirements relative to the dates of implementation and termination as follows:

**"No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communications for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days."**

**"...Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."**

## Minimization

18 U.S.C. 2518(5) states that the court order shall contain a provision that the authorization to intercept "...shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter..."

Minimization is discussed in detail later in this manual chapter.

## Covert Entry

If accomplishment of the interception requires surreptitious or covert entry, this fact should so be stated in both the application and court order. Neither the Electronic Communications Privacy Act of 1986 or the Fourth Amendment require that an interception order include a specific authorization to enter covertly the premises described in the order.

It is, however, the policy of the Department of Justice that such a provision be included in the order authorizing agent/technical personnel to enter the premises surreptitiously; install, maintain, place more effectively, and to remove the interception device at the expiration of the order. Once the initial entry has been accomplished pursuant to the court's order, it is not necessary to secure additional Department of Justice or court approval for subsequent entries in order to accomplish repositioning, maintenance, or removal.

## Persons Under Indictment or on Trial

If a probable interceptee is under indictment or on trial, this fact should be stated in both the application and court order. If this is the case, the interception order should contain restrictive language requiring particular care to avoid the monitoring of conversations pertinent to trial or other disposition of that case. Specific restrictions relative to attorney-client communications are provided later in this chapter.

## Interception of Foreign Languages and/or Codes

The interception of foreign languages and/or codes must also be addressed in the court order. If the target(s) of the interception occasionally speak in a foreign language or code, and none of the monitoring agents understand the language, the coded or foreign language portion of such conversations may be monitored and recorded. Later, when a translator or decoding information is available, the conversations can be minimized (after-the-fact minimization). However, if most of the conversation is in a foreign language or code, and the monitoring agent understands the language or code, the entire conversation is subject to the rules of minimization. Additional reference should be made to 18 USC 2518 (5).

## Details Relating to the Target Telephone Number(s)

The paragraph quoted below should always be included in the affidavit in the event the target might change his/her telephone number during the course of a non-consensual intercept. It should be placed just below the paragraph describing the target telephone number in the affidavit.

The paragraph to be included in the court order should read as follows:

"The authority given is intended to apply not only to the target telephone number listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding post utilized by the target telephone within the 30 day authorization period."

## Public Telephone Interceptions

If the telephone to be intercepted is a public telephone, this fact should be stated in both the application and court order. Where a public telephone is to be intercepted, the order should contain a provision to limit, insofar as practicable, monitoring activity to instances when the telephone is being used by those whose interception has been authorized. Physical surveillance of the telephone is usually necessary in this type of situation. Through the use of the surveillance, interception is limited to calls placed by, or to, the subjects.

## Toll and Subscriber Information

In order to save time during the conduct of the interception, it is recommended that a request for these records be made a part of the order. An example of this paragraph follows:

**IT IS FURTHER ORDERED**, pursuant to 18 U.S.C. 2703 (d), and upon request of the United States, that the \_\_\_\_\_ Telephone Company of \_\_\_\_\_ forthwith provide agents of the U. S. Secret Service, subscriber and toll information relative to this order.

## Periodic Reports by the Supervising Attorney

18 U.S.C. 2518(6) provides the following:

"Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require."

The statute does not make the filing of these reports mandatory unless the judge so directs in the authorization order. However, the Department of Justice takes the position that it is clearly in the interest of the Government to file these reports in order to demonstrate continuing judicial supervision over the

Interception. Accordingly, the supervising AUSA should, as a matter of course, recommend to the judge that the reporting requirement be included in any order which authorizes the interception of oral communications. The appropriate interval between reports depends upon what is reasonable under the facts of the case. The usual interval, however, is about ten (10) days. The AUSA may call upon the investigative case agent to assist in the preparation of the reports. The format of these reports is usually left to the discretion of the supervising Assistant United States Attorney.

#### **4) Authorization Request Letter From the Director or Designee**

During this process, the AUSA handling this non-consensual request will be in direct communication with the Department of Justice's Office of Enforcement Operations (OEO). The affidavit, application and court order (draft) will be reviewed and approved by the supervising AUSA and OEO. A copy of each of these documents must be forwarded by the USSS office involved in this application via e-mail, FAX or overnight package delivery service to ISD. Every effort should be made to expedite the submission of these documents, as the probable cause stated in the affidavit must remain current.

Once the documentation has been received, ISD will prepare a letter from the Director's office to the Attorney General, formally requesting authorization to apply for a court ordered interception.

After the formal request letter is prepared, ISD will obtain the signature of the Director or designee. The signed letter, along with the supporting documentation, will then be forwarded to the Electronics Surveillance Unit (ESU), Office of Enforcement Operations (OEO), Criminal Division, Department of Justice. OEO uses this letter as a signal that the Secret Service is in total agreement for the need to conduct this interception.

The following are examples of a formal request letter.

### Sample of Director's Formal Request Letter (Oral communication)

DATE: \_\_\_\_\_

File Number: \_\_\_\_\_

Name  
Assistant Attorney General  
Criminal Division  
U.S. Department of Justice

Dear \_\_\_\_\_,

This letter is submitted in support of an application for a court order authorizing the interception of wire communications on telephone number ( ) \_\_\_\_\_, subscribed in the name of \_\_\_\_\_, at the address of \_\_\_\_\_.

Based on information learned from the investigation, we believe the telephone number listed above is being used in connection with violations of Title 18, United States Code, Section \_\_\_\_\_, and possibly other crimes.

The investigation by this Service shows that the individual(s) identified in the affidavit have been and probably will continue to be involved in violations of the aforementioned sections of the United States Code.

Based on the facts documented in the attached affidavit, the Secret Service believes that the authorization for interception of wire communications will prove fruitful in identifying other co-conspirators, victims, and the manner in which the targets engage in criminal activity.

Sincerely,

\_\_\_\_\_  
Director  
United States Secret Service



## Sample of Director's Formal Request Letter (Electronic Communication)

Date: \_\_\_\_\_

File Number: \_\_\_\_\_

Name  
Assistant Attorney General  
Criminal Division  
U.S. Department of Justice

Dear \_\_\_\_\_,

Attached herewith are copies of the affidavit, application, and draft court order prepared in support of an application for a court order authorizing the interception of electronic communications to and from the Internet Protocol address block of xxx.xxx.xxx, with the usable IP address range xxx.xxx.xxx through xxx.xxx.xxx, which presently resolves to a (Name of network or website hosting the IP addresses), located at (address) on the following individuals:

Bob Doe (a/k/a "BDoe"); Jane Doe (a/k/a "Jane"); Roy Jones (a/k/a "RJ"); Peter Parker (a/k/a "Spiderman"), and others yet to be identified.

As the affidavit makes clear, the aforementioned subjects are utilizing a (Name of net work or web site) and are being hosted at (Name of the communication company). There is probable cause to believe that the subjects have committed, are committing, and will continue to commit felony identification document offenses, felony access device offenses, and felony computer crime offenses in violation of Title 18, United States Code Sections \_\_\_\_\_. Based on the facts documented in the attached affidavit, the Secret Service believes that the authorization for interception of electronic communications will prove fruitful in identifying other co-conspirators, victims, and the manner in which the targets engage in criminal activity.

Sincerely,

\_\_\_\_\_  
Director  
United States Secret Service

## Department of Justice Approval

After the affidavit(s), application and court order have been reviewed by the Office of Enforcement Operations, a recommendation of either approval or rejection will be made to the Deputy Attorney General, Associate Attorney General or a designated Assistant Attorney General. If the request for authorization is approved, the approving official will send a formal approval letter, authorizing the submission of the application for the interception to the United States Attorney in the District where application is to be made. The AUSA supervising the Title I should contact the affiant (the case agent) once the request is approved.

When the letter of approval is received by the AUSA, the case agent will obtain a copy of this letter and will forward the letter to ISD for inclusion in the non-consensual Intercept file maintained within the Investigative Support Division (ISD). If the Office of Enforcement Operations rejects the request for authorization, this Service and the supervising AUSA authorizing the application will be notified of the reasons for the rejection and advised of what measures need to be taken in order to reapply for the interception.

## Headquarters Team Assistance

After the application is submitted to Headquarters, and pending approval from DOJ Office of Enforcement Operations, a team comprised of the following personnel will travel to the field office involved to coordinate the administrative requirements and future conduct of the interception:

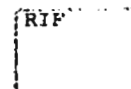
**Representatives from the Investigative Support Division (ISD)** will meet with the supervisory agents and the case agent of the office handling the interception concerning the manual requirements, minimization, and wire room restrictions for the interception operation. If requested, ISD will assist the case agent in preparing his or her portion of the briefing for the interception.

**Representatives from the appropriate operational division** will be responsible for meeting with the SAIC, case agent and the Assistant United States Attorney, as necessary, to go over any questions raised during the review of the affidavits, application, and court order. They will also meet with the case agent and office supervisory personnel to identify and resolve surveillance and wire room manpower requirements, costs, and other case related issues.

**Representatives from the Technical Security Division (TSD)** will coordinate with the local telephone company to review the technical aspects of the interception. TSD will determine a suitable site and additional equipment requirements. The type of intercept will dictate the equipment needs (i.e. phone, cellular phone, fax, e-mail).

This team assists the case agent in the details of planning the intercept and bringing to the site the necessary personnel and equipment without the case agent specifically requesting them.

After the Department of Justice has approved the interception and the court order is expected to be signed, this team may travel again to the office to assist in setting up the wire room and attend the minimization briefing given by the AUSA. The case agent needs to prepare the case briefing, specific agent assignments, and administrative data (scheduling, hotel information, etc.).





The minimization briefing must be attended by all interception personnel, including surveillance agents and field office administrative support. If wire room personnel must be replaced after the briefing due to exigent circumstances, the replacements must receive a similar briefing.

Once the wire room personnel have been briefed and are confident that all procedures and the conduct of the intercept comply with DOJ and Secret Service policy, the ISD representatives will return to Washington, DC.

ISD representatives will continue to monitor the progress of the intercept and be available to answer questions and give advice to the case agent and the wire room supervisor. If necessary, the ISD representatives can return to provide on-site assistance.

## **Application to the Court**

After the Department of Justice has formally approved the application for authorization of the interception, the supervising Assistant United States Attorney will submit the application to a judge having jurisdiction within the district where the interception is to take place. The application should be presented as expeditiously as possible following the receipt of authorization.

Although interception orders may be granted by judges of a United States District Court or judges of the United States Courts of Appeals, the Department of Justice mandates that, except in extraordinary circumstances, all applications should be presented to a District Court Judge. The documents to be presented to the judge include the originals and one (1) copy each of the affidavit(s), application(s), court order(s) (draft), and Department of Justice authorization letter.

## **Sealing of Documents**

If a court order is granted, the court or the supervising Assistant United States Attorney, in the court's presence, will seal the court order along with all related documents. The usual practice is either to file the sealed package with the District Court Clerk for safekeeping in the clerk's vault, or for the supervising Assistant United States Attorney to retain custody of the sealed documents until the interception has been completed, at which time they will be filed with the court.

A copy of the documents may be kept by the supervising Assistant United States Attorney. Each district may vary as to "sealing" procedures. Questions as to the proper procedure should be directed to the appropriate official in the U. S. District Court Clerk's office.

## **Procedure if the Application for an Interception Order is Denied**

If the court refuses to issue an interception order, the appropriate Assistant Director's office must immediately be notified of the reasons for this rejection. The supervising Assistant United States Attorney will immediately notify the Office of Enforcement Operations. That office will determine whether a new application can or should be made based on the facts immediately available, or whether additional investigation is needed.

## Emergency Interceptions

18 U.S.C. 2518(7) provides for the interception of communications for up to 48 hours, without a prior court order, under certain emergency conditions. However, that section also provides that an application for a court order approving the interception must be made within 48 hours after the interception has begun.

The Attorney General, Deputy Attorney General, and Associate Attorney General all have the power to authorize emergency interceptions. This emergency provision does not dispense with any of the application procedures prescribed under 18 U.S.C. 2518(1). It merely delays the application process for 48 hours. The Director or his/her designee must obtain oral authorization and submit a written request for the emergency interception. This request must identify the persons to be intercepted, the facilities from which, or the place where, the wire or oral communications are to be intercepted, and the offenses that are expected to be related to these interceptions.

Furthermore, 18 U.S.C. 2518(7) requires that the request letter specifically explain the justification for an emergency interception. 18 U.S.C. 2518(7) (a) clearly sets forth the definition of an "emergency situation" that will warrant an interception without first obtaining a court order. Emergency situations include those which involve conspiratorial activities which threaten the national security interest or which are characteristic of organized crime or any offense that involves immediate danger of death or serious physical injury.

The request should be accompanied by documentation setting forth probable cause that:

- (1) An individual is committing, has committed, or is about to commit a particular offense enumerated in 18 U.S.C. 2516;
- (2) That particular communications concerning the offense cited will be obtained through such interception;
- (3) That the facilities from which, or the place where, the wire or oral communications are to be intercepted, are being used, or are about to be used, in connection with the commission of such offense.

Explicit guidelines for the conduct of an emergency interception are set forth in 18 U.S.C. 2518(7). Whenever an emergency interception is being contemplated, the Assistant United States Attorney who would supervise such an interception should immediately contact the Office of Enforcement Operations (OEO) for guidance and advice. In practice, the emergency procedures are initiated when the AUSA in charge of the case contacts an Electronic Surveillance Unit (ESU) attorney at OEO. At the same time, the case agent should contact the Investigative Support Division (ISD) and the appropriate operational division. After discussions with the AUSA, the ESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements for the emergency interception have been met. Once approved, the ESU attorney notifies the AUSA supervising the case.

The Director or his/her designee (OEO) then contacts the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (AAG) to seek permission and to make a determination that an emergency situation exists as defined in the statute.

## Preparing to Conduct the Interception

After a judge has issued the interception "warrant", 18 U.S.C. 2518(5) requires that the authorization to intercept be executed as soon as practicable. If all of the preparatory procedures which have thus far been

outlined in this chapter have been followed, execution of the interception "warrant" can begin as soon as it is issued.

Prior to conducting any interception, all Secret Service employees and other law enforcement personnel participating in the interception must read and understand this chapter, minimization memorandum, affidavit, application and court order. The guidelines contained in this chapter have been designed to assure strict adherence to the laws and procedures which govern the use of these interceptions.

It is the philosophy of the Secret Service that it is preferable to err on the side of caution rather than risk any inadvertent violation of law or established procedure when conducting these interceptions.

## Staffing Requirements

Non-consensual interceptions are sensitive in nature, and, as such, require great care in their execution. The USSS field supervisor overseeing the interception should insure that staffing is properly allocated and utilized during the operation. Staffing may include personnel from other law enforcement agencies who are task force or joint investigation participants. Whenever possible, eight hour shifts should be utilized during the operation. However, twelve hour shifts may be acceptable depending on the volume of calls and activity anticipated and the availability of manpower.

## Supervising Agent

The Supervising Agent ("Wire Room Supervisor") normally is the liaison between the supervising Assistant United States Attorney (AUSA) and the monitoring agents. This insures that instructions from the AUSA are properly communicated to the monitoring agents and that the supervising attorney receives an accurate overview of what the interception is producing.

The Supervising Agent is also charged with the responsibility of conducting the interception in compliance with all instructions of the court and the supervising AUSA and insuring that the interception devices are installed as soon as practical after the court order is obtained.

The Supervising Agent will also insure that information gained from the interception is communicated, in a timely manner, to the case agent and surveillance personnel.

The Supervising Agent will be responsible for the chairing of daily meetings involving key interception personnel, providing timely distribution of information and updating operational instructions.

The Supervising Agent should prepare and deliver to the supervising AUSA daily written reports. Copies of these reports should be made for the case agent. There is no prescribed format for such reports, but they should show the nature and scope of the interception for that day. For instance, they should indicate the number of pertinent (relevant) conversations intercepted, the number of non-pertinent conversations minimized, whether any of the targets named in the order were intercepted, whether any new targets were identified, and whether any problems have arisen (e.g. equipment malfunction, privileged communications, or evidence of other crimes).

These daily reports should be made even throughout a weekend or holiday period and may initially be accomplished via telephone with the documentation being prepared the next working day. A copy of the corresponding day's consecutive call log should accompany each report. The Supervising Agent's duties include providing for the overall integrity of the interception as well as the integrity and admissibility of the evidence obtained by following the principles and guidelines set forth within this manual.

The Supervising Agent should insure that the interception is properly terminated at the time specified in the court order, or when the objective of the interception has been accomplished, whichever comes first. The Supervising Agent is responsible for the operation and will coordinate all external surveillance activity with the surveilling agents. It is important that he/she have an overview of the entire investigation and be able to confirm voice identifications, identify patterns of involvement and generally maximize the effectiveness of the interception.

Since the Supervising Agent's primary purpose is to insure the integrity of the interception operation, he/she will not be the case agent for the investigation for which the interception is conducted. (The case agent cannot properly devote the time and attention required during the execution of the interception.) Whenever possible, only one Supervising Agent should be assigned to the interception. However, more than one may be assigned during very active interception operations.

## Wire Room Shift Leader

The Wire Room Shift Leader will be a senior Special Agent who is familiar with the entire investigation. He/she will supervise wire room activities, monitor personnel, and ensure the integrity and security of the wire room during their particular tour of duty. The Shift Leader will maintain liaison with the Supervising Agent and TSD support personnel, who will maintain the integrity of the equipment under their supervision. In the absence of a Supervising Agent (i.e. midnight shift), the Shift Leader will assume the responsibilities of the Supervising Agent in notifying the supervising AUSA, case agent and surveillance personnel of relevant information when necessary. The Shift Leader will keep the monitoring personnel apprised of any significant developments in the case that may affect the monitoring of the interception.

## Monitoring/Minimization Personnel

The personnel (normally Special Agents) assigned to the actual interception, monitoring, and recording of conversations are in the most sensitive position of the interception operation. They must adhere carefully to the minimization guidelines set forth in the court order and by the supervising AUSA. The monitoring personnel must be accurate in the recording of all information in the Consecutive Call Log which they will maintain. They are not to discuss the content or context of any of the calls monitored with any individual (including agents or other personnel) who do not have a specific need to know.

Prior to assuming their monitoring duties, all monitoring personnel must listen to any recordings made earlier during the investigation in order to familiarize themselves with the voices of the targets intercepted during those conversations. Separate monitoring personnel must be assigned to each target telephone line; if any target telephone line is deemed to be extremely busy, then two people should be assigned to monitor that line.

In the case of interception of electronic communications, monitoring personnel requirements vary depending on number of Internet Protocol (IP) addresses intercepted. However, one minimization employee should be assigned per one Internet Protocol (IP) address. See the Interception of Electronic Communication section of this chapter for additional information, page 44).

## Technical Security Division (TSD) Personnel

In most cases, Technical Security Division (TSD) personnel will be responsible for obtaining the necessary technical information and equipment needed to accomplish the interception. TSD will also secure and establish the monitoring area in conjunction with the Supervising Agent and Shift Leader(s).

The only persons who are authorized to install and test interception and recording equipment are TSD specialists (Telecommunication and Security Specialist, or Special Agent). TSD personnel will be readily available at any time during the interception in order to respond to technical problems which may arise.

In the case of interception of electronic communications, ECSAP trained Special Agents may install, maintain and test interception and recording equipment in coordination with the TSD personnel.

In addition, TSD will make all necessary coordination with the telephone or internet service provider and equipment manufacturers to obtain necessary equipment for telephone (hard line and wireless) and electronic communication interception. The most up to date telecommunication interception equipment available and capable of intercepting oral communication and call data will be installed on all anticipated target telephone lines.

The TSD representative should coordinate his/her activities with the case agent or other designated agent personnel to provide the necessary information for the issuance of judiciary subpoenas requesting subscriber and other telephone information.

To preclude obtaining a subpoena each and every time subscriber information, or other information, is needed from the telephone company; the court in the original non-consensual interception order can direct the telephone company to provide this information as needed by this Service.

TSD personnel should never be used for monitoring, nor should they be used for any other function normally assigned to a Special Agent.

## Criminal Research Specialists (CRS) and Data Analysis

CRS personnel from ISD will be assigned to accomplish the required database searches and telephone toll link analysis as necessary using analytical software.

The number of CRS personnel assigned to the interception will depend on the volume of calls and activity anticipated during the interception. However, in most cases, it may be appropriate to assign at least one CRS who has been trained in the call data and telephone toll link analysis requirements and capabilities of PenLink, as well as other computer programs. Prior to the initiation of the interception, vital aspects of these applications will be discussed with the Wire Room Supervisor and case agent in accordance with the U.S. Secret Service guidelines for standardization of software.

For utilization of CRS support in an interception the SAIC - ISD must be contacted. For specific information regarding the Criminal Research Specialist Program, see the Investigative Manual, ISD-19.

RIP

## Transcribing Personnel

One of the most critical elements of the interception is the transcription of intercepted conversations. In order to effectively transcribe these conversations, the transcribers should have a thorough knowledge of the investigation, the targets involved, and the violations of law under investigation. Administrative support personnel may be used to type the transcribed conversations, but agent personnel must thoroughly review the transcription.

In cases where intercepted conversations are conducted in a foreign language, language specialists from other agencies or approved private contractors may be used to aid in monitoring the calls and transcribing them into English.

The amount of transcription during the interception will depend on the guidelines set forth by the supervising AUSA and the needs of the supervisory and case agents.

## Surveillance Personnel

Whenever possible, visual surveillance should be conducted in conjunction with the interception. Incriminating conversations, obtained from the interception, will have a greater impact during presentation at trial if it is corroborated by testimony from surveillance agents, or joint investigation/task force members, confirming that the target(s) were at a certain location or attended a certain meeting when an interception was made.

Surveillances conducted in conjunction with the interception will often provide a better overview of the target's involvement in the violation of law under investigation and may provide additional probable cause for court ordered extensions of interceptions. The use of surveillances may develop very valuable investigative leads and advance knowledge of target actions.

The number of surveillance agents required during the interception operation will depend on the number of targets involved, the number of target telephones, the violations of law under investigation, etc. In any case, the use of surveillance agents requires close communication and liaison with the Supervising Agent (Wire Room Supervisor) and the case agent.

## Other Investigative Tactics

In an ideal situation, pertinent conversations will be intercepted as soon as the interception operation begins. However, in many cases extensive monitoring takes place before pertinent and/or incriminating conversations are recorded. In these situations, it may be possible to induce the targets to discuss the violation of law under investigation.

