SURVEILLANCE HANDBOOK

CRIMINAL TAX DIVISION
OFFICE OF CHIEF COUNSEL
INTERNAL REVENUE SERVICE

Department of the Treasury
Internal Revenue Service
Document 9347 (12-94)
Catalog Number 12195K

PREFACE

Counsel attorneys perform a variety of duties in connection with providing legal services to the Criminal Investigation Division, Internal Revenue Service. Included among their duties are advising on, assisting with, and preparing the necessary documentation for using various methods of surveillance.

This handbook has been prepared by the Internal Revenue Service, Office of Chief Counsel, Criminal Tax Division, to assist Counsel attorneys who may have questions regarding the various methods of surveillance and the permissible uses of the evidence derived therefrom.

Although this handbook is intended to provide a basic understanding of each area of surveillance, it is not intended to replace thorough research.

This handbook is not intended to create or confer any rights, privileges, or benefits on prospective or actual cases. It is also not intended to have the force of law or of an Internal Revenue Service policy statement. See United States v. Caceres, 440 U.S. 741 (1979).

We acknowledge the efforts of Martin F. Klotz and Iris Miranda-Kirschner, who prepared this publication.

BARRY J. FINKELSTEIN
Assistant Chief Counsel
(Criminal Tax Division)

TABLE OF CONTENTS

INTRODUCTION 1

TITLE I - ELECTRONIC/MECHANICAL EAVESDROPPING 3

I. Oral/Wire Communications. 3

A. Scope of Title I. 4

B. Procedural Requirements. 7

C. Roving Interceptions 10

D. Violations of Title I. 11

E. Disclosure and Derivative Use Orders. 13

F. Law Enforcement Officers. 15

II. Electronic Communications 16

A. Electronic Communications Defined. 16

1. Electronic Mail. 17

2. Modems/Computer-To-Computer Communications. . 17

3. Electronic Bulletin Boards/Direct Dial Network. 17

4. Microwave or Satellite Transmissions. 17

5. Cellular Telephones. 18

6. Electronic Pagers. 19

7. Teletypewriter Exchanges (TELEX). 20

8. Facsimile Transmission. 20

B. Electronic Communications Interception. 20

1. Electronic Communications In Transmission. . . 20

TITLE II - STORED ELECTRONIC COMMUNICATIONS 22

I. Scope. 22

II. Electronic Communications In Storage. 22

A. Disclosure of Stored Communications. 22

B. Access. 23
C. Notice. 24
D. Cost Reimbursement. 25
E. Backup Preservation. 25
F. Offenses/Penalties. 26
G. ECPA Interface With Privacy Statutes 27
TITLE III - PEN REGISTERS/TRAPS-AND-TRACES 29
I. Definitions. 29
II. Statutory Procedures. 30
III. In Camera Hearings. 31
CONVERSATIONAL MONITORING 32
I. Without Devices. 32
A. Overhearing Telephone Conversations. 32
B. Prisoner Conversations. 32
C. Hearing Aids/Implants. 32
D. Telephone Extensions. 32
1. Communication Carriers. 33
2. Law Enforcement. 33
E. Informants/Undercover Operations and Agents. . . . 34
II. With Devices (Consensual Monitoring). 35
A. Telephonic Monitoring. 35
B. Non-Telephonic Monitoring. 36
1. Undercover Agents. 36
2. Informants. 37
HYBRID COMMUNICATIONS INTERCEPTION 38

I. Cordless Telephones 38

II. Cellular Telephones. 38

III. Voice Mail. 39

IV. Closed Circuit Television. 39

OTHER SURVEILLANCE METHODS 40

I. Beepers/Transponders/Electronic Tracking Devices. . . . 40

II. Mail Covers. 41

III. Visual Enhancement Devices (Binoculars or Telescopes or Nightscopes) 41

IV. Video Surveillance. 42

A. Fourth Amendment Considerations. 42

B. Video Surveillance of Public View Areas. 43

C. Public Access and Other Areas Entitled to Fourth Amendment Protection. 44

D. Video Surveillance When Consenting Party is Present. 45

E. Judicial Procedures for Nonconsensual Video Surveillance 46

V. Aerial Surveillance. 47

INTRODUCTION

Surveillance, in its broadest sense, encompasses many forms. Included are physical visual surveillance, video surveillance, and audio surveillance, such as consensual or non-consensual monitoring (i.e. - wiretapping and room bugging) which capture the contents of a conversation. Other forms of surveillance intercept only the fact that a conversation occurred, but not its contents (i.e. - pen registers and trap and trace devices). While this handbook focuses primarily on types of surveillance which utilize electronic devices and equipment, it also covers other forms of surveillance such as mail covers, video surveillance, and aerial surveillance. Each of these areas has its own set of rules, many of which reflect recent changes required to keep pace with a constantly changing technology.