These inducements can be accomplished in a number of ways. If the investigation involves the use of an undercover agent or confidential informant, the agent or informant may be used to generate conversations between targets by placing calls to these targets, thereby making inquiries about the illegal activity under investigation. The undercover agent or confidential informant may very well be in a position to place "orders" for contraband, thereby inducing the targets to engage in incriminating conversations.

Interviews of targets, or friends or associates of targets, conducted by agents may also induce conversations between the targets. If the targets believe that arrests are imminent, or that inquiries are being made about the violations of law under investigation, these targets may very well participate in pertinent and/or incriminating conversations.

The innovative investigator can utilize a myriad of investigative tactics designed to maximize the effectiveness of the interception, and this innovation is certainly encouraged. However, before any of these tactics are employed, their use should be approved by the supervising AUSA, and closely coordinated with the supervising agent and case agent.

## Field Office Wire Room

In most cases, and whenever possible, the interception operation will be established within a field office through acquisition of a leased (dedicated) telephone line(s) which is connected to the circuit utilized by the target telephone(s). The Investigative Support Branch of TSD should be consulted to ensure the most cost effective method of line installation.

The interception and recording equipment must be installed and secured within a room in the field office which can be separately secured and which will not be accessed by personnel who are not directly involved with the interception operation. As soon as the monitoring station is capable of becoming operational, i. e., the leased line(s) have been installed and is active and the interception and recording equipment is on site, the monitoring station should be considered secure and accessible to only authorized personnel who are directly involved with the interception.

At this time, a Personnel Access Log (SSF 3285A) must be posted and maintained at the entrance to the monitoring station. All persons who access the wire room must make the appropriate entries in the log each and every time they enter or exit. The Supervising Agent and/or Shift Leader have the responsibility to ensure that these procedures are adhered to by all personnel.

**Note:** Should the wire room be protected by an electronic access system, the use of the Personnel Access Log can be suspended in lieu of a computerized printout.

The Personnel Access Log (SSF 3285A) can be found via the USSS Forms Library at Intranet address <http://ssweb/mno/pars/forms>.

## Outside Wire Room

If circumstances prevent establishing a wire room within a field office, it is necessary to obtain a suitable site at an outside location. Twenty-four (24) hour security coverage will be placed on the wire room as soon as it is capable of becoming operational, i.e., the leased lines has been installed and is active and the interception and recording equipment is on site. At this time, the personnel operating the wire room will begin to maintain a "Personnel Access Log."

If the location of the wire room normally allows access by "outside" personnel (hotel room maids, etc.), arrangements should be made to deny them access to the wire room.

## Conducting the Interception

### Monitoring and Recording

The law makes no distinction between "listening to", "monitoring," or "recording" a conversation. Courts generally regard an interception order in the same light as any other warrant; it authorizes a limited "search" and limited "seizure" of evidence. Whether a conversation is merely overheard, or if it has been recorded, makes no difference legally; it has been seized.

### Minimization

One of the most critical issues relative to a court ordered interception pursuant to Title I is the issue of minimization. 18 U.S.C. 2518(5) requires that every court ordered interception must "contain a provision that the authorization to intercept...shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception..." This provision requires that the interception procedures be conducted in such a way so as to include the smallest possible number of interceptions of "innocent" communications.

In this context, the word "possible" means feasible or practicable consistent with the objective of obtaining evidence of the criminal activity described in the interception order. In a normal situation, some interception must take place before it can be determined that the interception of the communication should be interrupted. It is difficult to establish set rules in this area, for there appears to be an exception to every truism concerning minimization.

As a guiding principle, problems relating to minimization must be dealt with on an ad hoc basis, and monitoring personnel must be provided with instructions by the supervising AUSA as the interception operation progresses. The minimization process should be monitored closely by the Wire Room Shift Leader to ensure continuity. The character of the criminal enterprise, i.e., the nature of the activity, its complexity and size, its geographical reach, and similar considerations all bear on the conduct of an interception.

The purpose of the investigation may be a critical factor in determining the authorized scope of the interception. Where an objective of the interception is to define the scope of criminal activity, or to identify unknown conspirators, or to obtain information on the operation of an illegal enterprise, the parameters of interception are much broader than when an interception is instituted for a narrow, limited purpose.

If, however, the expected content of the communications to be intercepted is narrow in scope, efforts should be made to minimize accordingly. For example, if, at the time of the initiation of the interception, the monitoring personnel know all the targets who are suspected of the criminal offense, they can tailor their minimization efforts to avoid monitoring incoming or outgoing calls involving other persons. Similarly, if the monitoring personnel know during what time of day the telephone will be used for criminal activity, they can avoid intercepting calls at other times.

Such considerations affect the initial minimization tactics employed during the investigation, but the interception policy may be changed to conform with investigative requirements as the interception continues. On the other hand, where the monitoring agents do not, at the outset, have reason to believe that any identifiable group of calls will be innocent, it may be reasonable to monitor all calls until a pattern of innocent



calls develops. Such a pattern may not always be identifiable because it is often impossible to determine that a particular conversation would be irrelevant and innocent until it has been concluded.

The use of code words, cover-up jargon, or other evasive tactics makes investigation difficult and necessitates more detailed and extensive monitoring of conversations. Accordingly, the interception of all telephone communications for such time as is appropriate where evasive tactics are used does not constitute a failure to minimize.

In analyzing the overall interception, the courts have said that telephone conversations of brief duration do not permit monitoring personnel sufficient opportunity to identify the caller and characterize the conversation. Interceptions of conversations completed in less than two (2) minutes cannot be considered unreasonable. Moreover, calls between known co-conspirators may be monitored in their entirety since relevant information may emerge at any point in a call.

Where one of the parties is a known conspirator, the monitoring of his/her conversations may be more extensive than if he/she were not suspected, at least during the early phases of the interception; by listening to such calls, monitoring personnel can effect the screening of unknown parties. The interception of communications of suspected conspirators is similarly appropriate until their complicity can be determined.

The courts have endorsed a variety of methods which may be employed when attempting to "minimize" interceptions. The methods which would most likely be employed by this Service fall into three categories: extrinsic, intrinsic and after-the-fact minimization. Each approach to minimization involves different procedures; however, more than one approach may be employed during an interception operation.

## **Extrinsic Minimization**

Extrinsic minimization involves limiting the time period during which monitoring is conducted. Although a judge may issue a non-consensual interception order for an effective period of up to thirty days, most orders are effective for only fifteen or twenty days. This is one example of extrinsic minimization.

A second example of extrinsic minimization is the termination of interceptions before the expiration of the court order. A third example would be a situation where monitoring is restricted to certain hours each day, depending on the type of violations involved and the circumstances in the case.

## **Intrinsic Minimization (Spot Monitoring)**

Intrinsic minimization (or "spot monitoring") is the most common method of minimization used during voice interceptions. It involves the screening of all conversations as they are taking place. This method requires the monitoring personnel to make a reasonable, good-faith effort to avoid either listening to or recording non-pertinent conversations.

Monitoring personnel must be permitted a reasonable amount of flexibility to guard against the possibility that a conversation which appears non-pertinent at first may later become pertinent, involving discussions of violations cited within the court order. Spot monitoring is a method which provides the monitoring agents with this flexibility.

If the monitoring personnel listen to the first part of a conversation and cannot determine with certainty that it is either pertinent or non-pertinent, the monitor should deactivate the listening and recording devices. Periodically thereafter, the monitor should reactivate the listening and recording devices for brief periods until the nature of the conversation and/or the identity of the subject can be verified.

## After-the-Fact Minimization

After-the-fact minimization for an audio interception involves recording every conversation and then restricting disclosure of non-pertinent conversations by transcribing or re-recording only pertinent conversations and then sealing the original tapes. Except under extraordinary circumstances, and then under the strict supervision of the supervising AUSA, this method of minimization for an audio intercept will not be employed by this Service. (Foreign language minimization is covered in the section below.)

In the instance of interception of electronic communications (fax, internet, e-mail, and online instant chat), after-the-fact minimization has to be the method utilized. This will involve intercepting and reading all of the fax or email transmissions and then determining which are pertinent or non-pertinent. The supervising AUSA will provide guidance when using this type of minimization.

## Foreign Languages

If the targets of the interception occasionally speak in a foreign language, and none of the monitoring personnel understand the language, the foreign language portion of such conversations may be monitored and recorded. Later, when a translator is available, the conversations can be minimized (after-the-fact minimization). However, if most of the conversation is in a foreign language, and monitoring personnel understand the language, the entire conversation is subject to the rules of minimization. Seek the guidance of the supervising AUSA when using this type of after-the-fact minimization.

## Public Telephones

If the target telephone is accessible to the general public, as well as to the targets of the interception, the monitoring personnel must avoid interceptions of individuals who are not included in the court order, i.e., members of the general public. This can most easily be accomplished through a visual surveillance of the target telephone. The surveillance personnel can notify monitoring personnel when a target utilizes the target telephone.

If surveillance cannot be accomplished, the monitoring personnel should monitor conversations only when the voices are recognized as those of the targets or suspects or when the dialed telephone numbers are recognized as suspect.

## Evidence of Other Crimes

If the monitoring personnel overhear conversations which apparently relate to crimes which are not enumerated in the court order, they should continue to intercept and record this type of call as though these crimes were included in the court order. However, these newly developed crimes and the interceptions relating to them should be reported to the supervising AUSA as soon as possible, but not later than the next day.

The supervising AUSA will then make a determination as to whether the intercepted conversations may be evidence of a crime not listed in the court order. If so, the supervising judge will be informed by the supervising AUSA.

## New Targets

One of the stated and authorized purposes of the interception is to identify additional targets in the investigation who have not been named in the court order. Whenever any such individual is identified by name, nickname, telephone number, etc., the supervising AUSA should be notified immediately. He will then notify the court and a determination will be made as to whether or not an amendment to the court order is required.

## Privileged Communications

One of the primary objectives of authorized interceptions of private communications is to provide the investigative agency with legally admissible evidence of criminal activity which could not be obtained through normal investigative techniques. However, the confidentiality of conversations between individuals who stand in the relationship of husband - wife, clergyman - parishioner, physician - patient, and attorney - client are protected by testimonial privilege.

Accordingly, 18 U.S.C. 2517(4) states as follows:

**"No otherwise privileged wire, oral or electronic communications intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."**

If an intercepted communication would be otherwise privileged, it cannot be introduced as evidence. Whenever monitoring personnel become aware that the conversation being monitored is privileged, they should immediately deactivate the listening and recording devices and, as soon as practicable, notify the Wire Room Shift Leader and the supervising AUSA of the interception.

Whenever privileged communications are partially intercepted, the monitoring personnel must indicate this fact in the Consecutive Call Log. A more serious situation is presented when the conversations overheard by monitoring personnel are between the target and his/her attorney (or vice versa). In this instance, the confidential communication is not only protected by a testimonial privilege, but also by the Sixth Amendment's guarantee of the individual's right to the assistance of counsel.

If the intercepted communications deal with legal advice given by the attorney to the client concerning a pending criminal case, then care must be taken not to violate the client's Sixth Amendment rights. In the event that monitoring personnel intercept a communication between an attorney and client concerning a pending criminal case (i.e., a case in which the client is under indictment), the monitoring personnel must immediately deactivate the monitoring and recording equipment and make a notation in the Consecutive Call Log that the conversation was partially intercepted and was not completely overheard. The entries in the log should identify the attorney and the client who were intercepted.

In rare instances, this Service may be authorized to intercept the conversations of a target and his/her attorney after an indictment has been returned against the target. However, great care must be exercised by the supervising AUSA that pending cases against a target are not needlessly jeopardized in order to further potential cases.

In the event the electronic surveillance intercepts a communication between an attorney and client relating to matters other than a pending criminal case (e.g., a conversation in relation to an illegal activity), the monitoring personnel should, at the earliest practicable moment, bring this fact to the attention of the Wire Room Supervisor and the supervising AUSA. Upon being informed of the circumstances and content of the conversation, the supervising AUSA must decide if the conversation is, in fact, privileged.

If that determination is made, the supervising AUSA should instruct this Service not to disclose the content of the privileged communication to other investigative or police agencies, or conduct further investigation based upon the contents of the privileged communication. Such privileged conversations should not be included in the copies of transcriptions of the tapes, but should be recorded on the sealed copy that will remain in the custody of the court.

## Minimization Memorandum

The issue of minimization is one of the most critical issues relative to a court ordered interception conducted under Title I. For this reason, Secret Service policy requires that all personnel, who are to be responsible in any way for the conduct of the interception, read and initial a memorandum which outlines the issues involved with minimization prior to conducting the interception. In most cases, this memorandum will be authored by the supervising AUSA; if, however, the supervising AUSA is not the author, it will be the responsibility of the Supervising Agent to author the memorandum.

In addition to reading this minimization memorandum, all interception personnel will be responsible for reading the court order, application, and affidavit supporting the interception.

The following pages contain a sample minimization memorandum which addresses all of the issues that must be understood by all participating personnel prior to conducting the interception. **Note:** An after-the-fact minimization memorandum may differ in content at the discretion of the AUSA.

## Sample of Minimization Memorandum

<p>MEMORANDUM</p> <p>DATE: _____</p> <p>FROM: _____</p> <p>United States Attorney By: _____ Assistant United States Attorney</p> <p>SUBJECT: Minimization of Interceptions</p> <p>TO: All Supervisory and Monitoring Agents and other personnel of the U.S. Secret Service Participating in the Interception of Wire Communications, to and from Telephone Number(s)</p> <p><b>IMPORTANT:</b> This memorandum and the attached court order, application, and affidavit must be posted within the listening post and said items shall be read in their entirety by all supervisory and monitoring agents participating in any interception prior to such participation. The attached Review Log must be signed and dated acknowledging same. <b>YOU MUST NOT PARTICIPATE IN ANY MONITORING UNTIL ALL OF THE ABOVE LISTED ITEMS HAVE BEEN READ AND UNTIL YOU ARE TOTALLY FAMILIAR WITH THE FEDERAL VIOLATIONS ENUMERATED IN THE COURT ORDER.</b></p> <p>Your objective is to execute the court order, recording only those conversations which are specifically designated, and minimizing the interception of non-pertinent or privileged communications.</p> <p><b>I. LEGALLY THERE IS NO DIFFERENCE BETWEEN "MONITORING" AND "RECORDING"</b></p> <p>The law makes no distinction between "LISTENING," "MONITORING," or "RECORDING" a conversation. Courts generally regard a wire interception like any other search warrant: It authorizes a limited "search," and limited "seizure" of evidence. Whether a conversation is merely overheard or also recorded makes no difference legally; it has been seized.</p> <p>If you "seize" everything that is intercepted, the fruits of your investigation are likely to be suppressed. We have to establish that we neither LISTENED to nor RECORDED conversations we had no right to overhear. We have to establish that we are making and have made a reasonable effort to stay within the legal limits of the court order.</p>
---

## Sample of Minimization Memorandum (page 2)

### II. CONVERSATIONS WHICH MAY BE LISTENED TO

We have authority to intercept telephone conversations of \_\_\_\_\_ a/k/a \_\_\_\_\_ and \_\_\_\_\_ (list all targets) and others yet unknown concerning violations of Title 18, United States Code, Sections \_\_\_\_\_ and \_\_\_\_\_. (List all violations cited in court order). Any interception of a non-enumerated offense must be brought to my attention (supervising Assistant United States Attorney) through the Supervising Agent immediately.

Listen to the beginning of each conversation for only a period of time as is necessary to determine the parties and the nature of the conversation; if the parties or the nature of the conversation are not covered by the order, TURN OFF THE LISTENING AND RECORDING DEVICES.

If the targets act with great circumspection, i.e., coded, guarded, or cryptic language is used, the monitoring agents may be justified in monitoring a significant part, or perhaps all, of a conversation in order to be sure that it is indeed innocent.

### III. NEW TARGETS

One of the stated and authorized purposes of the interception is to identify additional targets in the investigation who may have not been named in the court order.

Whenever any such individual is identified by name, nickname, telephone number, etc., I (supervising attorney) should be notified immediately. I will then notify the court and a determination will be made as to whether or not an amendment to the court order is required.

### IV. CONVERSATIONS WHICH MAY NOT BE LISTENED TO AND RECORDED

The court order is quite clear that we must not listen to any "privileged" conversations, and must minimize the interception of conversations which do not relate to the criminal activity under investigation.

### V. PRIVILEGED COMMUNICATIONS

We must not listen to any conversation which would fall under any legal privilege. The general categories of privileged communications are as follows: Attorney - Client; Clergyman - Parishioner; Doctor - Patient; Husband - Wife.

#### A. ATTORNEY - CLIENT:

Consider this an absolute rule: NEVER knowingly listen to or record a conversation between a target and his attorney.

Should there be any conversations between any of the targets and any of their attorneys, you are NEVER to listen to ANY portion of ANY of these conversations at ANY time. To listen to any conversation with any of these attorneys could result in the dismissal of a pending indictment. If you should listen to a conversation with an unknown individual, and you determine that this individual is an agent or an employee of one of these attorneys, you should instantly cease monitoring the conversation. If you happen to accidentally monitor a conversation with one of these attorneys or their agents or employees, make a note of that conversation and its contents, immediately notify me, but until given further instructions, DO NOT relate to anyone the substance of that conversation (this includes any other agent of the USSS).

If at any time during the investigation we learn of the name(s) and/or telephone number(s) of any attorneys retained by our targets, this name and telephone number are to be posted in a conspicuous place in the monitoring site. Any dial-outs to that telephone number require that the recorder and monitoring device be turned off as soon as it is ascertained that it is an attorney who is calling our subject or being called by him/her.

#### B. PARISHIONER - CLERGYMAN:

All conversations between a parishioner and his clergyman are to be considered privileged. We could not obtain an interception warrant to listen to a man confess his sins to a priest in a confessional booth; similarly, we must not listen to a target discuss his or her personal, financial or legal problems with his or her priest, minister, rabbi, etc.

#### C. DOCTOR - PATIENT:

Any conversations a patient has with a doctor relative to diagnosis, symptoms, treatment, or any other aspect of physical, mental or emotional health is privileged. The instant it is learned that one of our targets is talking to a doctor about his or her health (or someone else's health), TURN OFF THE MACHINE. STOP LISTENING. STOP RECORDING.

## Sample of Minimization Memorandum (page 3)

### D. HUSBAND - WIFE:

Any conversation between a husband and his wife which relates in any way to the marital relationship is privileged. For example:

If they discuss their sex life - DONT LISTEN. DONT RECORD.

If they discuss problems their child is having in school - DONT LISTEN. DONT RECORD.

If they discuss a fight or argument they had a night or day or week ago - DONT LISTEN. DONT RECORD.

However, it may be that a target's wife or husband acts as a partner, message taker or message-deliverer for a target. Therefore a limited degree of spot monitoring may be conducted if a target calls his or her spouse. (See Section VII B, below.) If a pattern develops demonstrating that our target's spouse is in fact deeply involved in the target's dealings, then further monitoring as with any newly identified co-conspirator may be in order. However, the matter must be reported by me to the Court, so that an amendment to the court order can be made, adding the spouse as a target.

### E. OTHER RELATIONSHIPS

No legal privilege exists with regard to conversations between any of the targets and his or her paramour.

Similarly, no legal privilege exists with regard to conversations between any of the targets and their children.

However, keep in mind that our function is to intercept and record conversations related to violations of specific Federal statutes, not to indiscriminately invade the privacy of our targets and others.

In general, follow the rules outlined in paragraphs VI and VII.

### VI. "MINIMIZATION"

It is hereby ordered, that the execution of this order shall be conducted in such a way as to minimize the interception of communications not related to the violations of law under investigation. Your job is to listen to/record all pertinent conversations, while minimizing the interception of innocent (non-criminal) conversations.

That is easy to say, and difficult to do. We cannot expect the targets to oblige us by using words which specifically indicate their criminal activity. Codes, vague expressions, oblique references are quite likely to occur during monitoring.

Therefore, it may be necessary to listen to and record some non privileged conversations which in fact do not relate to the violations of law under investigation.

In my opinion, the courts will not suppress pertinent conversations simply because some non-privileged and non-pertinent conversations have been intercepted.

Always remember, however, that eventually a court may have to decide whether we executed the interception in a manner specified by the court order.

The standard which a court is likely to apply, in determining whether there was an overly broad listening to non-pertinent conversations, is simply:

Did the officers make a reasonable effort to comply with the restrictions and requirements of the court order?

"...a court should not admit evidence derived from an electronic surveillance order unless, after reviewing the monitoring log and hearing the testimony of monitoring agents, it is left with the conviction that on the whole the agents have shown high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion." U.S. v. TORTORELO

"...the monitoring agent and thereafter the reviewing court must consider many factors, including the precise relationship of the parties, the length of the relationship, the number of calls between the parties, the state of the investigation, activities... of the alleged conspirator who is a party to the conversation, and the content of the conversation to determine the appropriate degree of minimization." U.S. v. FALCONE

## Sample of Minimization Memorandum (page 4)

The Supreme Court has announced a standard for minimization which requires that interceptions be objectively reasonable in view of both the purpose of the investigation and the facts available to the monitoring agents at the time of the interception.

It is, therefore, important for each monitoring agent to be familiar with the factual background in this case in order that, if necessary, he may be prepared to articulate the reasons for the frequency and duration of any given interception in which he participated.

Keep in mind that each of you may be required to explain from the witness stand why a particular conversation was intercepted.

Make a good-faith effort to comply with the central purpose of the interception warrant: to intercept and record conversations pertaining to the conspiracy under investigation. Use your common sense. Make a good-faith effort to comply with the purposes and restrictions of the interception warrant. I can't expect anything more from you, and neither, in my opinion, will the courts.

### VII. SPOT MONITORING OR SPOT CHECKING

Assuming that a conversation does not, during the first two minutes, fall within the scope specified within the court order, the interception and recording devices must be turned off. However, it is possible that some time after the interception and recording devices have been turned off, a target may get on the telephone or the parties might begin to engage in conversations that relate to the violations of federal law which are set forth in the court order. To guard against missing such a conversation, listen periodically (spot monitor) by activating the interception and recording devices every 30 to 60 seconds or so to determine if the parties or nature of the conversation have changed to within the scope specified within the court order. LISTEN FOR A FEW SECONDS. If during this brief listening period, it appears that the conversation falls within the scope of the court order, continue to listen and record. If there is no such evidence, TURN OFF THE INTERCEPTION AND RECORDING DEVICES; STOP LISTENING.

Continue to spot-monitor as the circumstances indicate. Use your judgment as to when to spot monitor because many factors enter into your decision: parties to the call or conversation, precise relationship of the parties, the length of relationship, the number of calls or contacts between parties, present status of the investigation, past conduct of the parties, etc.

### VIII. CATEGORIES OF CONVERSATIONS

Most conversations will fall within one of the following categories:

#### A. "PATTERN OF INVOLVEMENT":

If during the course of the interception, one or more individuals is identified (by name, nickname, voice, etc.) as a co-conspirator or accomplice of our subjects, and there is no applicable privilege involved (Section F), the "spot monitoring" requirement may be relaxed somewhat as to conversations between our subject and those individuals.

#### B. CONVERSATIONS INVOLVING UNKNOWN:

When a conversation involves one or more unknown individuals, listen and record the conversation for up to two minutes (unless you are satisfied before then that the conversation is not, and is unlikely to become, pertinent). Many courts have agreed that two minutes is a reasonable period for monitoring agents to listen to a conversation before deciding whether it relates to the violations of law under investigation. If after this two minute period it appears that the conversation does not relate to the violations under investigation, TURN OFF THE RECORDER and STOP LISTENING TO THE CONVERSATION.

However, it is possible that at some time after this initial period, one or more of the targets may join the conversation, and/or the conversation may turn from innocent, unrelated topics to the violations under investigation. We have the right to SPOT MONITOR apparently innocent conversations to guard against such a possibility (particularly since we may anticipate that members of the violations under investigation will deliberately try to delay and disguise discussion of those violations to frustrate the use of the interception).

Periodically reactivate the recording and listening devices. Listen to and record the conversation for a brief period. If during this period you hear evidence pertaining to the violations under investigation, continue to listen and record; if not, DEACTIVATE THE LISTENING AND RECORDING DEVICES.

RIF

## Sample of Minimization Memorandum (page 5)

### C. PATTERNS OF INNOCENCE:

If, after a period of time, we have learned that conversations between particular individuals are invariably innocent, not crime-related, then a "Pattern of Innocence" exists and such conversations should not be recorded, listened to, or even spot-monitored unless exigent circumstances exist.

### D. EXIGENT CIRCUMSTANCES:

Under special circumstances, it may be necessary to record and listen to conversations which normally would not be intercepted.

If you anticipate such circumstances, consult me at once.

### IX. EVIDENCE OF OTHER CRIMES: ACTION REQUIRED

We do not have authorization to overhear evidence concerning the commission or planning of other crimes. This interception must be conducted with our sole legal purpose in mind: interception of conversations between our named subjects and co-conspirators and accomplices concerning those federal violations enumerated in the Court Order. Interception of non-enumerated offenses must be brought to my attention immediately.

### X. USE OF LISTENING AND RECORDING DEVICES

No interception or recording device is to be left unattended on "automatic." "MINIMIZATION" requires that monitoring agents determine whether or not each conversation is relevant and subject to interception.

Anytime a conversation or any part thereof is monitored it is to be recorded. If the interception or recording device has a separate monitor switch, the switch is not to be activated unless you are recording. However, if the interception or recording device malfunctions, or a recording tape has just run out, monitoring is permissible while the situation is being remedied. Be sure to report the overheard conversation and the circumstances of this situation in the Consecutive Call Log.

### XI. DAILY REPORT OR LOG

Abstracts of summaries of each conversation are to be made at the time of interception and are to be included in the Consecutive Call Logs. If the conversation was not entirely recorded, an appropriate notation should be made indicating the incomplete nature of the conversation (e.g., monitoring discontinued) and why the conversation was not completely recorded (e.g., non pertinent, privileged). Where the exact words used by the participants are important, that portion of the conversation should be included in the Consecutive Call Log. Copies of the logs should be delivered to me on the following day.

The logs are to be a reflection of all activity occurring at the listening post and concerning the intercepted calls or conversations as well as the equipment itself (e.g., replaced reel #2 with #3; malfunction of a recorder, etc.). These logs will ultimately be used by you to explain and to reflect your action taken in intercepting or not intercepting a particular communication. Therefore, it is vitally important to succinctly describe parties to the conversation, the nature of the call and the action taken (e.g., monitor discontinued, not pertinent or privileged, etc.).

The Consecutive Call Log is of extreme importance both for our reports to the issuing judge and ultimately to the court which will litigate the issue of minimization. If you keep an accurate account of the nature of the conversations, our efforts in preparing for any hearing or trial will be minimized.

The judge of the District Court who issued the court order has the right to require us to make periodic reports to him about the progress of the investigation and the manner in which the warrant is being executed. I will need this information in order to comply with the reporting requirement.

I must receive a copy of all logs, transcripts, and surveillance reports daily!

If anything appears to be breaking suddenly or a problem arises, CALL ME.

Signature

RIE



## Disclosure of Intercepted Communications

Strict guidelines have been established relative to the disclosure and use of communications seized during non-consensual interceptions. 18 U.S.C. 2517 sets forth who may disclose or use information derived through electronic surveillance, and to whom the information may be disclosed, and how the information may be used. Information can be disclosed to, or used by, the following individuals:

- (1) To another law enforcement officer for proper performance of his/her official duties;
- (2) Any law enforcement officer who legally obtained the information may use the information in proper performance of his/her official duties;
- (3) While giving testimony under oath in any proceeding held under the authority of the United States;
- (4) Privileged information can not be disclosed (i.e., husband/wife, lawyer/client, doctor/patient, clergyman/parishloneer);
- (5) The information related to other offenses may be used in accordance with the above sections when a judge of competent jurisdiction approved interception;
- (6) To any other Federal law enforcement officer or agency (intelligence, protective, immigration, national defense, national security, etc.) to assist the officials in the performance of his/her official duties;
- (7) To any foreign law enforcement officer to the extent that such disclosure is appropriate to the proper performance of his/her official duties and in accordance with the Privacy Act. The foreign law enforcement officer may also disclose or use the information in the performance of his/her official duties;
- (8) To any appropriate Federal, State, local or foreign government officials for the purpose of preventing or responding to a threat.

The contents of an intercepted communication is to be disclosed by an agent or attorney only after he/she is satisfied that the person to whom disclosure is made has a need to know the information. Disclosure of intercepted communications to any other investigative agency, pursuant to 18 U.S.C. 2517, should be made only after the Supervising Agent and supervising AUSA have agreed on such disclosure.

A memorandum of disclosure should be prepared by the investigative or law enforcement officer making the disclosure. This memorandum should indicate the name and agency of the person to whom disclosure was made, the date of disclosure, a brief summary of the information disclosed, identification of the interception (call number, etc.) and the purpose for making the disclosure. The investigative or law enforcement officer making the disclosure must inform the recipient that the disclosed information came from an authorized interception, and that subsequent authorization must be obtained before use in any proceeding. Any disclosure of the contents of intercepted communications, by Government attorneys and agents or any other person, which is not pursuant to 18 U.S.C. 2517, may subject the offending party to a civil action for damages under Title 18 U.S.C. 2520.

## Preliminary Meeting Held by Supervising Attorney (AUSA)

In anticipation of the issuance of the court order, but prior to the initiation of the interception, the supervising AUSA should hold a meeting with the Supervising Agent, case agent, all prospective monitoring personnel,

all transcription personnel, all TSD personnel, and headquarters representatives (ISD, et al.) involved with the interception operation. During this meeting, the supervising AUSA should inform all participants of the contents of the anticipated court order, emphasizing those provisions of the court order describing the type of communication sought for interception, the particular violations of law to which the communications relate, the guidelines for minimization, and the guidelines for terminating the interception when the objective has been attained.

The supervising AUSA should emphasize that any limitations in the court order relating to limited hours of operation, visual surveillance, etc., should be strictly followed. All personnel should be briefed on the rules relative to the disclosure of intercepted communications. Prior to participating in any of the specific functions associated with the interception, all personnel involved with the interception must carefully read the following documents:

1. Affidavit supporting the application for the interception order,
2. Application for the interception order,
3. Draft court order submitted for authorization,
4. Minimization memorandum prepared by or for the supervising AUSA,
5. Chapter III of The Interception and Recording of Wire, Oral and Electronic Communication Manual.

After reading these documents, each individual must sign and date the Document Review Log (SSF 3285).

The Document Review Log (SSF 3285) can be found via the USSS Forms Library at Intranet address <http://ssweb/mno/pars/forms>.

## Posting the Court Order

Since the interception must be confined to the terms of the court order, the order must be posted in the wire room, near monitoring personnel, for quick reference.

## Installation of the Interception Equipment

The only personnel who are authorized to install and test any of the equipment which will be used to accomplish the interception are specialists who are assigned to either the field office or to TSD. Once the equipment has been installed and is operational, these same personnel are responsible for the technical maintenance of the equipment. They should not be utilized for the routine operation of the recording equipment, i.e., maintaining the recorder, monitoring, etc., nor should they become involved in any other non-technical segment of the investigation. All routine operational functions which involve the operation of the intercept equipment should be performed by wire room personnel only.

## Pen Register

Whenever it is anticipated that a non-consensual interception is to be applied for, a request for the installation of a Pen Register should immediately be initiated. The Pen Register is an integral part of most non-consensual interceptions, and its use prior to the interception can provide additional probable cause needed in the application. Early installation of a Pen Register will also facilitate the initiation of the interception once it is authorized by the court. As stated earlier, Pen Register operation is covered under Title III of the Electronic Communications Privacy Act of 1986.

A separate Pen Register should be requested for each target telephone. Prior to requesting the installation of a Pen Register, Chapter IV of this manual should be read in its entirety by all of the investigating and supervisory personnel who will be directly involved in the conduct of the interception.

## Personnel Access

As soon as the Pen Register is installed and operational, the wire room should be considered secure and accessible to only authorized personnel who are directly involved with the interception.

At this time, a "Personnel Access Log" (SSF 3285A) must be posted and maintained at the entrance to the wire room. All persons who access the wire must make the appropriate entries in the log each and every time they either enter or exit.

## Headquarters Notification After Interception Is Initiated (Initiation Message)

As stated earlier, as soon as a judge has issued the interception warrant, 18 U.S.C. 2518(5) requires that the authorization to intercept be executed as soon as practicable. Immediately following the initiation of the interception, the SAIC of the office conducting the interception must submit an official message to headquarters under the case number of the investigation for which the interception is conducted. The distribution of this official message will include the appropriate operational division, the appropriate Assistant Directors Office, the Technical Security Division (TSD), and the Investigative Support Division (ISD). This official message should comment on the following factors:

1. Target telephone (or IP addresses) number(s) and subscriber(s) (area code and number; subscriber name and address),
2. Location of target telephone(s) (or Internet Service Provider) (apartment number, complete address),
3. Court order number, date and judicial district (date signed by judge),
4. Date and time interception initiated,
5. Anticipated duration of use (number of days).

If, during the course of the interception, new target line(s) are identified and approved for interception, an official message(s) must be sent notifying Headquarters of their initiation.

The following page has a sample official message for reporting the initiation of an interception.

## Sample Official Message Reporting the Initiation of a Non-Consensual Interception

FROM: SAIC-FIELD OFFICE	CASE NUMBER:
	CASE TITLE:
TO: SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO: AD-APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC- INVESTIGATIVE SUPPORT DIVISION SAIC-TECHNICAL SECURITY DIVISION	
SUBJECT: INITIATION OF NON-CONSENSUAL INTERCEPTION	
REFERENCE IS MADE TO (OFFICE) OFFICIAL MESSAGE DATED _____, REPORTING THE SUBMISSION OF A NON-CONSENSUAL INTERCEPT APPLICATION TO THE DEPARTMENT OF JUSTICE.	
INTERCEPTION ORDERS HAVE BEEN GRANTED AND INTERCEPTIONS HAVE BEEN INITIATED FOR THE FOLLOWING TARGET TELEPHONE LINES (OR IP ADDRESSES):	
NAME OF THE TARGET:	
TARGET TELEPHONE NUMBER (OR IP ADDRESSES) AND SUBSCRIBER: (AREA CODE AND NUMBER; SUBSCRIBER NAME AND ADDRESS)	
LOCATION OF TARGET TELEPHONE (OR INTERNET SERVICE PROVIDER): (APARTMENT NUMBER, COMPLETE ADDRESS)	
COURT ORDER NUMBER, JUDICIAL DISTRICT AND JUDGE:	
DATE AND TIME INTERCEPTION ORDERS GRANTED:	(DATE SIGNED BY JUDGE)
DATE AND TIME INTERCEPTION INITIATED/ACTIVATED:	
ANTICIPATED DURATION OF USE:	(NUMBER OF DAYS)
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC

## Preparation and Logging of Recording of Intercepted Communication

18 U.S.C. 2518(8) (a) directs that the contents of any intercepted communication "...shall, if possible, be recorded on tape... or other comparable device." This requirement is mandatory in all but the most extraordinary situations. Although the mechanical breakdown of recording equipment would probably be temporarily excusable under this section, the preferred practice is to provide for recorder redundancy in an effort to avoid such a situation.

## Recording of Intercepted Communication

Currently, the communication interception equipment employed by this Service utilizes two (2) high capacity recordable disks. The interception equipment can also store the intercepted communication on its hard drives.

The two high capacity disks will be utilized simultaneously for each target telephone line during the wiretap operation. One will be the "Primary Evidence" disk; the second disk will be the "Back-up" disk. The intercepted communication saved on the hard drive may be used to produce the work copy. Only the pertinent communication may be copied on the work copy for transcription.

The high capacity disks will be provided by TSD. Each of the disks will be digitally recorded with case number, case title, disk number, and the phone number intercepted by the wire room personnel. The disk cover will also be labeled with the same information.

All "Primary Evidence" disks may be pre-numbered prior to beginning interception in sequential order for use throughout the entire operation. A suffix letter of "E" (evidence) will follow the assigned disk number (example: Disk # - 001E). The disk numbers must be digitally recorded on the disk. The "Primary Evidence" disk should be replaced when the maximum capacity of disk space is filled. It is the responsibility of the Shift Leader to record the call number sequence (example: disk number - 001E, Call numbers - 001 to 100) on the disk label. The disk will be then placed in a Title I Evidence Control Record (SSF 3277) envelope. The wire room Shift Leader will make the appropriate entries on the envelope. Form SSF 3277 can be obtained from ISD.

A second disk will be utilized to record a "back-up" of the evidence disk. The "back-up" disk should also be pre-numbered in sequential order for use throughout the entire operation. The number of each disk will coincide with the "Primary Evidence" disk number, except that the suffix letter of "B" (back-up) will follow the number (example: 001B). The disk numbers must be recorded on the disk and disk label. The back-up (B) disk will be replaced at the same time as the evidence (E) disk. The disks will then be placed in a separate SSF 3277 (Title I Evidence Control Record) and the wire room Shift Leader will make the appropriate entries on the envelope. Form SSF 3277 can be obtained from ISD.

Only the pertinent conversations may be recorded using the data saved on the hard drive of the computer used in the interception. These separate recordings may be used to transcribe by the transcribing personnel. Each "work" disk containing pertinent conversations will be secured in a Title I Evidence Control Record (SSF 3277) after the conversation has been transcribed.

The SSF 3277's containing evidence, backup, work copy, transcript, and consecutive call log will be inventoried on SSF 1544 per the procedures outlined in INV-15.

RIP

## Procedure When No Recording Can Be Made

As was stated earlier, absent exigent circumstances, the contents of any intercepted communication shall be recorded on a tape or technologically comparable storage device. In those unusual situations where an interception cannot be recorded, (e.g., equipment failure) the intercepting agent must submit a memorandum reporting the contents of the interception.

This memorandum should be as near a verbatim transcript as possible under the circumstances of the interception, and should outline the circumstances that prevented the recording of the interception. The memorandum should indicate the date, time, and place of the interception, the court order authorizing the interception, and should be signed by the intercepting monitor. Upon completion, the memorandum should be treated as though it was a recording of the conversation, and secured in a Title I Evidence Control Record, SSF 3277, and the wire room Shift Leader will make the appropriate entries on the envelope.

## Disk Control Log

The Disk Control Log (SSF 3279A) is a record of the installation and removal of the "Primary Evidence" and "Back-up" disks and will be maintained by the Shift Leaders in the wire room. The "Work" disks are not entered into this log. All installation and removal of "Evidence" or "Back-up" disk will be recorded in the Disk Control Log.

The Disk Control Log (SSF 3279A) can be found via the USSS Forms Library at Intranet address <http://ssweb/mno/pars/forms>.

## Consecutive Call Log

The interception equipment currently employed by this Service generates the Consecutive Call Logs automatically and allows the operator to input all information pertaining to the call directly into the interception equipment during the interception of communication. The monitoring personnel shall input the necessary information into the equipment contemporaneous to intercepted phone communication in order to maintain accurate records. Some of the required information includes, whether the call is pertinent or non pertinent, synopsis of the call, and whether the call was or was not minimized. The call information, to include dialed number, duration of call, and incoming or outgoing call status, will be provided by the interception equipment automatically.

The Consecutive Call Log generated by the interception equipment will be printed daily at a predetermined time and will be handled as evidence. Three copies of the Consecutive Call Log will be made. The original will be secured in a Title I Evidence Control Record envelope (SSF 3277). One copy each will be provided to the case agent and AUSA. The remaining copy will be retained by the wire room Shift Leaders for use of wire room personnel.

If the monitoring personnel are unable to maintain the Consecutive Call Log via the interception equipment, the Title I Consecutive Call Log (SSF 3279) will be used to record necessary information.

The Title I Consecutive Call Log (SSF 3279) can be found via the USSS Forms Library at Intranet address <http://ssweb/mno/pars/forms>.

## Interception of Electronic Communication

The procedures for obtaining authorization remains the same as previously prescribed. Processing of evidence differs slightly as compared to interception of oral communication.

Processing evidence from electronic communication interceptions involves "After the Fact Minimization." A thorough review of the "evidence handling" procedures should be discussed with the AUSA.

In addition, interception of electronic communication requires slightly different configuration than the traditional Title I interception. Interception of electronic communication requires a minimization team, investigative team, and technical support team.

Intercepted communication will be downloaded by the minimization personnel at the predetermined time each day by transferring the e-mail/fax/chat/other files from the server's mainframe to the hard drive of the minimization personnel's computer terminal. Each transfer of data will be logged on the Activity Log and maintained by the minimization team. The minimization personnel will take necessary precautions to ensure the integrity of intercepted data during transfer from the server's mainframe and while reviewing and sorting into appropriate categories.

The minimization team will review all intercepted communications and a determination should be made whether they are pertinent or non pertinent; considering the identities of the sender, the recipient, the content of the transmission and other available information. The data should then be indexed into three categories. These categories are "Pertinent," "Non Pertinent," and "Unknown."

On the computer used to download and review the data, the minimization team will create three folders. These folders are "Pertinent," "Non Pertinent," and "Unknown." Each of the folders will also contain three sub folders. These subfolders are, "Chat," "E-mail/fax," and "Other."

All chat/instant messaging deemed pertinent will be reviewed and moved to the "Chat" folder of the "Pertinent" folder. All e-mails and faxes deemed pertinent will be reviewed and moved to the "Email/fax" folder of the "Pertinent" folder. All others, i.e. downloads and web browsing deemed pertinent, will be reviewed and moved to "Other" folder of the "Pertinent" folder.

All chat/instant messaging deemed non pertinent will be reviewed and moved to "Chat" folder of the "Non Pertinent" folder. All e-mails and faxes deemed non pertinent will be reviewed and moved to the "Email/fax" folder of the "Non Pertinent" folder. All others, i.e. downloads and web browsing deemed non pertinent, will be reviewed and moved to the "Other" folder of the "Non Pertinent" folder.

If the minimization team is unable to make a determination as to pertinent or non pertinent, the intercepted data should be moved to the "Unknown" folder. Every effort should be made to make the determination whether they are pertinent or non pertinent. The minimization team may consult with the investigative team without disclosing whole communication to determine whether the communication is pertinent or not.

Evidence of other crimes should be moved to the "Other" subfolder in the "Unknown" folder until the AUSA supervising the interception is notified and the court order is amended to monitor other crimes not authorized in the original court order.

Any data containing codes, foreign language, or encryption may be placed in the "Unknown" folder until determination is made to whether they are pertinent or non pertinent.

At the end of the interception, the entire intercepted communication/data will be stored on a technologically appropriate storage device. This includes pertinent, non-pertinent, and unknown communications. Also, all pertinent communication will be stored on a separate technologically appropriate storage device.

The storage device containing all intercepted communication/data will be logged, per INV-14 and INV-15, as evidence and sealed at the completion of the interception. The storage device containing only the pertinent communication will also be logged as evidence and properly stored.

A print out of the folder directory should be made and stored along with the storage device. The evidence handling procedures should be discussed in detail with the AUSA supervising the interception.

The investigative team may consist of Agents who are familiar with the case. These agents will have access to only the "Pertinent" folder of the intercepted communication. The investigative team will have minimum contact with the minimization team to prevent undue influence.

The technical support team may consist of TSD or ECSAP trained personnel. If required, outside vendors may be utilized in technical aspects of the interception under the supervision of the TSD or ECSAP Agents. The technical support team will ensure all the equipment used in the interception is in proper working condition. They may install, maintain, and test the equipment to ensure working condition. Prior to installation, the technical support team will ensure that all the computers and storage devices are free of contamination.

If an intercepted communication contains privileged information, the AUSA supervising the interception should be notified immediately.

## Transcripts

Generally speaking, it is not necessary to routinely transcribe all of the pertinent conversations that are intercepted. However, if the intercepted conversation is only marginally audible or intelligible, a transcript will probably facilitate the understanding of the conversation. In these cases, it is highly recommended that a transcript be made.

If it is probable that the intercepted conversation will be used during any judicial proceeding, the conversation should be transcribed. Transcripts facilitate the writing of investigative reports, aid in the preparation for judicial proceedings, facilitate the direct and cross-examination of witnesses, enable an attorney to quote relevant portions of conversations during summation, and facilitate appellate review of the trial record.

If the transcripts are to be distributed to the jury, every effort should be made to ensure that they are as complete and accurate as possible. If the key evidence in a case consists of recordings which are difficult to comprehend without the use of transcripts, the verdict may depend upon whether the jurors can follow the transcripts and whether the jurors accept them as accurate. An omitted word or phrase, though irrelevant to the importance of the conversation, may reduce the credibility of the transcription of a less easily understood but more important passage. The transcript should also contain auditory signposts to assist the jurors in following the conversation. Inaudible passages should be marked as such, with an indication of how long the inaudible passage is.

Noticeable changes in the volume or character of background noise should be highlighted. Such signposts may enable a juror who has lost his/her place on the transcript to find it again. A transcript which was perfectly adequate for investigative purposes may not be sufficient for judicial presentation.