Prior to 1968, there were no federal statutes regulating government wiretapping and surveillance activities. That same year, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968. Title III of the Act, 18 U.S.C. § 2510 et seq., (hereinafter "Act") provided a comprehensive scheme regulating wiretapping; electronic surveillance; interception of oral or wire communications; and use of evidence derived therefrom. The Act imposed very exacting requirements upon the use of the investigative devices within its scope. However, due to technological advances within the past decade, the Act could not keep pace. Congress, once again, responded.

On October 21, 1986, President Reagan signed into law the Electronic Communications Privacy Act of 1986, Public Law No. 99-508 (hereinafter ECPA). This legislation was primarily a comprehensive revision of the Act designed to cover all of the technological advances in the area of electronic communications which were developed since the passage of the original Act. ECPA extended protection to all known electronic communications to which expectations of privacy could reasonably attach during the transmission and storage stages. ECPA also regulates various forms of electronic surveillance by setting forth procedures and remedies relating to them. ECPA contains three separate, but closely related, titles which follow.

Title I pertains to the Interception of Communications and Related Matters, 18 U.S.C. § 2510 et seq., and regulates wire, oral, and electronic communications. This statute was formerly called Title III.

Hence, whenever wiretap information is to be released to the Service, it should be released to a special agent who will review the evidence and, in turn, may provide it to the revenue agent. The court order which permits the special agent to receive the information must contain broad language to permit him to use it for all tax-related purposes, including civil action.

The courts have supported the Service's civil use of such evidence pursuant to court order as long as the original intent of the surveillance was not to obtain the information for a civil tax investigation. Exchanges between the FBI and the IRS have also been upheld by the courts. See Resha v. United States, 767 F.2d 285 (6th Cir. 1985); Dickens v. United States, 671 F.2d 969 (6th Cir. 1982); United States v. Civella, 666 F.2d 1122 (8th Cir. 1981); Griffin v. United States, 588 F.2d 521 (5th Cir. 1979); Fleming v. United States, 547 F.2d 872 (5th Cir. 1977); United States v. Iannelli, 477 F.2d 999 (3rd Cir. 1973), aff'd, 420 U.S. 770 (1975); United States v. Levine, 690 F. Supp. 1165 (E.D.N.Y. 1988); and Perillo v. Commissioner, 78 T.C. 534 (1982).

II. Electronic Communications (Communications Not Containing The Human Voice)

Access to electronic communications in transmission is governed by Title I, while access to stored electronic communications is covered by Title II, 18 U.S.C. § 2701 et seq.

A. Electronic Communications Defined.

Generally, electronic communications are those which do not contain the human voice at any point during the transmission. 18 U.S.C. § 2510(12) defines an electronic communication as "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, photoelectronic or photooptical system that affects interstate or foreign commence". This category includes systems such as digital display pagers; electronic mail; electronic bulletin boards; computer-to-computer transmissions; facsimile transmissions and private video transmissions (but not video surveillance). Some of the forms of electronic communications which are covered by the statute are defined more fully below. The key point to bear in mind is that an interception order is required before interception can begin on any of these forms, unless there is consent.

1. Electronic Mail.

Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. Messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail. It is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system. You need an order to intercept these communications during transmission.

2. Modems/Computer-To-Computer Communications.

Common computer-to-computer communications include the electronic transmission of financial records or fund transfers among financial institutions; medical records between hospitals and/or physicians' offices; and the transmission of proprietary data among the various branch offices of a company. You will need an order to intercept such communications in transmission.

3. Electronic Bulletin Boards/Direct Dial Networks.

Electronic bulletin boards are communication networks created by computer users for the transfer of information among computers. These may take the form of proprietary systems or they may be noncommercial systems operating among computer users who share special interests. These systems may involve fees covering operating costs and may require special "passwords" which restrict entry to the system. These bulletin boards may be private, public, or semi-public in nature, depending on the degree of privacy sought by users, operators or organizers of such systems. You will need an order to intercept these networks.