Transcripts which are prepared during the interception will probably require extensive revision when preparing for trial. The transcription style should be consistent from conversation to conversation. The following information obtained from the computer generated Consecutive Call Log and the disks must be contained in the heading and body of the transcript.



1. Target Telephone Number,
2. Call Number,
3. Date of Call,
4. Page Number (page \_\_\_ of \_\_\_),
5. Transcriber Name,
6. Date(s) of Transcription (Date In/Date Out),
7. Case Number,
8. Ingoing/Outgoing,
9. "In" Parties,
10. "Out" Parties.

In the case of interception of electronic communication, transcription may not be necessary unless the communication is in codes or in foreign language.

The transcription should be devoid of any editorial insertions. For example, if one of the parties to the conversation referred to "Big Jim," the identity of "Big Jim" should not be inserted in the transcript.

Transcription may be done by non-agent administrative personnel. However, they must work in conjunction with an agent working on the interception; that agent must then review the transcription for accuracy. Copies of all transcripts should be made for both the supervising AUSA and Wire Room Supervisor.

The original transcript is evidence and should be handled as such. Upon completion, the transcript will be placed in a Title I Evidence Control Record (SSF 3277) and secured.

## Termination of the Interception

18 U.S.C. 2518(5) commands that the court ordered interception terminate either when the objective of the surveillance has been realized or on a specified date within 30 days after the start of the interception, whichever comes first. The interceptions of conversations must terminate as soon as the Government has obtained the evidence which was the objective of the authorization. If the interception is continued beyond that point, evidence derived from continued interception will not be construed as obtained pursuant to a court order.

Such an unauthorized interception would violate the Fourth Amendment and would have three serious consequences: First, evidence derived from the unauthorized interception would be rendered inadmissible. Second, the personnel conducting the unauthorized interception might be subject to criminal penalties. Third, the personnel conducting the unauthorized interception might be subject to civil suit by persons whose conversations were intercepted.

It should be noted that, while many court orders cite the identification of co-conspirators as one of the primary objectives, a blind reliance upon this language as grounds for continuing the surveillance until the calendar expiration date could be subject to serious consequences. While it is true that identifying and defining the

roles of conspirators is a proper objective, it must be realized that these interceptions rarely result in the identification of all participants. The primary consideration is whether a continued interception can stand the test of subsequent court scrutiny.

The Wire Room Supervisor bears initial responsibility for determining when the interception should be terminated. When, during the course of the interception, the Wire Room Supervisor determines that the communications expected to be overheard have been intercepted and recorded, he/she shall immediately consult with the supervising AUSA regarding the decision. If the supervising AUSA does not concur, then interception under the original court order shall continue. If the supervising AUSA determines that sufficient evidence has been obtained from the authorized interception, the electronic surveillance must cease.

Regardless of whether or not an authorized interception has achieved its objective, it may only take place during the period authorized by the court order. When nearing the end of this time period, it is the responsibility of the Wire Room Supervisor to notify the supervising AUSA of the impending termination of the interception. The Wire Room Supervisor must then ensure that the interception is terminated by the time the court order elapses.

## Application for Extension of Interception

In many instances, a court ordered interception will reveal some, but not all, of the evidence sought in the application. On other occasions, the interception will reveal so much evidence that the scope of the investigation must be expanded considerably. In either situation, it may be desirable to continue the interception of the target telephone or apply for authorization for the interception of additional target telephones. The AUSA, in consultation with the Wire Room Supervisor and Case Agent, will make the decision as to whether or not an application for extension is appropriate.

18 U.S.C. 2518(5) provides as follows:

**"...No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days..."**

Any application for the extension of a court ordered interception must satisfy all of the statutory provisions which govern the initial application and court order. Although Title I does not place a limit on the number of extensions that may be applied for, the courts look very carefully at extended use of court ordered interceptions.

Applications for extensions by the AUSA can often be processed in three or four days, but the time frame can vary widely. If it is important that the electronic surveillance not be interrupted, the extension request must be submitted to the AUSA with sufficient lead time.

When a time gap exists between the termination of the original interception and the signing of the extension order, it is not necessary that the interception facilities be removed or dismantled. It is sufficient that they be

deactivated, that is, turned off. During this period it is imperative that interception personnel understand that they do not have authority to intercept or record communications unless and until the court signs the extension, and even then their authority is circumscribed by the terms of the extension order and not the original.

During the extension interception, the same procedures should be followed as during the original interception. Headquarters must be notified via official message upon the initiation of the extension.

## **Final Headquarters Notification (Termination Message)**

Immediately following the termination of each interception, the SAIC of the office conducting the interception must submit an official message to headquarters under the case number of the investigation for which the interception was conducted. The distribution of this official message will include the appropriate operational division, the appropriate Assistant Directors Office, the Technical Security Division (TSD), and Investigative Support Division (ISD).

This official message will reference the previous Headquarters initiation official message reporting initiation of the interception.

This official message will certify the termination of use, disconnection and removal of all of the interception equipment and should comment on the following factors:

1. Target telephone number (or IP addresses) and subscriber (area code and number; subscriber name and address);
2. Location of target telephone (or Internet Service Provider) (apartment number, complete address);
3. Court order number, date and judicial district (date signed by judge);
4. Date and time of interception termination;
5. Duration of use (date and time it was first operational through date and time it was disconnected; total number of days operational);
6. Investigative benefits derived (brief synopsis);
7. Security specialist completing the removal of equipment;
8. Telephone company representative notified of removal (title, name and telephone number);
9. Location equipment removed from (location name and address).

## Sample Headquarters Notification Official Message for Reporting the Termination of a Non-Consensual Interception

FROM: SAIC-FIELD OFFICE	CASE NUMBER:
	CASE TITLE:
TO: SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO: AD-APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC-TECHNICAL SECURITY DIVISION SAIC-INVESTIGATIVE SUPPORT DIVISION	
SUBJECT: TERMINATION OF NON-CONSENSUAL INTERCEPTION	
REFERENCE IS MADE TO OFFICIAL MESSAGE, DATED _____, REPORTING THE INITIATION OF THIS NON-CONSENSUAL INTERCEPTION. THIS INTERCEPTION HAS BEEN TERMINATED.	
NAME OF THE TARGET:	
TARGET TELEPHONE NUMBER (OR IP ADDRESSES) AND SUBSCRIBER:	(AREA CODE AND NUMBER; SUBSCRIBER NAME AND ADDRESS)
LOCATION OF TARGET TELEPHONE (OR INTERNET SERVICE PROVIDER):	(APARTMENT NUMBER, COMPLETE ADDRESS)
COURT ORDER NUMBER, DATE AND JUDICIAL DISTRICT:	(DATE SIGNED BY JUDGE)
DATE AND TIME INTERCEPTION TERMINATED:	
DURATION OF USE:	(DATE AND TIME IT WAS FIRST OPERATIONAL THROUGH DATE AND TIME IT WAS DISCONNECTED; TOTAL NUMBER OF DAYS OPERATIONAL)
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS)
SECURITY SPECIALIST COMPLETING THE REMOVAL OF EQUIPMENT:	
TELEPHONE COMPANY REPRESENTATIVE NOTIFIED OF REMOVAL:	(TITLE, NAME AND TELEPHONE NUMBER)
LOCATION EQUIPMENT REMOVED FROM:	(LOCATION NAME AND ADDRESS)
FIELD OFFICE	CASE SA /SUPERVISOR/SAIC)

## **Sealing and Custody of the Evidence Upon Termination of Interception**

Immediately upon termination of the interception, the original recordings of the conversations (evidence disks, storage devices), the intercepted electronic communication should be submitted by the supervising AUSA to the judge authorizing the interception. The judge will then order these evidentiary items sealed and order their place of custody.

As most courts and their clerks are not equipped to safeguard evidence, the supervising AUSA will probably suggest that the court order the custody of the sealed evidence to remain with the investigating office which undertook the surveillance. In many instances, the bulk of the evidentiary material will preclude their being kept by the clerk of the court.

The sealing should be done under the supervision of the authorizing judge. Careful attention should be observed when safeguarding the evidence. If recordings are to be sealed, careful attention must be paid to environmental conditions such as extreme heat or cold or strong magnetic forces which can adversely affect the original condition of the storage devices. Any such conditions must be avoided.

## **Inventory - Disclosure of the Wire Tap**

Whenever law enforcement officers conduct a search pursuant to the issuance of a warrant, they must subsequently notify the person or persons whose property has been searched and give that person or persons an inventory of the items that have been seized. A similar notice and inventory must be served upon the subject of an eavesdropping warrant. 18 U.S.C. 2518(8) (d) states in part as follows:

**"Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of -**

- (1) the fact of the entry of the order or the application;**
- (2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application and;**
- (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.**

**The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice..."**

## Postponing of the Inventory - Disclosure of the Wiretap

Congress recognized that the continuing investigation of a subject could be compromised if the inventory invariably was served within the prescribed 90 day period. Therefore, the filing of the inventory may be postponed during a period when the supervising AUSA can demonstrate that there is "good cause" for the postponement. 18 U.S.C. 2518 (8) (d) states in part as follows:

**"...On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed."**

Whenever the supervising AUSA has reason to believe that there is "good cause" to postpone the serving of the inventory, he/she should immediately file an ex parte motion stating the good cause and requesting postponement. The motion may be made to any judge of competent jurisdiction. Normally, it would be made before the judge to whom application for the order was originally made.

## Preparing the Inventory List for Disclosure of the Wiretap

The Supreme Court has held that 18 U.S.C. 2518 (8) (d) requires the Government, when the intercept is over, to classify all persons whose conversations have been overheard and to provide that information to the issuing judge so that he/she may use it in causing mandatory notice to be served on persons named in the application or order and in exercising his/her discretionary power to have notice served on unnamed persons who were intercepted.

The following are essential classifications:

1. Persons named in the order or the application,
2. Other persons whose intercepted communications apparently incriminate them in the offense or offenses specified in the interception order,
3. Other persons whose intercepted communications apparently incriminate them in offenses not specified in the interception order, and
4. Persons whose intercepted communications are apparently non-incriminating.

If any omission is discovered after the judge has been provided with the classifications, a supplementary report correcting the omission should be made to him/her as soon as possible. To facilitate the preparation of the inventory listing, the supervising AUSA should require the Wire Room Supervisor to furnish him/her a preliminary report detailing the names of those intercepted and the category into which each falls, approximately 90 days after termination of the interception.

The inventory listing should be forwarded by the supervising AUSA to the court approximately 5 days prior to the date that the inventory is due. Attached to the inventory should be a proposed order of those who must be inventoried. The supervising AUSA should assist the judge in the exercise of this function by making recommendations.

Ordinarily, those in the first three of the above categories are inventoried, and those in the fourth category are not. **It is important to insure that every indictee and prospective indictee who has been identified subsequent to the inventory proceedings, is served with an inventory as soon as practicable.**

## Record Retention

As per 18 U.S.C. 2518(8)(a), recordings of intercepted conversations or other evidentiary material (e-mail, faxes, etc.) must be retained, maintained and protected for a minimum of ten years at a location so ordered by the court. The seal placed upon the recordings by the court will not be broken during this maintenance period unless authorized by the court. Upon expiration of the retention period, the recordings may only be destroyed pursuant to court order by the original authority granting interception.

The Secret Service case file and all administrative records pertaining to the investigation shall be retained for a minimum of ten years in the field office (refer to ADM Manual, Section MNO-07(06)). Each case file must have a SSF 3103, Non-Consensual Interception, affixed to the front of the file folder to preclude unauthorized disclosures and to prevent premature destruction of the file. The SSF 3103 may be obtained from ISD.

A copy of the inventory submitted to the supervising AUSA, and a list of all telephone numbers associated with subjects on this inventory list, is forwarded to ISD for inclusion in the electronic interception file. Other documents included in the electronic interception file are all court orders, affidavits, applications, extensions, and minimization instructions.

## Indexing of the Targets in MCI

It is the responsibility of the controlling field office to ensure that all pertinent information is entered into the MCI system. During the indexing of subjects intercepted under the court order, subject interest codes 42 and 43 will be used in conjunction with other codes (suspect or defendant). Interest code 42 will be used to identify subjects who are being intercepted or who have been intercepted by this Service. The subjects will include primary targets of an investigation, as well as any additional targets who may become a suspect or a defendant. Interest code 43 will be used to identify subjects who are being intercepted or who have been intercepted by other law enforcement agencies.

The interest codes 42 and 43 may be entered by the field office personnel. However, modification of the codes can only be done by ISD personnel. The new interest codes will not affect the status or closing of the case.

In addition to updating the subject screen with the interest codes 42 and 43, the Subject Summary (SSUM) will also be updated with the subject's telephone numbers, address, date of interception, agency conducting the interception and other pertinent information to include charges, sentencing information, and whether the subject is a primary target of the investigation or was an additionally developed target. In the case of intercepted faxes, this will include all subjects, fax numbers and addresses. In the case of intercepted email, this will include email addresses and internet protocol addresses.

## Reports to Department of Justice

Title 18 U. S. C. 2519 requires that in January of each year this Service provide to the Attorney General of the United States an annual report of all interceptions conducted in the prior twelve (12) months. This report will cover each application for any non-consensual wire, oral, and electronic interception made by this Service under provisions of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986.

Manual : Interception  
RO : ISD

Section : Chapter III  
Date : 03/01/2006

This annual report will be compiled by the Investigative Support Division (ISD) with input from the field and will be reported on Court Forms WT1 (Annual Prosecutor Summary of Wiretap Reports), WT2 (Report of Application and/or Order Authorizing Interception of Communication), and WT3 (Supplementary Report for Wiretaps Reported in Previous Calendar Years). Office of Enforcement Operation (OEO), DOJ will provide instructions on completion of the required forms.

The completed forms (WT1, WT2, and WT 3) will be forwarded, under covering memorandum from the Office of the Director to Office of Enforcement Operations (OEO), DOJ.



## Stored Wire and Electronic Communication and Transactional Records Access

### Table of Contents

	Page
Introduction .....	1
Definition .....	1
Disclosure of Communication or Records .....	2
Governmental Access Requirements .....	3
Transactional Records .....	4
Backup Preservation .....	4
Delayed Notice .....	5
Cost Reimbursement .....	5

RIF

# STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

## Introduction

Title II of the Electronic Communications Privacy Act of 1986, as previously outlined in Chapter I of this manual, is designed to protect the privacy of stored electronic communications. This includes storage prior to transmission to a recipient as well as any copy of the transmitted communications kept after delivery to a recipient.

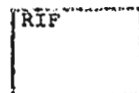
Chapter 121 under Title 18 U. S. C. 2701 to 2712, governs these areas of communications. Criminal as well as civil sanctions may be applied to any violations of the provisions of Title II. Therefore, it is strongly recommended that early consultations be made with the appropriate United States Attorney's office in conjunction with the appropriate operational division when seeking disclosure in areas covered under Title II.

## Definitions

1. **Electronic storage** is defined in 18 U.S.C. 2510 (17) as "... any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

For example, if electronic mail has been sent, but not opened by the intended recipient, then it is in "electronic storage," incidental to transmission. Once the electronic mail has been opened by the recipient, it can be argued that the electronic mail is no longer in electronic storage incidental to transmission.

2. An **"electronic communication service"** provides its users the ability to send or receive wire or electronic communication.
3. **Remote computing service:** the provision to the public of computer storage or processing services by means of an electronic communications system. Remote Computing Service "allows persons to use the facilities of these services to process and store their own data." Subscriber to a remote computing service "transmits records to a third party for the purpose of computer processing."
4. **Transactional record:** any record showing business taking place between the provider of an electronic communications service and a subscriber/party (i.e., service agreements, toll records, subscriber information, etc.).



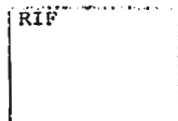
It should also be noted that other definitions concerning Titles I, II, and III of the Electronic Communications Privacy Act of 1986 may be found under related chapters/sections of the Federal Criminal Law Handbook

## Disclosure of Communications or Records

Generally, a person or an entity providing a public electronic communication service, or remote computing service, shall not knowingly divulge the contents of a communication held in electronic storage by the individual or company. The same holds true in relation to any communication carried on or maintained by any public remote computing service. Included in the foregoing are communications received by way of electronic transmission, created by means of computer processing, or held solely for the purposes of storage or computer processing.

Exceptions for disclosure of stored wire and electronic communications and transactional records, fall into the following eight categories (Title 18, U.S.C. 2702 (b)). The contents of such communications and records may be disclosed to:

1. Addressees, intended recipients or their agents;
2. Those individuals or entities as otherwise authorized in sections 2517, 2511 (2) (a) or 2703 of this title;
3. Others with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
4. A person employed or authorized or whose facilities are used to forward such a communication to its destination;
5. Others as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
6. To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);
7. A law enforcement agency, if such contents were inadvertently obtained by the service provider, and appear to pertain to the commission of a crime; and
8. To a Federal, State, or local government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.



## Governmental Access Requirements

In this section, requirements for Federal law enforcement access shall be reviewed. However, it should be noted that access is also provided for State and/or local government entities. For additional information in this regard, reference is made to Chapter 121 of Federal Criminal Law Handbook.

The Secret Service may require a service provider to disclose the contents of an electronic communication that is in **electronic storage in an electronic communication system for one hundred and eighty (180) days or less, only with a warrant** issued by a court with jurisdiction over the offense under investigation as outlined in 18 U.S.C. 2703(a).

If the communication has been in **electronic storage in an electronic communications system for one hundred and eighty (180) days or more**, disclosure may be sought in several ways, as described in Title 18 U.S.C. 2703 (a) (b). These include:

1. A search warrant (without prior notice to the subscriber).
2. A court order (with prior notice to the subscriber, and may request seeking delayed notice to the subscriber.)
3. An administrative, grand jury, or trial subpoena (with prior notice to the subscriber, may request delayed notice up to 90 days with written certification by a supervisory official).

It should be noted, that in the obtaining of a court order, the relevancy of the material requested must be shown. Time limitations relating to the maximum duration of such orders or extensions thereof are not applicable.

Under Title 18 U.S.C. 2703 (b), the government may obtain the contents of any electronic communication held in remote computing services. If the electronic communication that is held on these services is on behalf of, and received by means of, electronic transmission from a subscriber and solely for the purpose of providing storage, the information may be obtained in the following ways:

1. A search warrant,
2. An administrative, grand jury, or trial subpoena,
3. A court order authorized by Section 2703 (d), with a request seeking delayed notice to the subscriber.

When a search warrant is contemplated to obtain the records, contact should be made with the Assistant United States Attorney and Computer Crimes and Intellectual Property Section of the Office of Enforcement Operation, DOJ, for proper language of the search warrant.

## Transactional Records

Under Title 18 U.S.C. 2703(c ), transactional records, to include name, address, local and long distance telephone connection records, length of service, telephone or instrument number or identity including any temporarily assigned network address, and means and source of payment for such service (including any credit card or bank account number), may be obtained through following ways:

1. A search warrant issued by court of jurisdiction,
2. A court order issued by court of competent jurisdiction,
3. By a consent of the subscriber,
4. A formal written request relevant to an investigation concerning telemarketing fraud,

Unlike other sections, notice to a subscriber is not required under this section.

**Backup records** may be obtained by court order or subpoena (18 U.S.C. 2704). Time limitations relating to the maximum duration of such orders, etc. are again not applicable. As to notification, once a backup copy of an electronic communication has been created (within two days of the individual's or company's receipt of a court order or subpoena), notice shall be made to the subscriber or customer within three days of the receipt of confirmation that the backup copy has been created. Such notification shall be made by the Governmental entity unless such notice is delayed pursuant to section 2705 (a).

**"...the service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider-**

**...has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and**

**...has not initiated proceedings to challenge the request of the governmental entity ..."** (18 U.S.C. 2704(4) (A) (B))

Finally, **transactional records** may be obtained through consent, court order, subpoena, or warrant, with no time limit or notification requirements.

## Backup Preservation

Regarding backup record preservation (18 U.S.C. 2704), the Secret Service, acting under 18 U.S.C. 2703(b)(2), may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications.



With no notification given to the subscriber or customer of such subpoena or court order, a service provider must create such a backup copy as soon as practicable consistent with its regular business practices, and shall confirm to the Secret Service that such a backup copy has been made. Such a backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order. Additional provisions under 18 U.S.C. 2704 cover the rights of a service provider to destroy a backup record copy and the rights of the subscriber or customer to quash such a subpoena or court order.

## Delayed Notice

Under Title II, the Secret Service may request a delay of up to ninety (90) days in the notification of a customer or subscriber of grand jury subpoena, or administrative subpoena as outlined in 18 U.S.C. 2705, upon written certification by a supervisory official that such notification as required by 18 U.S.C. 2703(b) may have an adverse result. Such an adverse result is defined in 18 U.S.C. 2705 as:

1. Endangering of the life or physical safety of an individual;
2. Flight from prosecution;
3. Destruction of or tampering with evidence;
4. Intimidation of potential witnesses; or
5. Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

It should be noted that a true copy of any such certification shall be maintained by the Secret Service. Extensions of the delay of notification up to ninety days each may be granted by the court upon application by this Service.

## Cost Reimbursement

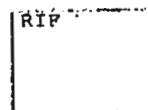
Except as otherwise provided, the Secret Service, in obtaining communications, records, or other information under sections 2702, 2703 or 2704 of Title 18, shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise producing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information might be stored.

The amount of the fee shall be mutually agreed upon by the Secret Service and the person or entity providing the information. In the absence of agreement, the fee shall be determined by the court which issued the order for production of such information. If no court order was issued, the fee shall be determined by the court before which a criminal prosecution relating to such information would be brought. This payment requirement does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of Title II. A court may,

however, order payment as previously described if the court determines the information required is unusually voluminous in nature or otherwise has caused an undue burden on the provider.

In conclusion, Title II (Chapter 121, Title 18, U.S.C. 2701 to 2712) represents a comprehensive tool to be used in investigations by the Secret Service. Where case law precedent is not firmly established in this area, care must be taken in its use. Timely consultations with the Office of the United States Attorney are recommended, as well as review and understanding of the terminology outlined in 18 U.S.C. 2510 and 18 U.S.C. 2711.

**Finally, all personnel in dealing with any of the matters covered in this manual should be fully aware of the range of civil and criminal sanctions incorporated under the Electronics Communications Privacy Act of 1986 (Titles I, II, and III).**



# **MySpace.com**

## **Law Enforcement Guide**

**Last updated November 1, 2007**

### **Mailing Address:**

Custodian of Records  
MySpace.com  
407 N. Maple Drive  
Beverly Hills, CA 90210

### **Law Enforcement Telephone Hotlines:**

Phone: 888-309-1311  
Fax: 310-356-3485

### **Law Enforcement Email Address:**

LawEnforcement@MySpace.com



## Table of Contents

I.	Preface.....	3
II.	General Information about MySpace and Law Enforcement Requests.....	3
III.	Information Collected and Retained, and Legal Process Required .....	4
IV.	Information that may Reside on a MySpace User's Computer (not with MySpace).....	7
V.	Requests to Preserve Records .....	8
VI.	Service of Process and Production of Records .....	8
VII.	Interpreting Information Produced by MySpace .....	9
VIII.	User Consent.....	11
IX.	Emergency Disclosures.....	11
X.	Sample Language for Requests.....	11
XI.	Websites and Resources.....	14
XII.	Information to Provide to Parents and Schools.....	14

## **I. Preface**

MySpace.com (“MySpace”) is committed to assisting law enforcement, to the extent permitted by law, in investigations related to unlawful activity. This Law Enforcement Guide is designed to serve that purpose by providing information to facilitate law enforcement requests for user data held by MySpace. The Guide specifies what information is collected by MySpace, how long that information is retained, how to tailor requests to ensure MySpace produces the specific information sought, and the legal process necessary to permit MySpace to disclose different types of information. Finally, the Guide provides contact information for MySpace personnel dedicated specifically to responding to law enforcement requests, including emergency requests.

Because MySpace wishes to prioritize law enforcement requests, it has established dedicated lines of communication reserved solely for law enforcement. This Guide is intended solely for use by bona fide law enforcement agencies and may not be distributed to any other person or organization without the express written authorization of MySpace. MySpace will require verification that the person requesting this Guide is a bona fide law enforcement officer or acting on behalf of a law enforcement agency or prosecutor’s office prior to releasing this Guide.<sup>1</sup>

## **II. General Information about MySpace and Law Enforcement Requests**

The MySpace service empowers millions of users to communicate with a worldwide network of friends. MySpace is a free online social networking service that allows users to create their own profile pages, which can include lists of their favorite musicians, books and movies, photos of themselves and friends, and links to pages within and outside the MySpace environment. The service also permits users to send and receive private messages (the functional equivalent of emails) with other MySpace users, and to restrict the disclosure of certain information (blogs, profile information) exclusively to their MySpace friends. Users have extensive control over their own accounts, both with regard to the identity information they provide, and in their ability to retain or delete information stored in their profiles. Finally, the MySpace site has extensive help pages that may assist law enforcement in determining if the information sought is publicly available, and may further assist law enforcement in understanding the particular features offered. The MySpace help pages can be found via a link at the top right hand corner of the MySpace.com home page.

MySpace is committed to assisting law enforcement investigations to the fullest extent, consistent with applicable law. The primary set of laws governing MySpace’s ability to disclose

---

<sup>1</sup> This Guide is the property of MySpace and MySpace reserves the right to change any of the policies stated in this Guide at any time without notice. MySpace will make reasonable efforts to inform law enforcement of any significant changes in policies or procedures through updates to this Guide. The information in this Guide is not intended to create any enforceable rights against MySpace.

user information is found in the Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq. ("ECPA"). ECPA mandates that MySpace may disclose certain user information to law enforcement only in response to specific types of legal process, including subpoenas, court orders, and search warrants. Generally speaking, ECPA permits the disclosure of basic user identity, log-in information, and stored files in response to a subpoena; but requires a court order under § 2703(d) to disclose additional user records (such as message headers), or a search warrant to authorize disclosure of content (such as private messages). Should you seek further clarification about ECPA's restrictions on providers like MySpace, we suggest you contact the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) at 202-514-1026.

### **III. Information Collected and Retained, and Legal Process Required**

#### **A. Information Overview**

MySpace has four basic types of information about its users that may be relevant to a criminal investigation: 1) basic identity/subscriber information supplied by the user in creating the account; 2) IP log-in information captured by MySpace from the user's computer; 3) files stored in a user's profile (such as "about me" information or lists of friends); and 4) user sent and received message content. Depending on the type of information sought, ECPA may require the use of a different form of legal process, and the period MySpace retains the information may differ. In order to assist law enforcement in narrowly tailoring its requests and ensuring the necessary process is provided, we identify below the specific categories of information and corresponding process required to lawfully produce that information under ECPA. When drafting subpoenas, court orders, or search warrants, please be as specific as possible about the profile at issue, and the nature of the information sought. Clearly worded requests will reduce confusion, enable MySpace to respond more quickly, and ensure that no issues arise under ECPA limiting MySpace's ability to comply.

#### **B. Public vs. Private Profiles**

Please note that users may choose whether to make certain profile information (e.g., their "about me" details, blogs, and friends lists) publicly viewable and available to anyone visiting their profile (including law enforcement), or to keep it private and limited only to the MySpace "friends" of their choosing. For public profiles, law enforcement may access and save screen shots of publicly available information without involvement by MySpace. Because users can change the content on their profile and change the status from public to private at any time, MySpace encourages law enforcement to preserve content on public profiles themselves by using screen shots (preserving electronic copies of html files).

#### **C. Identifying the "Friend ID"**

As a threshold matter, given the size of MySpace's user population, it is critical and required that the 'FriendID' of the relevant account be included in the legal process. The FriendID can be located in the web address of the profile in question.

Example of FriendID for Tom's profile:

<http://www.myspacc.com/index.cfm?fuseaction=user.viewProfile&friendID=6221&Mytoken=20050518161358>

The above FriendID in this example is '6221'. This unique number allows us to locate the profile. If the profile appears as 'MySpace.com/Tom', click on the 'View More Pics' link. This will display the following link:

<http://viewmorepics.myspace.com/index.cfm?fuseaction=user.viewPicture&friendID=6221&friendName=Tom&Mytoken=20050829192700>

The FriendID can then be located in the URL.

**D. Specific Categories of Information Retained and Associated Legal Process Required**

**1. Basic user identity information**

*Type of Information Available:* date profile created; first and last name provided by user; user ID; e-mail address provided by user; zip code, city, and country provided by user; account creation date and time; and the IP address at time of sign-up.

*Process required:* Grand jury subpoena, administrative subpoena or civil investigative demand pursuant to 18 U.S.C. § 2703(c)(2); or court order; or search warrant; or user consent.

**2. IP address logs**

*Type of Information Available:* Logs showing the IP address assigned to the user and the date stamp at the time the user accessed his or her profile (PST or PDT, depending on the date of log-in).

*Process required:* For historical records - grand jury subpoena, administrative subpoena or civil investigative demand under 18 U.S.C. § 2703(c)(2); or court order; or search warrant; or user consent. To capture log-in IPs prospectively - a Pen Register/Trap and Trace Order under 18 U.S.C. § 3121.

**3. Private messages and bulletins**

*Type of Information Available:* the contents of private mail messages and/or bulletins sent from and held for users on MySpace servers.

*Process required for messages less than 180 days old:* Search warrant under 18 U.S.C. § 2703(a); or user consent.

*Process required for messages over 180 days old:* Subpoena or court order where the government provides prior notice to the subscriber (or delays notice under 18 U.S.C. § 2705) for messages over 180 days old; or search warrant; or user consent.

#### **4. Stored user files (photos, videos, blogs)**

*Type of Information Available:* Profile information including photos, videos, blogs, blog comments by other users, the identities of their friends, and "About Me" entries.

*Process required:* A grand jury or administrative subpoena, civil investigative demand; or court order where the government provides prior notice to the subscriber (or delays notice under 18 U.S.C. § 2705), 18 U.S.C. § 2703(b)(2); or search warrant; or user consent.

#### **5. Other general records or information**

*Type of Information Available:* user's date of birth, gender, hometown, and occupation, as well as historical private message header information, excluding subject.

*Process required:* Court order under 18 U.S.C. § 2703(d); or search warrant; or user consent.

### **E. MySpace Retention Periods**

The retention periods identified below reflect MySpace's retention of user data in the normal course of business. MySpace honors all law enforcement preservation requests made during the period the data is available. MySpace also automatically preserves the data of users who are identified as registered sex offenders and removed from the MySpace site pursuant to MySpace's Sentinel SAFE project.<sup>2</sup> Please note that all retention periods are estimated and may vary depending on system conditions and other circumstances.

#### **1. Active Accounts**

##### **a. Basic user identity information, stored user files, and general records:**

The basic identity information entered by a user in creating a profile, all data displayed on the profile (blog entries, about me information, etc.) and all stored files (images and videos) contained in an account are maintained as long as the user has not edited the data or removed the files from the profile. Once a change is made by the user, the previously existing information is overwritten. Upon receipt of a preservation request, however, MySpace will capture all user data available at that time, and future actions by the user will not affect the preserved data.

---

<sup>2</sup> MySpace's Sentinel SAFE project is designed to identify and remove from the MySpace site any users identified as registered sex offenders. MySpace deletes all profiles identified by the Sentinel SAFE process as RSOs within approximately 24 hours of making a conclusive match. Importantly, when MySpace deletes a profile as a result of a registered sex offender match with the Sentinel SAFE database, the information contained in and related to the profile, including photos, private messages, etc. are preserved by MySpace. Upon receipt of the appropriate legal process for the information sought, MySpace will promptly produce this preserved user information.

b. IP address logs:

The IP Log for each FriendID is logged after every log in to the MySpace system. The IP Log for each FriendID is available for one year after the applicable login on the account. This data cannot be modified by the user once it is recorded.

c. Private messages and bulletins:

Private messages in a user's inbox are available until the user removes them. MySpace does not maintain copies of messages marked for deletion by a user and cannot recover deleted messages. Private messages in a user's sent box are retained for 14 days unless the user has manually deleted them.

2. Deleted Accounts

a. Basic user identity information, stored user files, and general records:

User identity information is available for one year after account deletion. Other stored files, such as photos, may be lost at the time of account deletion.

b. IP address logs:

MySpace retains Friend ID, IP Address and Login time and date stamps dating back one year.

c. Private user communications:

No private messages (inbox or sent mail) are available for deleted accounts (except those deleted through our Sentinel SAFE project).

#### **IV. Information that may Reside on a MySpace User's Computer (not with MySpace)**

Available Forensic Evidence includes:

A. Instant Messenger Chat Logs: MySpace Messenger IM Client logs may be stored to the local machine. The default pathway for these logs is C:\Documents and Settings\USERNAME\Application Data\MySpace\IM\Conversations. For a machine running Windows Vista, the default pathway is C:\Users\USERNAME\AppData\Roaming\MySpace\IM.

B. Cookie Data: If a user logged into that machine accessed MySpace.com, and did not clear their cookies, you can locate cookies in the C:\Documents and Settings\Username\Cookies directory. The cookies will be named 'username@word.myspace.com'

C. Cached MySpace Pages: Electronic copies of viewed MySpace pages will be stored to the local machine temporarily (until the user or machine flushes them out). The default

location for these files is C:\Documents and Settings\Username\Local Settings\Temporary Internet Files. Images viewed by the user that were stored on MySpace will also be stored here.

D. Stored login information: Sites and browsers allow users to 'save' their login settings. Check form fields in the browser to see if they have pre-populated information.

## V. Requests to Preserve Records

MySpace honors requests by law enforcement to preserve information in accordance with 18 U.S.C. § 2703(f). In response to such requests, MySpace will preserve the specific information identified in the request for up to 180 days and will extend the preservation as necessary at your request. Please email or fax a signed letter on law enforcement agency letterhead requesting that MySpace preserve the records to 310-356-3485. Please specifically list the particular information that you seek to preserve, and limit your preservation request to information for which you intend to seek legal process. Attached in our form section is a sample letter for a preservation request.

MySpace can only preserve a currently active (non-deleted) account. Please note that once information in an active account has been preserved, the following will occur unless other arrangements are made with MySpace and indicated in the request:

- The account will remain publicly viewable; and
- The user will be prevented from logging into the account.

*If restricting the user's access to the profile will impede an investigation, you must specifically request in the letter that the subject account should not be locked.* In such cases, MySpace will output to a flat file the specific information for which preservation is sought that is available at the time the request is processed. Because the user will retain access to the account, please note that any interim changes to account information made between the time the flat file is created and the ultimate legal process is served may not be retained. Accordingly, when serving follow-up legal process for information previously the subject of a preservation request, please specify that the request seeks both the information preserved and any existing updated user profile information. Please also reference any prior preservation requests so that we may respond to your legal process more efficiently.

## VI. Service of Process and Production of Records

In order to streamline the process for satisfying law enforcement requests, MySpace will accept service of all subpoenas, court orders, search warrants, emergency requests and user consents by fax (310-356-3485), by email to [compliance@myspace.com](mailto:compliance@myspace.com) or mail (at the address on the cover of this Guide). MySpace will also accept service and produce documents in response to out-of-state domestic subpoenas, court orders, and search warrants.

MySpace's preferred method for producing information in response to legal process is to submit the information in an Excel spreadsheet sent via e-mail. MySpace can also provide a signed authentication letter for the production by PDF or Fax. Accordingly, where possible,

please specify on the applicable subpoena, order or warrant (or cover letter) the email address to which results can be sent and where an authentication letter can be faxed (if you prefer to have the letter faxed).

## **VII. Interpreting Information Produced by MySpace**

The explanations provided below are intended to assist law enforcement in understanding the meaning of the information produced by MySpace, and respond to the most frequently asked questions about MySpace productions.

### **A. Email Address**

Please note that an email address consists of two parts: A username and then the domain that hosts the email account.

Example: Abuse@MySpace.com

'Abuse' is the username and all information after the '@' belongs to the domain (which in this case is MySpace.com). Therefore, you should contact MySpace.com to make inquiries about the username 'Abuse'. If the email domain belongs to a different ISP (e.g., MSN, AOL, Yahoo, or Gmail), then information about that email address should be sought from that provider.

### **B. IP Address Logs**

IP (Internet Protocol) Logs include the IP address assigned to the user (by their ISP (Internet Service Provider)) at the time of login, and also include a date stamp showing when the login occurred. All IP logs provided by MySpace.com are Pacific Standard or Pacific Daylight Time, depending on the date of log-in. Please refer to the month and day on the log to determine whether PDT or PST is applicable.

Example: 67.134.143.254 08/22/2005 3:15 PM PST

You can find out which Internet Service Provider the IP address belongs to by performing a "Whois" lookup on the IP address at any of the following sites:

<http://whois.domaintools.com> or <http://www.networksolutions.com/cgi-bin/whois/whois>

The IP Address in the example above (67.134.143.254) generated the following result:

Qwest Communications QWEST-BLKS-5 (NET-67-128-0-0-1)

67.128.0.0 - 67.135.255.255

This result means the IP address belongs to Qwest Communications. Qwest Communications could be contacted to provide the information about what individual or company was using that IP address at that date and time.



### C. Private Messages

Private messages will be produced in Excel spreadsheet form, with two separate tabs on the bottom of the spreadsheet for messages. One tab is the 'Sent From User' messages (user's sent mail) and the other is 'To User' (user's inbox).

The spreadsheet for private messages will have the following five headers:

ToUserid	FromUserid	Subject	Body	CreatedDate
----------	------------	---------	------	-------------

ToUserid is the FriendID of the account the message is sent to.

FromUserid is the FriendID of the account the message is sent from.

Subject is the subject line of the message in question.

Body is the actual content of the message.

CreatedDate is the date stamp of the message.

Example:

ToUserid	FromUserid	Subject
6221	22234567	RE: Welcome to MySpace.com

Body

Thank you Tom for the welcome!

----- Original Message -----

From: <A  
HREF='http://www.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=6221&Myt  
oken=20050423222742'>Tom</a> Date: Apr 23, 2005 4:49 PM

Hi, My name is Tom! Welcome to MySpace

CreatedDate

4/23/2005 22:29

Please note the '----- Original Message -----' in the body of the message and the 'Re' ("Regarding") in the subject line shows that the user in question is responding to an existing private message sent to him. The responding email shows who the original sender is, as well as the time and date sent.

## **VIII. User Consent**

Because ECPA provides an exception for disclosures of information with the consent of the user, MySpace will disclose information based on user consent obtained by law enforcement where sufficient information is provided to verify that the person providing the consent is the actual creator of the profile, and where law enforcement endorses the authenticity of the consent. Accordingly, in addition to a description of the specific information sought, the user must provide the information called for in the sample Consent Form set out below. MySpace will be unable to release the information if the user is unable or unwilling to provide registration information that correlates to the information in MySpace user records.

## **IX. Emergency Disclosures**

Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), MySpace is permitted to disclose information, including user identity, log-in, private messages and other information voluntarily to a federal, state, or local governmental entity when MySpace believes in good faith that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay. MySpace will disclose records to assist law enforcement in the case of emergencies meeting ECPA's threshold requirements. Accordingly, we request that law enforcement provide information in writing sufficient to show the existence of the emergency. If you find it useful, you may provide the information requested in MySpace's Emergency Disclosure Form (contained below) on your Law Enforcement letterhead. Providing such information will ensure that true emergencies receive the swiftest response. The Emergency Disclosure request must be submitted by a law enforcement officer.

For emergency law enforcement requests, MySpace also reserves a special telephone hotline that MySpace staffs 24 hours a day/7 days a week. The emergency hotline is 888-309-1311.

## **X. Sample Language for Requests**

This section provides sample language that law enforcement may use to complete the section of their legal process identifying the information they seek from MySpace. These are examples of the most commonly requested information from MySpace. It is important to be as specific as possible when identifying the information you are requesting from MySpace.

### **A. Sample Subpoena Language for Basic User Identity Information and IP logs:**

Records concerning the identity of the user with the FriendID ##### consisting of name, postal code, country, e-mail address, date of account creation, IP address at account sign-up, and logs showing IP address and date stamps for account accesses

**B. Sample Search Warrant Language for User Information Including Private Messages:**

Records concerning the identity of the user with the FriendID ##### consisting of name, postal code, country, e-mail address, date of account creation, IP address at account sign-up, logs showing IP address and date stamps for account accesses, and the contents of private messages in the user's inbox, and sent mail folders.

**C. Sample Preservation Request Letter**

(Must be on law enforcement department letterhead)

Custodian of Records  
MySpace.com  
407 N. Maple Drive  
Beverly Hills, CA 90210

Re: Preservation Request

Dear Custodian of Records:

The below listed account/profile is the subject of an ongoing criminal investigation at this agency, and it is requested pursuant to 18 U.S.C. § 2703(f) that the following information associated with said account/profile be preserved pending the issuance of a search warrant or other legal process seeking disclosure of such information: [Specify information to be preserved]. I understand that MySpace.com will lock the profile/account in question, thereby rendering the account inaccessible to its owner.

Profile URI:

FriendID:

If you have any questions concerning this request please contact me at [insert e-mail address and phone contact]

Thank you for your assistance in this matter.

Sincerely,  
(Your Signature)  
(Your Name Typed)  
(Your Title Typed)

**D. Sample Consent Form**

(Must be on the investigating agency or department letterhead)

I, "XYZ", being duly sworn, on this [insert date] do hereby state the following:

I have one or more profiles on MySpace.com.

The URLs / FriendIDs are:

\_\_\_\_\_  
\_\_\_\_\_

I understand that the "ABC" agency is conducting an official criminal investigation and has requested that I grant my consent to authorize the "ABC" agency to access, request, receive, review, copy and otherwise utilize, as they deem appropriate, the following information from the above profiles: [specify information sought]

I hereby authorize MySpace.com to provide to any agent of the above referenced agency, the above-specified information associated with my identified MySpace.com profiles/accounts.

The following information should be used to verify my identity:

Email address for account: \_\_\_\_\_

Password for account: \_\_\_\_\_

Date of birth for account: \_\_\_\_\_

Zip Code for account: \_\_\_\_\_

Pursuant to this Consent, I waive any claims against, indemnify and hold harmless MySpace.com, its affiliates, and their respective directors, officers, agents, and employees from and against any claims, damages or expenses relating to or arising from, in whole or in part, the disclosure of such information, records and data.

I have not been promised anything in exchange for providing this consent and authorization.

In witness whereof, the undersigned makes the above statements under penalty of perjury.

Member Signature and Printed Name                      Date

Law Enforcement Witness Signature, Printed      Date  
Name and Printed Title

### **E. Sample Emergency Disclosure Form**

(Must be on the investigating agency or department letterhead)

#### **Emergency Disclosure Form**

Please complete this form to assist MySpace in exercising its discretion to disclose information to you pursuant to 18 U.S.C. § 2702(b)(7) and § 2702(c).

1. What is the nature of the emergency involving death or serious physical injury?
2. Whose death or serious physical injury is threatened?
3. What specific information in MySpace's possession related to the emergency do you need?

\_\_\_\_\_  
Signature of Officer

\_\_\_\_\_  
Printed Name of Law Enforcement Officer

## **XI. Websites and Resources**

[www.myspace.com/safety](http://www.myspace.com/safety) - MySpace.com's Safety Tips section which includes a section dedicated to parents concerned about their child's Internet use.

United States Department of Justice, Computer Crime and Intellectual Property Section,  
[www.cybercrime.gov](http://www.cybercrime.gov) - DOJ guidance on authorities governing obtaining electronic evidence.

United States Department of Justice, Office of Justice Programs, National Institute of Justice - publishes an investigative guide for electronic crime. The information contained in Electronic Crime Scene Investigation-A Guide for First Responders (available free of charge and downloadable from the Department of Justice website ([www.ncjrs.org/pdffiles1/nij/187736.pdf](http://www.ncjrs.org/pdffiles1/nij/187736.pdf))) helps line officers perform their jobs.

[www.ncmec.org](http://www.ncmec.org) - National Center for Missing and Exploited Children website.

## **XII. Information to Provide to Parents and Schools**

### **A. Parent Resources**

MySpace offers information for parents concerned about their child's use of MySpace on the bottom of every single MySpace.com page.

[www.myspace.com/safety](http://www.myspace.com/safety) is the web address for the Safety Tips section. Click on the 'Tips for Parents' tab to access the parent section.

This area offers:

Internet safety tips for parents to communicate to their child.

Step by step instructions on how to remove a MySpace account.

Links to monitoring software and additional safety related information.

Contact information for MySpace for further assistance.

A parent pamphlet available for download and distribution.

**B. School Resources**

MySpace has a team dedicated to assisting with school related issues. Please have your local school email [SchoolCare@MySpace.com](mailto:SchoolCare@MySpace.com) in regards to teacher identity theft, school threats, the school forums on MySpace, or any other school related issue. There is also a School Administrator's Guide available to school administration that they can request at [SchoolCare@MySpace.com](mailto:SchoolCare@MySpace.com).