4. Microwave or Satellite Transmissions.

Microwave or Satellite Transmissions consist of high frequency radio waves transmitted point-to-point on line-of-sight paths between antennae located on towers or building tops (in terrestrial microwave systems), or between satellites and earth station "dish" antennae (in satellite-based systems).

Cable or Premium Pay television transmissions are considered electronic communications and are protected by Title I because the transmissions are usually scrambled or encrypted. See 18 U.S.C. § 2510(16). Modifying or cloning Satellite Descrambler Modules for the purpose of receiving premium pay or cable television transmissions without paying a fee to the cable programmers violates Title I. In United States v. One Macom Video Cipher II, 985 F.2d 258 (6th Cir. 1993), the Sixth Circuit ruled that committing such an act is subject to criminal prosecution under Title I and the equipment that improperly intercepted the transmission, is subject to forfeiture under Section 2513. See also United States v. Herring, 993 F.2d 784 (11th Cir. 1993); United States v. Shriver, 989 F.2d 898 (7th Cir. 1992); and United States v. Lande, 968 F.2d 907 (9th Cir. 1992).

Radio and network television broadcasts are not considered electronic communications for Title I purposes because they are not encrypted and are intended to be readily accessible by the viewing public. See 18 U.S.C. § 2511(2)(g) and Greek Radio Network of America, Inc. v. Vlasopoulos, 731 F. Supp. 1227 (E.D.Pa. 1990).

5. Cellular Telephones.

This technology uses both radio-to-wire or radio-to-radio to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wires or cables.

In a cellular telephone system, large service areas are divided into "cells", each of which is equipped with a lower-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there, the signal travels over phone lines or a microwave to a computerized mobile telephone switching office (MTSO) or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone (typically in a motor vehicle) moves from cell to cell.

Cellular technology, because it is complex, is more difficult to intercept than traditional telephones. It is, however, more accessible than microwave transmissions. Cellular telephone calls can be intercepted by either sophisticated scanners designed

77

for that purpose or by regular radio scanners modified to intercept cellular calls. Using either method, without a court order, violates Title I.

Title I specifically protects cellular telephone calls by including this type of communication within the definition of "wire" communication, whether or not any portion of the transmission utilizes traditional telephone systems. See 18 U.S.C. § 2510. This was done to clear confusion in existing law and to recognize that the public, in using new forms of communication, should have a reasonable expectation that their entire conversation will be private.

6. Electronic Pagers.

Pagers (which are erroneously called beepers) are radio activated devices through which a user is notified of another's attempt to contact him/her. Pagers come in three basic forms: "tone-only"; "digital display" or "clone"; and "tone-and-voice".

The "tone-only" pager emits a "beep" or other signal to inform the user that a message is waiting, and that the message can be retrieved by the user calling a predetermined number (usually an office or answering service). "Tone-only" pagers are exempt from Title I requirements. See 18 U.S.C. § 2510(12)(c).

"Display" or "clone" pagers are equipped with screens that can display visual messages (usually the telephone number of the person seeking to reach the person being paged.) The party seeking to contact the user is instructed to provide a message, usually by pushing the buttons of a touch-tone telephone. This message is stored by the paging company's computer until it can be transmitted to the user's pager. The message can then be read directly by the user, obviating the need for the user to make a telephone call to retrieve the message. These pagers are included within the ambit of "electronic communications". "Display" pagers, unlike "tone-only" pagers, require a court order for interception. See United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990).

The most sophisticated type of pager is the "tone-and-voice" pager. It can receive a spoken message that the paging company's computer has taken from the party seeking to contact the user. After the beep tone is made, the pager "repeats" the recorded message. This requires that a radio signal containing voice communications be sent from the paging company's base

to the mobile unit. This type of pager is included within the category of "wire communications" of Title I, and a court order pursuant to 18 U.S.C. § 2518 is required. See 18 U.S.C. § 2510(1).

7. Teletypewriter Exchanges (TELEX).

A "TELEX" refers to a message sent or received through a communication system consisting of teletypewriters connected to a telephone net work which is designed to send and receive signals. You need an order to intercept these transmissions. See United States v. Gregg, 829 F.2d 1430 (8th Cir. 1987).