# MYSACE LAW ENFORCEMENT GUIDE

## QUICK REFERENCE SHEET

24/7 HOTLINE: 888-309-1311 FAX: 310-356-3485 EMAIL: LawEnforcement@MySpace.com

CRIMINAL	Type of Information Sought	Subpoena (Admin., Grand Jury, Trial, CID)	2703(d) Order	Search Warrant	PenTrap Order
	Basic Subscriber Information		✓	✓	✓
IP addresses		✓	✓	✓	
Private messages (sent/inbox) less than 180 days				✓	
Private messages (sent/inbox) older than 180 days		✓	✓	✓	
Private message headers (subject lines redacted)			✓	✓	
Subject lines in private message headers				✓	
Stored user files (blogs, images, friends)		✓	✓	✓	
Realtime capture of IP log-ins					✓

### IMPORTANT REMINDERS

1. **Friend IDs** - Please provide the FriendID/URL in all requests.
2. **Specificity** - Please describe the data sought as specifically as possible.
3. **Preservation** - MySpace will preserve data when requested to do so under 18 U.S.C. 2703(f) - please refer to the full Law Enforcement Guide for more details.
4. **Emergencies** - MySpace will provide Law Enforcement with user data where Law Enforcement provides sufficient information to give MySpace a good faith belief that a threat of death or serious injury requires disclosure - please refer to the full Law Enforcement Guide for more details or call our hotline listed above.

**Confidential: For Law Enforcement Use Only**

## **Law Enforcement Information Handout**

*Prepared by MySpace.com 09/02/2005*

### **Mailing Address:**

Custodian of Records  
MySpace.com  
1333 2<sup>nd</sup> Street, First Floor  
Santa Monica, CA 90401

### **Email Address:**

lawenforcement@MySpace.com

### **Telephone Numbers:**

Phone: 310.917.4949 x8  
Fax: 310.394.4180

### **Overview of MySpace.com**

MySpace.com is a free, online community, where millions of individuals create individual 'web page profile', and communicate easily with other users.

We recommend creating an account to understand the full functionality of the site. Users create profiles for themselves, in which they can upload images, post journal entries ("blogs"), post comments on their friends' profiles, and send private messages to other MySpace.com members. You can add/be added to a 'Friends List', in which all people on your Friends List will show up on your profile page (and conversely, you will show up on their profile pages).

### **Information Collected at Signup**

Here are screenshots of how a user creates an account. Please note that this is all the information we collect about a user during sign up:



Already a member? [Click Here to Log In](#)

**JOIN MYSPACE HERE!**

Email Address:

First Name:

Last Name:

Password:

Confirm Password:


Country:  ▼


Postal Code:  (required for US, UK & Canada only)

Gender:  Female  Male

Date Of Birth:  ▼ /  ▼ /  ▼

By checking the box you agree to the MySpace [Terms of Service](#) and [Privacy Policy](#)

Verification:   
Please enter the text from the image above:



**Available Information**

Most profile information is publicly viewable and available. Publicly available information includes journal entries (in most cases), images, user comments, and public profile information.

In order to make an electronic copy of the profile, save the webpage(s) and files on your own computer. Do this before it gets modified or deleted. While viewing the profile in question, click your browser's File (in the upper left-hand corner) then click 'Save As'. Make sure to do the same for all journal entries and the image gallery.

To request the following information from MySpace.com, we require a subpoena:

- IP logs (recorded at time of login)
- Dates and times of login (PST)
- Email address
- Zip code



- Name
- Private Messages

Please note that all information above is not necessarily accurate. Users do not need to confirm their email address, nor provide verified information. Users may also fake IP addresses if they use a proxy.

Please note that we do not have street address or credit card information. MySpace.com is a free site and does not require credit card use at any time.

MySpace may disclose private information to law enforcement without a subpoena in limited, emergency situations in which the safety of a MySpace user or member of the public is at risk and there is insufficient time for the law enforcement agency to obtain a subpoena. In these circumstances, MySpace will require the delivery of a signed statement on law enforcement letterhead certifying the existence of an emergency and supplying all the information that would be required in a subpoena.

#### **Length of time MySpace.com retains records**

##### **Active Accounts**

##### **Data/Images on an active account**

MySpace.com does not retain information that is altered/removed on an active profile. Once a change is made, existing information is overwritten.

##### **IP Logs**

IP Logs are available for up to ninety days after a user's last login.

##### **Private Messages in an active account**

User's Inbox – Retained until user removes them. We cannot recover that message unless it is in another user's Sent Mail.

Sent Mail – Retained for 14 days.

Trash Mail – Retained 30 days or less. Users can empty their trash at any time.

##### **Deleted Accounts**

No mail is available for deleted accounts.

User ID, IP Address, Login date stamps are retained for up to 90 days after account deletion.

Profile information is available for up to ten days after account deletion.

##### **Preserving an account**

A letter of preservation can be faxed to MySpace.com. Please note the following regarding preserved accounts:

- They are still publicly viewable



- The user will not be able to log into the account
- We can only preserve a currently active (non-deleted) account
- Information in the Sent Mail/Trash can is still subject to automatic deletion.

If restricting the user's access to the profile will impede an investigation, you can request that private messages be output to flat file for preservation before a subpoena is served.

#### **Court Order/Subpoena Language**

The time will come when you need to draft a subpoena in order to request private information. MySpace.com has millions of users -- you MUST state the 'FriendID' in the subpoena of the account(s) you need information for. The FriendID can be located in the web address of the profile in question.

Example of FriendID for Tom's profile:

<http://www.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=6221&Mytoken=20050518161358>

The above FriendID in this example is '6221'. This allows us to locate the profile. If the profile appears as 'MySpace.com/Tom', click on the 'View More Pics' link. This will display the following link:

<http://viewmorepics.myspace.com/index.cfm?fuseaction=user.viewPicture&friendID=6221&friendName=Tom&Mytoken=20050829192700>

The FriendID can then be located in the URL.

When requesting information, please use the following exact phrases for whichever parts of information you need:

- "Email Address"
- "IP Logs" (which includes the timestamps of the IP logs at login)
- "Private messages in the user's Inbox, Trash and Sent Mail"

Please be as specific as possible in the subpoena as to what information you are requesting. For example, "Request for FriendID 6221 IP logs, email address and private messages located in the user's Inbox and Sent Mail Records for date range 5/14/2004-6/16/2005."

We can respond to court requested information with approximately a two-week turnaround. The preferred way to transmit requested data is via E-mail, as it will be in an Excel spreadsheet. Therefore, if possible, specify on the subpoena document the email address results can be sent to.

MySpace.com will accept subpoenas delivered by fax or mail. We also respond to out-of-state subpoenas.

### Deciphering the information sent from MySpace.com

#### Email Address

Please note that an email address consists of two parts: A username and then the domain that hosts the email accounts.

*Example: Abuse@MySpace.com*

'Abuse' is the username and all information after the '@' would belong to the domain (which is MySpace.com). Therefore, you would want to contact MySpace.com to make inquiries about the username 'Abuse'.

#### IP Logs

IP Logs also include a date stamp. All IP logs are Pacific Standard Time zone.

*Example: 67.134.143.254 08/22/2005 3:15 PM PST*

You can find out which Internet Service Provider the IP address belongs to by going to a Reverse DNS site, such as <http://www.whois.sc> and entering the IP address into a search field.

The example in question generated this as the following result:

*Qwest Communications QWEST-BLKS-5 (NET-67-128-0-0-1)  
67.128.0.0 - 67.135.255.255*

That means the IP address belongs to Qwest Communications. You will then need to contact Qwest Communications to see what individual or company was using that IP address at that date and time.

#### Private Messages

There will be two separate tabs on the bottom of the Excel spreadsheet for the Private Messages. One is the 'Sent From User' and the other is 'To User'. These are messages that are sent from the user in question to other users and that are located in the user's "Sent Mail" records, and messages from other users to the user in question that are located in the user's "Inbox" records.

The spreadsheet for private messages will have the following five headers:

ToUserId	FromUserId	Subject	Body	CreatedDate
----------	------------	---------	------	-------------

ToUserId is the User ID of the account the message is sent to.



FromUserid is the User ID of the account the messages is sent from.  
Subject is the subject line of the message in question.  
Body is the actual content of the message.  
CreatedDate is the date stamp of the message.

*Example:*

<u>ToUserid</u>	<u>FromUserid</u>	<u>Subject</u>
6221	222345245322	RE: Welcome to MySpace.com

Body

Thank you Tom for the welcome!

----- Original Message -----

From: <A

HREF='http://www.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=6221  
&Mytoken=20050423222742'>Tom</a> Date: Apr 23, 2005 4:49 PM

Hi, My name is Tom! Welcome to MySpace

CreatedDate

4/23/2005 22:29

Please note the '----- Original Message -----' in the body of the message and the 'Re' (as in Reply) in the subject line shows that the user in question is responding to an existing private message sent to them. The responded email shows who the original sender is, as well as the time and date sent.

Overview of MySpace.com's Terms of Use Agreement

MySpace's Terms of Use Agreement contains the rules for use of the site by users. Unfortunately, as with any set of rules, the rules governing the use of MySpace are violated by users from time to time. We are not always able to identify those violations in a timely manner.

- These are some of the key points in our Terms of Use Agreement:  
Users must be age 16 or older to be on MySpace.com.
- Users are not allowed to post personally identifiable information on their profile (last names, telephone numbers, addresses, etc)
- Users are not allowed to use the site for commercial purposes
- Users are solely responsible for the content they publish and display
- Members are responsible for their personal disputes with other members
- We reserve the right to delete any profile from our service
- We may review "private" content at our discretion



### Overview of Safety Settings

MySpace.com offers a range of settings for users to protect themselves from unwanted attention.

- Block user – This will prevent users from being able to private message or post comments/journal responses on another user's profile.
- Restricting journal entries to friends only.
- Privacy Settings – Hide online status, approving comments, requiring email/last name in order to add as a friend, Friend only Blog comments and Friend only Group invite.
- IM Privacy Settings – Controls who can instant message a user.

### Cybercrime Websites and Resources

[www.whois.sc](http://www.whois.sc): Reverse DNS and Website lookup to see who owns an IP address or Web Address.

[www.wiredsafety.org](http://www.wiredsafety.org): Resource for online safety

The Facebook logo, consisting of the word "facebook" in a white, lowercase, sans-serif font, centered on a solid black rectangular background.

## **Facebook Law Enforcement Guidelines**

This document describes procedures law enforcement authorities should follow to request data from Facebook.

This document is **CONFIDENTIAL** and intended for law enforcement use only. Please do not redistribute it without the express written permission of Facebook.

Facebook services continuously change and the company may modify these policies without notice. This version was released in May, 2010. Contact Facebook at [subpoena@facebook.com](mailto:subpoena@facebook.com) to request the latest version of these guidelines.

FACEBOOK CONFIDENTIAL AND PROPRIETARY  
© Facebook, Inc. 2010. All Rights Reserved.

**Address**

All requests for records must be sent one of three ways:

- By fax to (650) 644-3229
- By e-mail to [subpoena@facebook.com](mailto:subpoena@facebook.com)
- By mail to: Facebook, Inc.  
Attn: Security Department/Custodian of Records  
1601 California Avenue  
Palo Alto, CA 94304

**Type of Request**

All requests for records should clearly identify the type of request in the subject line. Only the following types of requests will be accepted:

- **Preservation Requests.** For requests that identify an account by User ID, Username or email address, we will preserve then-existing account records for 90 days, pending service of formal legal process.
- **Formal Legal Requests.** For requests pursuant to formal compulsory legal process issued under U.S. law, we will provide records as required by law. Response times vary depending on case complexity and records requested.
- **Emergency Requests.** Emergency requests must be made using the attached Emergency Request Form, and will only receive a response if we believe in good faith that serious bodily harm or death of a person may occur if we do not respond quickly.

**Important Considerations**

You should review the Facebook Statement of Rights and Responsibilities to understand more about rules of conduct on Facebook. In particular you should be aware of the following, as they may impact your investigation:

- We will always disable accounts that supply false or misleading profile information or attempt to technically or socially circumvent site privacy measures.
- We are required to disable accounts engaged in illegal activity, even if that activity is brought to our attention through a request for records.

If disabling or restricting user access to the user's profile will jeopardize your investigation, you should clearly specify "**DO NOT DISABLE UNTIL XX/XX/XXXX**" on your request. Please note however, if the matter has already been reported independently to our operations team, they may take independent action.

By default we will return data no older than 90 days prior to the date we receive the request. You must specify a date range or specific date if you need information outside that range.



FACEBOOK CONFIDENTIAL AND PROPRIETARY  
© Facebook, Inc. 2010. All Rights Reserved.

**Types of Data**

Depending on the type of formal legal process provided, we will be able to respond with one or more of the following types of data:

*Basic Subscriber Information* (sometimes referred to as Neoselect) will be delivered in XML format and may include:

- User Identification Number
- E-mail address
- Date and Time Stamp of account creation date displayed in **Coordinated Universal Time**
- Most Recent Logins (generally captures the last 2-3 days of logs prior to processing the request) in **Coordinated Universal Time**
- Registered Mobile Number

*Expanded Subscriber Content* (sometimes referred to as Neoprint) will be delivered in PDF format and may include:

- Profile Contact Information
- Mini-Feed
- Status Update History
- Shares
- Notes
- Wall Postings
- Friend Listing, with Friends Facebook ID's
- Groups Listing, with Facebook Group ID's
- Future and Past Events
- Video Listing, with filename

*User Photos* (sometimes referred to as User Photoprint) is delivered in PDF format and may include photos uploaded by the user and photos uploaded by other users that have the requested user tagged in them.

*Group Information* will include the BSI of the group creator/administrator in XML format and the current status of the group in a PDF format.

*Private Messages* if retained will be in PDF format.

*IP Logs* are very limited and frequently incomplete, but when available are provided in a tab delimited text file and include:

- [Column One] **Viewtime** – Date of execution, in **PACIFIC TIME ZONE** (UTC -8 / -7).
- [Column Two] **UserId** – The Facebook user ID of the account active for the request
- [Column Three] **IP** – Source IP address
- [Column Four] **Script** – Script executed. For instance, a profile view of the url "http://www.facebook.com/profile.php?id=29445421" would populate script with "profile.php" and **Scriptget** – Additional information passed to the script. in the above example, scriptget would contain "id=29445421"
- [Column Five] **Session Cookie** – HTTP cookie set by user session.

FACEBOOK CONFIDENTIAL AND PROPRIETARY  
© Facebook, Inc. 2010. All Rights Reserved.

**Request Requirements**

Formal requests for records must address each of the following 3 areas:

**Authorized Law Enforcement Agent information:**

The following contact information is required for every request:

- Requesting Agency Name
- Requesting Agent Name and Badge/Identification number
- Requesting Agent work-authorized e-mail address
- Requesting Agent phone number including any extension
- Requesting Agent Mailing Address
- Requested response due date (Please allow at least 2 – 6 weeks for processing)

**Facebook User Information:**

We only respond to requests that identify an account by email address, user ID or username. Facebook IDs are intrinsic in site URLs. If you have a subject's profile page URL, you can find the ID by looking for the string "id" in the URL and passing along the number immediately following.

For instance, the user ID for the following profile is "29445421":

<http://www.facebook.com/profile.php?id=29445421>

Group IDs follow a similar pattern, but the string to look for is "gid". The group ID of the following URL is 2204894392:

<http://www.facebook.com/group.php?gid=2204894392>

Instead of a Facebook ID in the URL, you may see a Facebook username. For example:

<http://www.facebook.com/john.smith>.

In order for us to accept a username as a valid account identifier, you must also supply the date when you viewed the URL in question.

**Investigation Details:**

We review each request for records individually and prioritize requests based upon case circumstances and other factors not always obvious from the formal process. Please provide any additional details about the case that you can, so that we can make sure that your case is prioritized appropriately and the records you receive are most relevant to your case.



**EMERGENCY DISCLOSURE REQUEST FORM**

Requesting Agency Name  
Requesting Agent Name  
Requesting Agent Badge #  
Requesting Agent work-authorized e-mail  
Requesting Agent phone number including any extension

Detailed description of the nature of the emergency (i.e. potential bodily harm, crime being committed):

Identifying information for user account (Facebook User ID, Username, Email & DOB):

Detailed explanation of information needed to resolve emergency:

I, \_\_\_\_\_, attest that the above-mentioned facts are true and accurate to the best of my knowledge.

\_\_\_\_\_  
Signature and Badge #

\_\_\_\_\_  
Date

The Facebook logo, consisting of the word "facebook" in a white, lowercase, sans-serif font, centered on a black rectangular background.

## **Facebook Subpoena / Search Warrant Guidelines**

This document describes the procedure for requesting data from Facebook, Inc. and its corporate affiliates ("Facebook") along with the types of data available. Please note that this document is dated February 2008. If it is more than 6 months old, please contact Facebook at [subpoena@facebook.com](mailto:subpoena@facebook.com) for any updates.

This document is CONFIDENTIAL. It contains Facebook Proprietary Information. It is intended for law enforcement and legal counsel use only and should not be redistributed without the express written permission of Facebook.

**Changes in this version:**

- Updated Submission Process
- Various Grammar/Formatting changes.

**Facebook reserves the right to charge reasonable fees, where permissible, to cover our costs in replying to subpoena and warrant requests.**

***Acceptable Use Policy***

Privacy and Integrity are cornerstones of the Facebook application and company philosophy. Our privacy settings allow an individual to control access to their data on the site. We actively monitor the site for accounts that try and circumvent our privacy features, either by technical means or by providing false profile information. In accordance with our terms of service (available at <http://www.facebook.com/terms.php>), we will disable any and all accounts, including accounts that may belong to law enforcement, which supply false or misleading profile information and/or attempt to technically or socially circumvent our privacy measures.

**Information required in your Subpoena or Warrant**

In general, data retrieval is based upon a Facebook user ID or group ID. When the Facebook ID is not available, an e-mail address(s) associated with the account is often the most useful information for locating an account. While Facebook will accept requests without these types of information, the additional time required to identify a particular user account will delay response substantially. In some cases, we may not correctly identify an account without additional information. We may purge data as part of our normal operations before we are able to identify a particular user or group if a user ID or group ID is not provided.

***How to find the Facebook ID***

Facebook IDs are intrinsic in our URLs. If you have a subject's profile page URL, you can find the ID by looking for the string "id" in the URL and passing along the number immediately following.

For instance, the user ID for the following profile is "29445421":

<http://www.facebook.com/profile.php?id=29445421>

Group IDs follow a similar pattern, but the string to look for is "gid". The group ID of the following URL is 2204894392.

<http://www.facebook.com/group.php?gid=2204894392>

### How to Submit a Request

Please contact our legal department at [subpoena@facebook.com](mailto:subpoena@facebook.com) to inform us that a request may be coming. This is especially important if you are interested in IP logs and the timeframe is approaching 90 days.

Please have as much of the following information as possible available:

- Requestor's (i.e. Law Enforcement Department, Law Office) full contact information (Point of contact name, physical address, phone number and e-mail): *please note we generally send information via e-mail. Therefore, an e-mail address is necessary.*
- Response Date Due (Please allow 2-4 weeks for processing):
- Full name of user(s):
- Full URL to Facebook profile(s):
- School(s)/network(s):
- Birth date(s):
- Known e-mail address(s):
- Instant Messenger Account Id(s):
- Phone number(s):
- Address:
- Period of activity at issue (specific dates will most likely expedite your request):

We may take steps to preserve relevant data, but will not work on producing data until a subpoena or search warrant is received. These should be faxed to: (650) 644-3229, e-mailed to [subpoena@facebook.com](mailto:subpoena@facebook.com) or mailed to:

Facebook  
Attn: Security Department  
151 University Avenue  
Palo Alto, CA 94301

Facebook will generally respond via e-mail. If the volume of returned data is larger than a few megabytes, Facebook will respond via read-only media (CDROM or DVDROM). Responses will be in PDF, Excel or text formats.

## Types of Information Available

### User Neoprint

The Neoprint is an expanded view of a given user profile. A request should specify that they are requesting a "Neoprint of used Id XXXXXX".

### User Photoprint

The Photoprint is a compilation of all photos uploaded by the user that have not been deleted, along with all photos uploaded by any user which have the requested user tagged in them. A request should specify that they are requesting a "Photoprint of user Id XXXXXX".

### User Contact Info

All user contact information input by the user and not subsequently deleted by the user is available, regardless of whether it is visible in their profile. This information may include the following:

Name  
Birth date  
Contact e-mail address(s)  
Physical address  
City  
State  
Zip  
Phone  
Cell  
Work phone  
Screen name (usually for AOL Messenger/iChat)  
Website

With the exception of contact e-mail and activated mobile numbers, Facebook validates none of this information. A request should specify that they are requesting "Contact information of user specified by <some other piece of contact information>". No historical data is retained.

### Group Contact Info

Where a group is known, we will provide a list of users currently registered in a group. We will also provide a PDF of the current status of the group profile page.

FACEBOOK CONFIDENTIAL AND PROPRIETARY  
© Facebook, Inc. 2008. All Rights Reserved.

A request should specify that they are requesting "Contact information for group XXXXXX".  
No historical data is retained.

## IP Logs

IP logs can be produced for a given user ID or IP address. A request should specify that they are requesting the "IP log of user Id XXXXXX" or "IP log of IP address xxx.xxx.xxx.xxx".

The log contains the following information:

- Script – script executed. For instance, a profile view of the URL <http://www.facebook.com/profile.php?id=29445421> would populate script with "profile.php"
- Scriptget – additional information passed to the script. In the above example, scriptget would contain "id=29445421"
- Userid – The Facebook user id of the account active for the request
- View time – date of execution in Pacific Time
- IP – source IP address

IP log data is generally retained for 90 days from present date. However, this data source is under active and major redevelopment and data may be retained for a longer or shorter period.

## Special Requests

The Facebook Security Team may be able to retrieve specific information not addressed in the general categories above. Please contact Facebook if you have a specific investigative need prior to issuing a subpoena or warrant.



**Microsoft® Online Services**

**Global Criminal Compliance**

**Handbook**

**U.S. Domestic Version**

**March 2008**

2007-2008© Copyright Microsoft Corporation. All rights reserved. Microsoft, MSN, Hotmail, Xbox and Xbox 360 are trademarks of the Microsoft group of companies. No part of this handout may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the written permission of Microsoft Corporation.

# MICROSOFT ONLINE SERVICES

## Law Enforcement Hotline: (425) 722-1299

### Where to Serve Legal Process in Criminal Matters

Windows Live™, Windows Live ID (Passport),  
MSN®, Xbox & Other Online Services:

FAX: (425) 708-0096  
Microsoft Corporation  
Attn: Online Services Custodian of Records  
One Microsoft Way  
Redmond, WA 98052-6399

#### EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves "the danger of death or physical injury to any person..." as permitted in 18 U.S.C. § 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

#### NON-U.S. LAW ENFORCEMENT

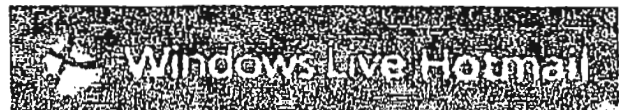
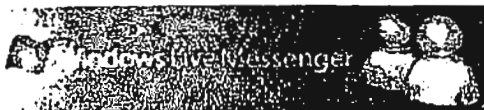
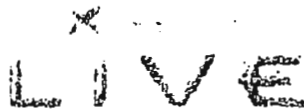
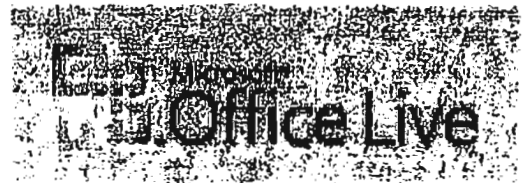
Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at [globalcc@microsoft.com](mailto:globalcc@microsoft.com), and you will be directed to the local contact handling requests from your country.

All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be directed to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft's local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

# What are Microsoft Online Services?

---

- E-mail Services
- Authentication Service: Windows Live ID
- Instant Messaging: Windows Live Messenger
- Social Networking Services: Windows Live Spaces & MSN Groups
- Custom Domains: Windows Live Admin Center & Office Live Small Business
- Online File Storage: Office Live Workspace & Windows Live SkyDrive
- Gaming: Xbox Live




# E-mail Services

## What are the Various E-mail Services Microsoft Provides?

- Several different domains:
  - @hotmail.com
  - @msn.com
  - @live.com
- Microsoft also provides some country specific domains such as .co.uk, .fr, .it, .de, .es, .th, .tk, .co.jp
  - Currently all e-mail service customer data is stored in the U.S. even if the account name contains a country specific domain.
- E-mail accounts may be either free or associated with a paid service
  - Accounts that start out as paid accounts may later become free ~OR~ accounts that start out as free may later be associated with a paid service.
  - Therefore, the records available in response to law enforcement requests will vary depending on the type of e-mail service.

Below are several examples of the paid e-mail services Microsoft offers:



Windows Live Hotmail

**It's here: The award-winning next-generation version of Hotmail.**

Designed to keep you safe and productive, Windows Live Hotmail is available in free and premium versions. Which one is right for you?

**Windows Live Hotmail**

Learn more




**Free**

- A whopping 2 GB of inbox storage
- Enhanced security, color-coded alerts for suspicious e-mail
- Choose the full version or the streamlined classic version
- Choose your own colors and layout
- Preview window for all messages
- Drag, drop, and organize it all

Switch to the full version of Windows Live Hotmail

**Windows Live Hotmail Plus**

Learn more



**\$19.95/yr**

**All the goodness of Windows Live Hotmail, plus:**

- More storage: now 4 GB
- No account expiration\*
- No graphical ads
- Bigger attachments: up to 20 MB

**Windows Live Hotmail**

Learn more

**Windows Live Hotmail Plus**

Learn more

Microsoft Online Services Home | Microsoft services | Support

[IM & Blogging](#)
[Search & Learn](#)
[Internet Access](#)
[Entertainment](#)
[Mobile](#)

**msn. Premium**

Advanced e-mail, PC-wide protection, and more.


[Overview](#)
[Features](#)
[FAQ](#)
[System Requirements](#)

**Protect**  
 Help safeguard your system with Virus Guard and Firewall Guard powered by McAfee® Security. Get powerful parental controls to help keep kids safe online.

**Organize**  
 Stay on top of your to-do list by creating tasks for yourself or others. Share your calendar to stay in sync with friends or family.

**Create**  
 Design special stationery with fonts, colors and custom signatures to make your e-mail unique.


**Share**  
 Share a single photo or an entire slide show right inside your e-mail with cool photo sharing and editing tools.



**\$9.95 monthly**  
Two months free

[Get it now](#)

[Click for quick demo](#)



## What E-mail Services Records are Retained and for How Long?

E-mail account registration records are retained for the life of the account. Internet Protocol ("IP") connection history records are retained for 60 days.

## How Do I Read E-Mail Account Results?

**Sample E-mail Account Registration Records:**

**Microsoft** Created 2/24/2008 1:53:11 PM

---

[criminal-compliance-training@botmail.com](mailto:criminal-compliance-training@botmail.com)

Microsoft		criminal-compliance-training@hotmail.com	
		2/21/2006 1:00:43 PM	
Name	Field	Value	
Cover Letter	Job#	criminal-compliance-training@hotmail.com	
User Info	First Name		
History Info	Alt Name		
Folders	State	California	
Email	Zip	94240	
Other Info	Country	US	
Home	Timezone	America/Los_Angeles	
	Registered from IP	64.4.1.1	
	Date Registered	2/22/2006 9:37:21 AM	
	Last To Address	criminal-compliance-training@hotmail.com	
This account forwards to the following accounts: Accounts Forwarding To This Account: 114 users			

- All registration data is provided by the user EXCEPT for the Registered from IP Address.
- Occasionally the "Registered from IP Address" field may blank for some accounts. In this situation the user's IP address was not captured by Microsoft's systems during the registration process.
- Microsoft retains e-mail account registration records for the life of the account.
- For free MSN Hotmail and free Windows Live Hotmail accounts, the e-mail content is typically deleted after 60 days of inactivity. Then if the user does not reactivate their account, the free MSN Hotmail and free Windows Live Hotmail account will become inactive after a period of time.

**Sample E-mail Account IP Connection Records:**

Microsoft		criminal-compliance-training@hotmail.com	
		2/21/2006 1:00:43 PM	
Name	IP	Date (Pacific)	Pass/Fail
Cover Letter	64.4.1.11	2/22/2006 9:36:14 AM PST	2000
User Info	64.4.1.11	2/22/2006 9:37:21 AM PST	2000
History Info	64.4.1.11	2/22/2006 9:38:43 PM PST	2000
Folders	64.4.1.11	2/22/2006 9:39:37 PM PST	2000
Email	64.4.1.11	2/22/2006 9:40:18 PM PST	2000
Other Info	64.4.1.11	2/22/2006 9:41:48 PM PST	2000
Home	64.4.1.11	2/22/2006 9:42:58 PM PST	2000
	64.4.1.11	2/22/2006 9:44:49 PM PST	2000
	64.4.1.11	2/22/2006 9:46:49 PM PST	2000
	64.4.1.11	2/22/2006 9:48:49 PM PST	2000
	64.4.1.11	2/22/2006 9:50:49 PM PST	2000
	64.4.1.11	2/22/2006 9:52:49 PM PST	2000
	64.4.1.11	2/22/2006 9:54:49 PM PST	2000
	64.4.1.11	2/22/2006 9:56:49 PM PST	2000
	64.4.1.11	2/22/2006 9:58:49 PM PST	2000
	64.4.1.11	2/22/2006 10:00:49 PM PST	2000
	64.4.1.11	2/22/2006 10:02:49 PM PST	2000
	64.4.1.11	2/22/2006 10:04:49 PM PST	2000
	64.4.1.11	2/22/2006 10:06:49 PM PST	2000
	64.4.1.11	2/22/2006 10:08:49 PM PST	2000
	64.4.1.11	2/22/2006 10:10:49 PM PST	2000
	64.4.1.11	2/22/2006 10:12:49 PM PST	2000
	64.4.1.11	2/22/2006 10:14:49 PM PST	2000
	64.4.1.11	2/22/2006 10:16:49 PM PST	2000
	64.4.1.11	2/22/2006 10:18:49 PM PST	2000
	64.4.1.11	2/22/2006 10:20:49 PM PST	2000
	64.4.1.11	2/22/2006 10:22:49 PM PST	2000
	64.4.1.11	2/22/2006 10:24:49 PM PST	2000
	64.4.1.11	2/22/2006 10:26:49 PM PST	2000
	64.4.1.11	2/22/2006 10:28:49 PM PST	2000
	64.4.1.11	2/22/2006 10:30:49 PM PST	2000
	64.4.1.11	2/22/2006 10:32:49 PM PST	2000
	64.4.1.11	2/22/2006 10:34:49 PM PST	2000
	64.4.1.11	2/22/2006 10:36:49 PM PST	2000
	64.4.1.11	2/22/2006 10:38:49 PM PST	2000
	64.4.1.11	2/22/2006 10:40:49 PM PST	2000
	64.4.1.11	2/22/2006 10:42:49 PM PST	2000
	64.4.1.11	2/22/2006 10:44:49 PM PST	2000
	64.4.1.11	2/22/2006 10:46:49 PM PST	2000
	64.4.1.11	2/22/2006 10:48:49 PM PST	2000
	64.4.1.11	2/22/2006 10:50:49 PM PST	2000
	64.4.1.11	2/22/2006 10:52:49 PM PST	2000
	64.4.1.11	2/22/2006 10:54:49 PM PST	2000
	64.4.1.11	2/22/2006 10:56:49 PM PST	2000
	64.4.1.11	2/22/2006 10:58:49 PM PST	2000
	64.4.1.11	2/22/2006 11:00:49 PM PST	2000
	64.4.1.11	2/22/2006 11:02:49 PM PST	2000
	64.4.1.11	2/22/2006 11:04:49 PM PST	2000
	64.4.1.11	2/22/2006 11:06:49 PM PST	2000
	64.4.1.11	2/22/2006 11:08:49 PM PST	2000
	64.4.1.11	2/22/2006 11:10:49 PM PST	2000
	64.4.1.11	2/22/2006 11:12:49 PM PST	2000
	64.4.1.11	2/22/2006 11:14:49 PM PST	2000
	64.4.1.11	2/22/2006 11:16:49 PM PST	2000
	64.4.1.11	2/22/2006 11:18:49 PM PST	2000
	64.4.1.11	2/22/2006 11:20:49 PM PST	2000
	64.4.1.11	2/22/2006 11:22:49 PM PST	2000
	64.4.1.11	2/22/2006 11:24:49 PM PST	2000
	64.4.1.11	2/22/2006 11:26:49 PM PST	2000
	64.4.1.11	2/22/2006 11:28:49 PM PST	2000
	64.4.1.11	2/22/2006 11:30:49 PM PST	2000
	64.4.1.11	2/22/2006 11:32:49 PM PST	2000
	64.4.1.11	2/22/2006 11:34:49 PM PST	2000
	64.4.1.11	2/22/2006 11:36:49 PM PST	2000
	64.4.1.11	2/22/2006 11:38:49 PM PST	2000
	64.4.1.11	2/22/2006 11:40:49 PM PST	2000
	64.4.1.11	2/22/2006 11:42:49 PM PST	2000
	64.4.1.11	2/22/2006 11:44:49 PM PST	2000
	64.4.1.11	2/22/2006 11:46:49 PM PST	2000
	64.4.1.11	2/22/2006 11:48:49 PM PST	2000
	64.4.1.11	2/22/2006 11:50:49 PM PST	2000
	64.4.1.11	2/22/2006 11:52:49 PM PST	2000
	64.4.1.11	2/22/2006 11:54:49 PM PST	2000
	64.4.1.11	2/22/2006 11:56:49 PM PST	2000
	64.4.1.11	2/22/2006 11:58:49 PM PST	2000
	64.4.1.11	2/22/2006 12:00:49 PM PST	2000

- Occasionally the "Pass/Fail" column will include an entry entitled "mysn". When this indication is present, it means the user logged in from the [www.msn.com](http://www.msn.com) homepage.

**Stored E-mail Records for MSN Premium Customers:**

- Microsoft's systems only store the e-mails a user has elected to maintain in the account. Therefore, the only e-mails provided in response to legal process seeking stored e-mail content will be the e-mails stored in the "Folders on MSN" section of a user's account.
- Be aware that users may also store e-mail content on their computer's hard drive. Microsoft will not be able to disclose e-mail content stored on a user's computer – only e-mail content stored on Microsoft's e-mail servers.



**Additional Tips:**

- Within the available IP records, an entry could exist that belongs to Microsoft services due to internal configurations. 'Registered From IP' addresses or other IP addresses in the IP history that are in the blocks of 65.54.xx.xx (MSN Hotmail) or 207.68.174.xx, 207.46.237.xx, 65.54.198.xx, 64.4.55.xx (MSN Mobile) are from Microsoft-owned servers, but they do not provide any further information which relates to the user.
- If there is an entry of 1.1.1.1 or 2.2.2.2 in the 'History Info' the entry is a Microsoft system generated line item. The 1.1.1.1 and 2.2.2.2 entries are not generated by user activity. Specific questions can be directed to the Global Criminal Compliance Team.

**FREE E-MAIL ACCOUNT AGE OUT TIMELINE**



- Users may self delete an account at any point along this process. The 30 day inactivity period is canceled if someone tries to create the same account name ~or~ attempts to access it. Between 120 and 365 days, users can recreate an e-mail mailbox.



# Authentication Service: Windows Live ID

---

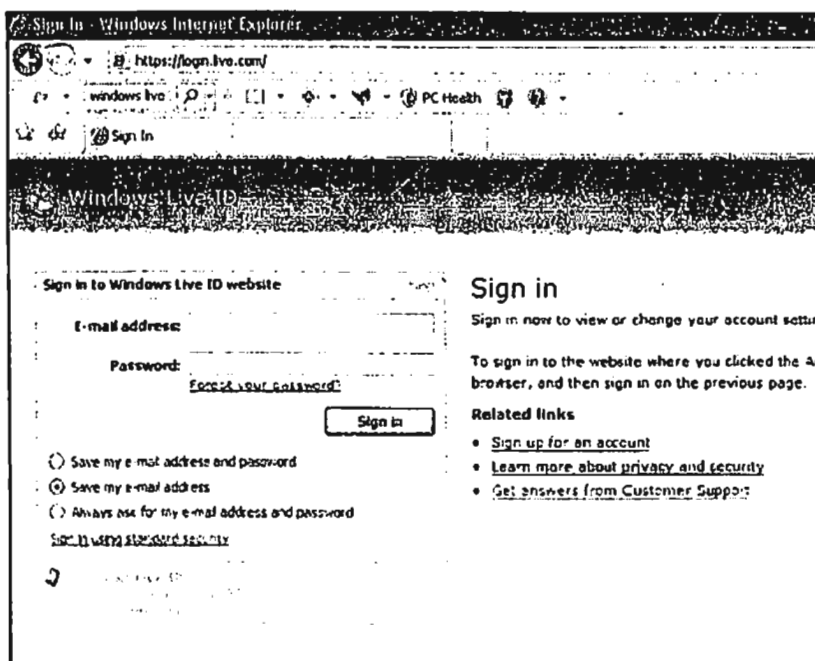
## What is the Service?

The Windows Live ID authentication service, formerly known as "Passport", helps simplify your sign in: Create your sign in credentials – *e-mail and password* – once, and then use them everywhere on the Windows Live Network. There are three different ways you may obtain a Windows Live ID:

- Use a @live, @hotmail or @msn e-mail account
- Easy ID: Use an e-mail address you already have – @other\_email\_provider.com.
  - You can use any existing e-mail address from any e-mail provider when you create your credentials for Windows Live ID. Then you can use those credentials to sign in to any Windows Live ID site.
- Sign up for a limited account – @passport.com
  - Create credentials only – Log on using e-mail address and password only. Account cannot send or receive e-mail.

### Windows Live ID / Passport accounts:

- Works with MSN, Office Live, and Microsoft Passport sites
- Have an MSN Hotmail, MSN Messenger, or Passport account? It's your Windows Live ID.



The screenshot shows a web browser window titled "Sign In - Windows Internet Explorer" with the address bar displaying "https://login.live.com". The page content includes a "Sign in" button in the top left, a "Windows Live ID" header, and a main sign-in form. The form has two input fields: "E-mail address:" and "Password:". Below the password field is a link that says "Forgot your password?". A "Sign in" button is located below the password field. To the right of the form, there is a "Sign in" heading followed by the text "Sign in now to view or change your account settings" and "To sign in to the website where you clicked the Account button, and then sign in on the previous page." Below this is a "Related links" section with three links: "Sign up for an account", "Learn more about privacy and security", and "Get answers from Customer Support". At the bottom of the form, there are three radio button options: "Save my e-mail address and password", "Save my e-mail address", and "Always use for my e-mail address and password". Below these options is a link that says "Sign in with stored security".

## What Windows Live ID (Passport) Records are Retained and for How Long?

Microsoft retains the following:

- Windows Live ID retains registration records as long as the account exists in our systems. All registration data is provided by the user.
- The last 10 Microsoft site and IP connection record combinations (not the last 10, consecutive IP connection records.)

## How Do I Read Windows Live ID (Passport) Account Results?

### Sample Sign-in Summary

Last Modified	Entry Created	Action	Value	Site Name	Site ID	IP Address
2008/11/30 10:22:35	2006/08/12 10:24:42	Login Success			0	192.192.240.192
2008/11/30 10:22:35	2006/08/12 10:24:42	Site IP History	Hotmail 192.192.240.192 Nov 30 2008 10:22 AM Hotmail 192.228.114.88 Nov 29 2008 11:06 AM Hotmail 192.192.240.192 Nov 28 2008 12:22 AM Hotmail 192.192.240.192 Nov 28 2008 11:07 AM Hotmail 192.192.240.192 Nov 28 2008 11:05 AM Hotmail 192.192.240.192 Nov 18 2008 12:57 PM Hotmail 192.248.157.201 Nov 18 2008 12:56 PM Hotmail 192.248.157.201 Nov 18 2008 12:55 PM Hotmail 192.248.157.201 Nov 18 2008 12:54 PM			
2008/11/02 17:50:38	2006/08/12 10:24:42	IP Address History	192.209.154.235;192.212.1.52;82.20.2.45;192.209.154.66;192.192.45.86;		0	192.209.154.235
2008/11/02 17:50:38	2006/08/12 10:24:42	Site IP History	Hotmail 192.209.154.235 Nov 02 2008 17:50:38 Hotmail 192.209.154.235 Nov 02 2008 17:50:38 Hotmail 192.209.154.235 Nov 02 2008 17:50:38			
2008/09/28 17:02:08	2006/08/12 10:24:42	Current State (login succeeded)			0	192.192.45.86
2008/09/28 17:02:08	2006/08/12 10:24:42	Site IP History				
2006/08/12 10:24:42	2006/08/12 10:24:42	Create Credential	1 JMDCE6AM	Hotmail	2	192.192.45.86

### Create Credential Row

2006/08/12 10:24:42	2006/08/12 10:24:42	Create Credential	1 JMDCE6AM	Hotmail	2	192.192.45.86
---------------------	---------------------	-------------------	------------	---------	---	---------------

The time when the account was created

ignore this value

The Microsoft site where the account was created

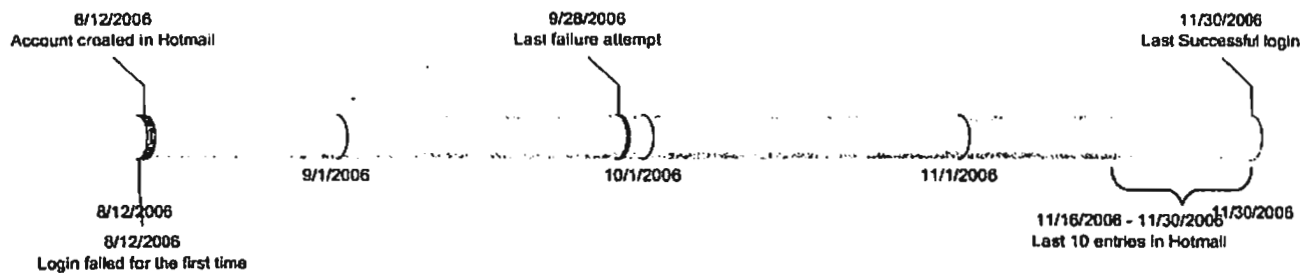
The IP address from where the account was created



### Additional Tips:

1. In Create credential Row
2. In the Current State Row
  - a. The IP address DOES NOT denote the IP address of the machine of the last attempt. If the last login was a failure, then the IP address is present in the "IP address" column of the Login Failure Row while if it was success then the IP address is present in Site/IP/Time history row.
  - b. If the state is "Login failed", then refer the "Last Modified" timestamp in the "Login Failure Row" to find the last time the user tried to login and failed. If the state is "Login Successful", then refer to the "Last Modified" timestamp in the "Login Success Row" to find the last time the user signed in successfully.
3. In Login Failure Row
  - a. The value (number of failure tries) is cleared once the user is able to successfully login. Hence, if a user failed to login on several tries, but eventually logs in successfully, there is no record of the previous failures.
4. In Site IP/Time/History Row
  - a. The Site IP/Time/History table is not updated if the user logs in again from the SAME IP address to the SAME Microsoft site. It only shows the FIRST login of the LAST day for the user, from the same IP and to the same machine.
  - b. There are many cases where end user IP address is hidden by ISP proxy server. SIS shows the IP address of ISP proxy server, instead of real end user IP address. So for the individual user information you can approach the ISP.
  - c. The table is limited to only the last 10 MS SITE and IP combinations.
5. Sign-In Summary records are restricted to initial authentication so subsequent authentication to other Microsoft sites are not logged.
6. All times are UTC and the time-stamps come from Windows Live ID (Passport) servers and not the user's computer.
7. Ignore rows "IP Address History" and "Date/Time History". These are present for some older accounts and have now been replaced by "Site IP/Time/History" row.

⇒ One way to understand the table is to draw the timeline and plot the individual events in it. It gives a quick view of the activities in that account. Here is the timeline for the Sign-In Summary Table provided above:



# Instant Messaging: Windows Live Messenger

## What is the Service?

Windows Live Messenger is the "Next generation of MSN Messenger"

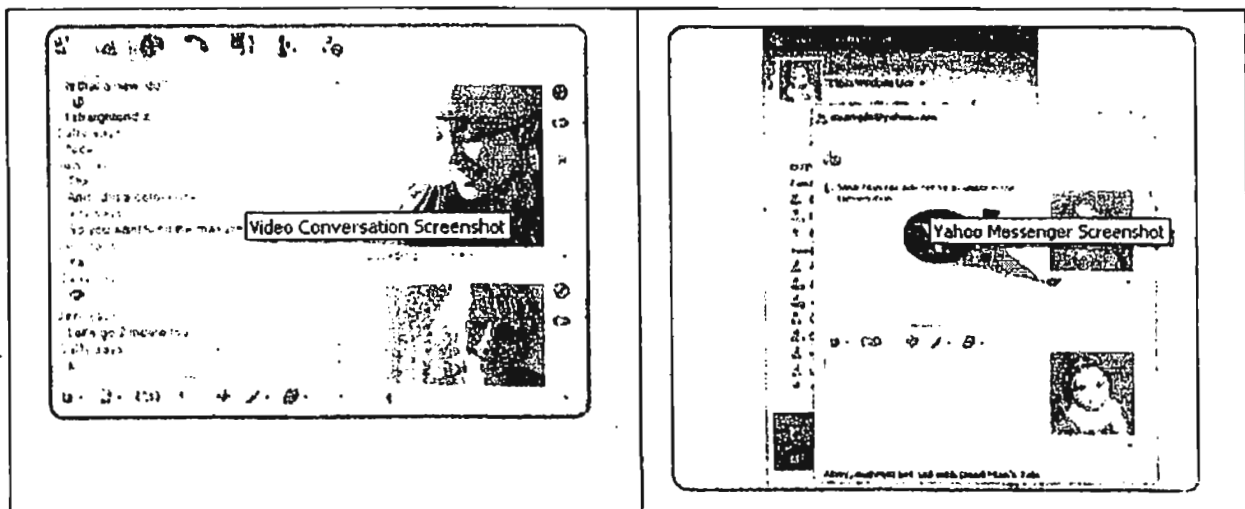
- Free service
- Customers use Windows Live ID / Passport account to sign-in
- Microsoft retains:
  - Windows Live ID / Passport account registration data
  - Some Windows Live ID / Passport account IP connection records

Windows Live Messenger program is downloaded onto client

- Microsoft servers authenticate users, but Microsoft does not log the content of communications between users

Windows Live Messenger customers talk to Yahoo! contacts

- If a Windows Live Messenger customer adds a Yahoo! contact to his or her contact list, Microsoft will have the name of the Yahoo! contact.



## What records are retained and for how long?

Since the Windows Live ID service is used to authenticate Windows Live Messenger or MSN Messenger users, Windows Live ID records are retained. Please refer to the "Authentication Services: Windows Live ID" section above.

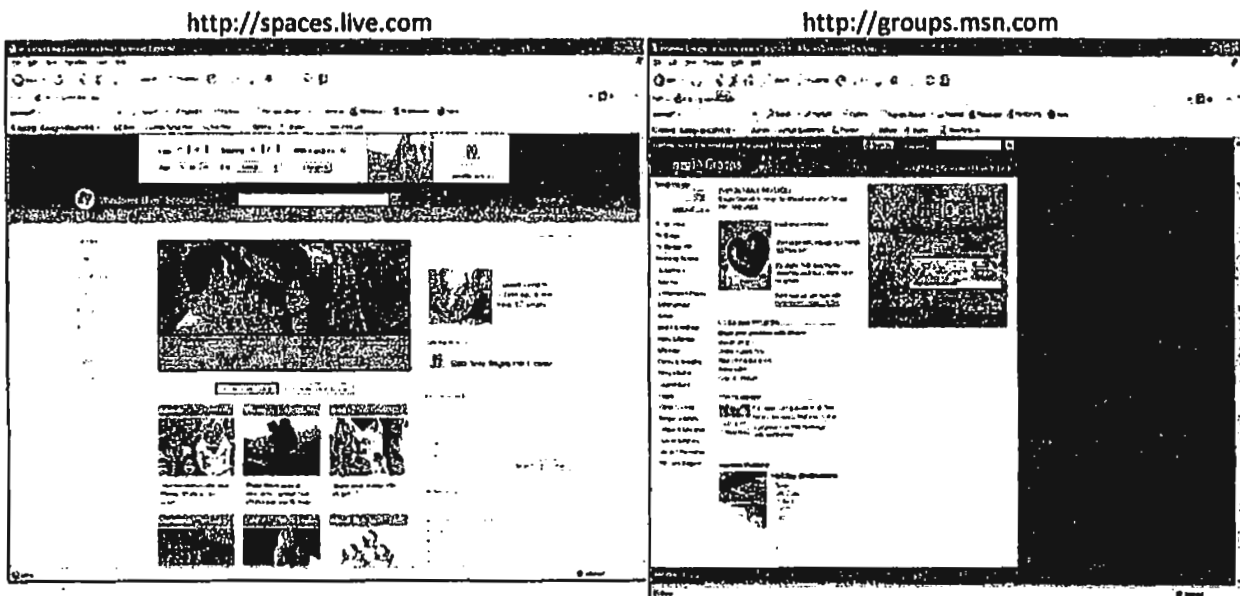
Please note that Microsoft needs a full account name with domain (@hotmail.com, @msn.com or @live.com) in order to identify a Windows Live ID (Passport) account. An account cannot be identified when only an alias or screen name has been provided.

# Social Networking Services: Windows Live Spaces & MSN Groups

## What are the Services?

Windows Live Spaces is a free service where users may create and customize their own blog, upload photos and network with other users (friends and friends of friends).

MSN Groups are free websites that provide features such as message boards, chat rooms and photo albums.



Windows Live Spaces	MSN Groups
<ul style="list-style-type: none"> <li>▪ One owner</li> <li>▪ Only the owner of the space can upload content</li> <li>▪ Spaces can be public or private</li> <li>▪ Space owner can invite you to a private space if you belong to his or her contact list and/or e-mail you the link to the space</li> </ul>	<ul style="list-style-type: none"> <li>▪ Has only one manager but manager may have assistant managers</li> <li>▪ Anyone who is a member of the group can upload content</li> <li>▪ Groups can be public or private</li> <li>▪ Manager must e-mail link in invitation to a private group</li> </ul>

## What Records are Retained and for How Long?

**Windows Live Spaces:** Only the owner of a Windows Live Space can upload content (e.g. images, documents, videos), and when they do so, the IP address and date and time is also captured. In addition, if someone posts a comment to the blog, Microsoft captures the text of the comments as well as the IP address, date and time of upload and the nickname. These transactional records are retained for 90 days.

**MSN Groups:** When a manager or member of an MSN Group uploads content, Microsoft captures the IP address and date and time of content upload. These transactional records are retained for 60 days.

## Sample Language

**Windows Live Spaces:** The Windows Live Spaces online service enables customers to reach out to others by publishing their thoughts, photos, and interests in an easy way. They can be as inclusive or exclusive as they want to be. They can set three levels of permissions to view their Space: 1) public – allows anyone on the Internet, 2) allows only the group of people from their Windows Live Messenger allow list, or 3) private – allows only each person specified individually from their MSN Address Book. Information that they publish in their Space is arranged in units called content modules. Content modules contain information and links to their items such as photos, music, blogs, and lists. However, when you are looking for information on a specific incident like a photo posting or blog posting, please request all content and logs for the Space. We cannot retrieve single incident data.

When submitting legal process for information on Windows Live Spaces, please include the following item descriptions as needed (listed below in bold):

- For information requests on Spaces website content & logs: content including photos; photo albums; blogs; lists etc.; and IIS (website activity) logs:  
***Any and all website information for the [Space requested] including content, photos, blogs, lists, and all IIS logs.***
- For information requests on the creator (owner) of the Space:  
***Any and all subscriber information for the creator of the [Space] including means and source of payment of any such paid subscription records associated with the owner's e-mail account as well as associated IP history for the account.***
- For information requests on other visitors of the Space (e.g. by nickname or email address):  
***Any and all subscriber information for the visitor [visitor name] of the Space [Space name] including means and source of payment of any such paid account and associated IP logs for these accounts. Note: we have information only on visitors who posted comments posted to the Space.***

**MSN Groups:** When submitting legal process for information on MSN Groups, please include the following items (in bold):

- For information requests on group website content/logs: content, including images; member lists; IIS (activity) logs:  
***Any and all website information for the [group requested] including content, images, member lists, and all IIS logs.***
- For information requests on the manager of the group:  
***Any and all subscriber information for the manager of the group including means and source of payment of any such paid account and associated IP logs for these accounts.***
- For information requests on other members of the group (e.g. by nickname or email address):  
***Any and all subscriber information for the member [member name] of the group [group name] including means and source of payment of any such paid account and associated IP logs for these accounts.***

Please note that the following items cannot in any way be associated with MSN Groups: Telephone number(s) and Local and long distance telephonic connection records. In addition, when you are looking for information on a specific incident like a photo posting or message posting, please request all group content and logs. We cannot retrieve single incident data.



# Custom Domains: Windows Live Admin Center

---

## What is the Windows Live Admin Center Service?

The Windows Live Custom Domains is now Windows Live Admin Center, which includes Windows Live Custom Domains, Windows Live @edu, Windows Live @net and Windows Live Community Builder. You may learn more about all of these services at <http://domains.live.com>.

Windows Live Custom Domains provides customers with their own domain name and, initially, up to 100 e-mail accounts. For example, John Doe may create a custom domain [www.johndoefamily2.com](http://www.johndoefamily2.com) and may create e-mail addresses such as [john@johndoefamily2.com](mailto:john@johndoefamily2.com), [mary@johndoefamily2.com](mailto:mary@johndoefamily2.com), etc.

Windows Live@edu delivers student and alumni e-mail as well as communication and collaboration services. The e-mail accounts offer a 5 GB in box, university domain name, as well as other features and students may keep their e-mail after they graduate. Additional services may also be utilized by Windows Live@edu customers such as Office Live Workspace and Windows Live SkyDrive. Learn more about Windows Live@edu at <http://get.liveatedu.com/Education/Connect>.

**Law enforcement should know to send their criminal legal process to Microsoft if a domain name lookup indicates association with Microsoft.**

### Windows Live Admin Center

Windows Live Custom Domains is now Windows Live Admin Center.

We're changing the name to better reflect our features and capabilities, but don't worry, this is still where you access the same great features you did with Custom Domains. In fact, we're introducing exciting new features we think you'll really like. Thank you for understanding as we transition to our new name.

- **Existing customers** - You may not notice anything new beyond the name change. This is still the same great service you've been using.
- **All users** - We're excited to introduce the ability to customize Windows Live services like Windows Live Hotmail with your own logo. Now your domain users will see your organization's logo every time they check their Hotmail. Just select the co-branding link in the left navigation to get started.
- **New customers** - Get started below to register your domain and create customized Windows Live accounts.

Learn more about Windows Live programs for organizations

- **Windows Live @ edu** - This program is specifically tailored for the needs of educational institutions. [Learn more](#)
- **Windows Live @ net** - This program enables network operators to bring hosted communication services to their customers. [Learn more](#) (additional information is available in English only)
- **Windows Live Community Builder** - This program helps organizations build and strengthen their communities with Windows Live services. [Learn more](#) (additional information is available in English only)

# Custom Domains: Office Live Small Business & Office Live Workspace

## What is the Office Live Service?

Office Live Small Business provides customers with web sites, custom domain name and e-mail as well as e-commerce and other tools. Office Live Workspace provides storage and access to Microsoft Office documents as well as space to share documents and projects.

Law enforcement should know to send their criminal legal process to Microsoft if a domain name lookup indicates association with Microsoft or "Office Live". Learn more about Office Live at: <http://officelive.com>.

The screenshot shows the Office Live Small Business homepage. At the top, there is a navigation bar with "Office Live Small Business" and a "Sign In" link. The main content area is titled "Get Online" and includes the following sections:

- Get Online:** "Create your own professional Web site - for FREE". Text: "Microsoft Office Live Small Business makes it easy to create a professional-looking Web site for your business. Sign up and you'll have everything you need to get started - including free Web hosting, a custom domain name, e-mail accounts, e-commerce, and more." Text: "Sign up and get a custom domain (.com, .net, .org) and up to 100 company-branded e-mail accounts - free for the first year." Below this is a "Sign Up Free" button.
- Web Site:** "Create a professional online presence, including free Web hosting, easy-to-use design tools, site updates, and much more." Below this is a "Sign Up Free" button.
- Custom Domain Name and E-Mail:** "Make more contact with a custom domain and business e-mail accounts - free for the first year." Below this is a "Sign Up Free" button.
- E-Commerce:** "Sell your products and services online." Below this is a "Sign Up Free" button.

On the right side, there is a "Quick Links" section with icons for "Website", "E-mail", and "E-commerce". Below that is a "Business Office Live" section with a "PowerPoint" icon.

The screenshot shows the Office Live Workspace homepage. At the top, there is a navigation bar with "Home", "Learn More", "Examples", "FAQ", and "Community". The main content area is titled "An online extension of Microsoft Office" and includes the following sections:

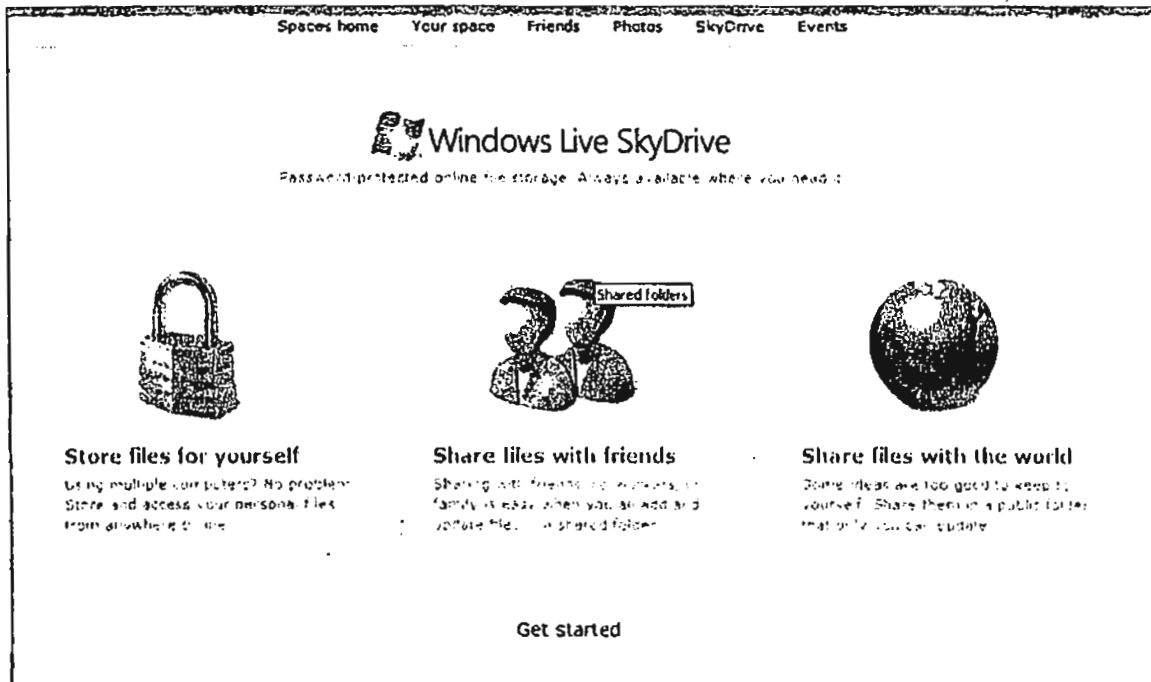
- Sign Up Free:** "For notes and spreadsheets" and "Search the index". Below this is a "Sign Up Free" button.
- Key Features:**
  - Since 2000, Microsoft Office documents are online.
  - Access them from almost any computer with a Web browser.
  - So more flash drives or server space? Not anymore. Use e-mail.
- Key Features:**
  - Share work with the world.
  - No control panel, no email, no attachments, and no over 100MB.
  - Simple, intuitive, and easy to use.
- Key Features:**
  - Open and save files directly from Word, Excel, and PowerPoint.
  - Print, copy, paste, and even edit with Outlook.
  - No need to learn a new program.

On the right side, there is a "TechCrunch, ZDNet, and more" section with a "TechCrunch" icon and a "ZDNet" icon. Below that is a "More examples" section with a "More examples" icon.

# Online File Storage: Windows Live SkyDrive

## What is the Windows Live SkyDrive Service?

Windows Live SkyDrive provides password-protected online file storage for yourself, to share with others or share with the world. Learn more at <http://skydrive.live.com>.



The screenshot shows the Windows Live SkyDrive website interface. At the top, there is a navigation bar with links: Spaces home, Your space, Friends, Photos, SkyDrive, and Events. Below the navigation bar is the Windows Live SkyDrive logo and the tagline "Password-protected online file storage. Always available where you need it." The main content area is divided into three columns, each with an icon and a heading:

- Store files for yourself:** Represented by a padlock icon. Text: "Using multiple computers? No problem. Store and access your personal files from anywhere online."
- Share files with friends:** Represented by an icon of two people and a folder labeled "Shared folders". Text: "Sharing with friends, colleagues, or family is easy when you can add and update files in a shared folder."
- Share files with the world:** Represented by a globe icon. Text: "Some ideas are too good to keep to yourself. Share them in a public folder that only you can update."

At the bottom of the main content area, there is a "Get started" button.

# Gaming: XBOX LIVE®

---

## What is the Service?

Xbox LIVE is the premier online gaming and entertainment service that enables customers to connect their Xbox® to the Internet and play games online. The Xbox LIVE service is available on both original Xbox and new Xbox 360® consoles.

### Original Xbox

- Accounts restricted to ages 13 and up
- Credit card required
- Data collected: Date of birth, name, e-mail address, physical address, telephone, credit card number, type of credit card, credit card expiration date

### Xbox 360 – User under 13

- Credit card required
- Data collected: Date of birth, name, e-mail address, physical address, telephone, credit card number, type of credit card, credit card expiration date, Microsoft Passport

### Xbox 360 – User 13 and up – No credit card requirement (but can be used)

- Data collected without credit card: Date of birth, name, e-mail address, physical address, telephone, Microsoft Passport
- Data collected with credit card: Date of birth, name, e-mail address, physical address, telephone, credit card number, type of credit card, credit card expiration date, Microsoft Passport

**Note:** General subscriber information is unverified. Detailed credit card verification has been implemented.

## What records are retained and for how long?


Both registration and IP connection history records are retained for the life of the gamertag account. Because the volume of IP connection history records may be large, when possible please ask for the specific date range of records you are specifically interested in receiving. A full listing of retained records is below:

- Gamertag
- Credit card number
- Phone number
- First/last name with zip code

- Serial number but only if box has been registered online. "Console ID" is better.
- Service request number from Xbox Hotline (e.g. SR 103xx-xx-xx)
- E-mail account (e.g. @msn.com, @hotmail.com or any other Windows Live ID account name)
- IP history for the lifetime of the gamertag (only one gamertag at a time)

If your investigation involves a stolen Xbox console, if the console serial number or Xbox LIVE user gamertag is provided and the console has been connected to the Internet, IP connection records may be available.

### Sample Xbox LIVE Account Results

XBOX LIVE IP ACTIVITY REPORT					
					
Activity IP Report for Gamertag:					
This report contains usage through Saturday, February 10 2007					
Start Time (UTC)	End Time (UTC)	Gamer Tag	Title Name	IP	
10/29/2005 08 59 PM	10/29/2005 09 00 PM		Xbox Dashboard		
10/29/2005 09 01 PM	10/29/2005 10 39 PM		SW Jedi Academy		
10/29/2005 10 39 PM	10/29/2005 10 40 PM		Xbox Dashboard		
10/29/2005 10 41 PM	10/29/2005 10 43 PM		Midnight Club 3 DUB		
10/29/2005 10 43 PM	10/29/2005 10 44 PM		Xbox Dashboard		
10/29/2005 10 45 PM	10/29/2005 10 56 PM		Midnight Club 3 DUB		
10/30/2005 01 34 AM	10/30/2005 05 02 AM		Midnight Club 3 DUB		
10/31/2005 03 36 AM	10/31/2005 04 08 AM		Midnight Club 3 DUB		
10/31/2005 12 33 PM	10/31/2005 12 36 PM		Midnight Club 3 DUB		
10/31/2005 09 28 PM	10/31/2005 10 10 PM		Midnight Club 3 DUB		
11/1/2005 12 30 AM	11/1/2005 01 07 AM		Midnight Club 3 DUB		
11/1/2005 01 10 AM	11/1/2005 01 10 AM		Xbox Dashboard		

# Legal Process

---

## Legal Process Required for Customer Account Information and Content

The Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2701-2712) sets forth the appropriate legal process required to compel Microsoft's Online Services Records Custodians to disclose customer records and contents:

**Information that may be disclosed with a subpoena.** Basic subscriber information includes name, address, length of service (start date), screen names, other email accounts, IP address/IP logs/Usage logs, billing information, content (other than e-mail, such as in Windows Live Spaces and MSN Groups) and e-mail content more than 180 days old as long as the governmental entity follows the customer notification provisions in ECPA (see 18 U.S.C. §§ 2703(b), 2705.)

**Court orders are required for the rest of the customer's profile (18 U.S.C. § 2703(d)).** A court order issued pursuant to 2702(d) will compel disclosure of all of the basic subscriber information available under a subpoena plus the e-mail address book, Messenger contact lists, the rest of a customer's profile not already listed above, internet usage logs (e.g. WEBTV or MSN Internet Access), and e-mail header information (to/from) excluding subject line.

**Search warrants are required for contents.** A search warrant will compel disclosure of all information available with a court order issued pursuant to 2703(d) (as listed above), plus all contents (if prior notice is not provided or an order for delayed notice is not obtained), and is the only means to compel the disclosure of e-mails, including subject line, in electronic storage 180 days or less\*\*.

**\*\*A Note About Opened E-mail Content less than 181 days:** Under ECPA, e-mail in electronic storage for 180 days or less may be disclosed pursuant to a search warrant. While some have interpreted "in electronic storage" to refer only to unopened mail, a Ninth Circuit decision in Theofel et al v. Farey-Jones and Kwansy, 341 F.3d 978 (9<sup>th</sup> Cir. 2003) held that opened e-mails on ISP servers are also in "electronic storage." Therefore, as Microsoft receives and processes legal process for its online services in the Ninth Circuit, Microsoft discloses both opened and unopened e-mail in electronic storage for 181 days or less only upon pursuant to a search warrant.

**Preservation Requests 18 U.S.C. § 2703(f):** Upon the request of a governmental entity, Microsoft shall preserve all information, including IP logs and contents for a period of 90 days from the date of the preservation. A preservation creates a snapshot of the information in or about the account at a particular point in time, but there is no update of the information throughout the preservation period. Per Microsoft policy, preservations may be extended up to two (2) times. Each extension shall be for a period of 90 days from the expiration of the current preservation, resulting in a maximum of 270 days on a given preservation. An extension does not create a new snapshot, but merely preserves the information for the additional period.