8. Facsimile Transmission.

This method transmits an exact copy or reproduction of a document. The user enters a document through a machine (similar to a photo copier) which duplicates the document and electronically transmits the copy over telephone lines to a different location. Many facsimile machines use special encryption which will make interception all the more difficult. You must know the equipment you seek to intercept. You need an order to intercept these transmissions.

B. Electronic Communications Interception.

ECPA sets forth procedures for interception of electronic communications while in transmission (Title I) as well as access to stored (Title II) electronic communications.

1. Electronic Communications In Transmission.

Interceptions of electronic communications in transmission are governed by Title I, thus an application and an affidavit must be prepared. A court order must be obtained before monitoring can begin. See 18 U.S.C. § 2518. Seeking the order is the same as seeking a "wiretap" order, except for the following major differences:

a. An application may be made in connection with any federal felony, including Title 26 offenses. See 18 U.S.C. § 2516(3).

b. The term "intercept" has been broadened to accommodate the non-aural acquisition of electronic communications. Prior to ECPA, interceptions included only those

communications which could be heard and received by the human ear. See 18 U.S.C. § 2510(4).

Even though 18 U.S.C. § 2516(3) provides that " [a]ny attorney for the Government . . . may authorize an application to . . . a federal judge . . . ," to insure uniformity, the Department of Justice informed Congress that, for the first few years following enactment, applications for this type of interception must be approved by the same Department officials who approve wire and oral interception applications. This requirement has been extended beyond its expected duration and continues to be in effect.

Intentional violations of the statute are punishable by up to 5 years imprisonment and fines can range up to $500,000. See 18 U.S.C. § 2511(4)(a). An exception to the felony provision is made for first time interceptions of electronic communications not for tortious purposes or for private commercial gain. First time offenders face one year in jail and/or fines up to $100,000, depending on the circumstances. See Section 2511(4)(b)(i) and (ii).

TITLE II - STORED ELECTRONIC COMMUNICATIONS

I. Scope.

Title II of ECPA, 18 U.S.C. § 2701 et seq., governs access to stored electronic communications and transactional records. It is modeled after the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq, in that it balances privacy interests in personal and proprietary information, with the government's legitimate law enforcement needs. It establishes procedures for obtaining this information.

CAVEAT: If you seek access to stored wire information, such as a telephone answering machine which contains a human voice, you need a Title I order. Title II of ECPA only covers stored electronic communications.

II. Electronic Communications In Storage.

Electronic communications which are in storage includes storage of electronic messages both before and after transmission; backup copies retained for re-access by the recipient; and backup copies used by the communications company.

This statute also addresses a storage system called a "Remote Computer Service". These computer entities provide various electronic bulletin board services to customers or subscribers. They process and store subscriber/customer electronic data for future use or reference. Data is most often transmitted between these entities and their customers by means of electronic communications.

A. Disclosure of Stored Communications.

18 U.S.C. § 2702 prohibits disclosure of electronic communications by the party storing the information unless:

1. The information is given to its intended recipient or addressee. See 18 U.S.C. § 2702(b)(1);

2. The information is given to the government pursuant to court order; search warrant; subpoena. See 18 U.S.C. § 2702(b)(2);

3. The subscriber/customer gives consent. See 18 U.S.C. § 2702(b)(3);

4. The disclosure is to a facility used to forward the communication. See 18 U.S.C. § 2702(b)(4);

5. The disclosure is incident to testing equipment or quality of service. See 18 U.S.C. § 2702(b)(5); or

6. The information was obtained inadvertently and it refers to a crime. See 18 U.S.C. § 2702(b)(6)(A) and (B).

B. Access.

18 U.S.C. § 2703 sets forth the requirements for government access to electronic communications in storage and in a remote computing service. This includes data stored in a display pager. In United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990), the Sixth Circuit ruled that the seizure of the defendant's telephone number stored in a display pager was within the scope of the search warrant for telephone numbers of the drug dealer/target's customers, suppliers, and couriers.

If the contents of an electronic communication have been in storage for 180 days or less, the government must obtain a search warrant in order to have the carrier disclose the contents. The search warrant must be based upon probable cause and notice is not required. As with any federal search warrant, it must comply with Fed. R. Crim. P. 41. See 18 U.S.C. § 2703(a).

If the contents of an electronic communication have been in storage for more than 180 days, or if the contents are stored in a remote computing service, 18 U.S.C. § 2703(b) sets forth the following requirements for obtaining access:

1. Without notice to the subscriber or customer, the government must obtain a Fed. R. Crim. P. 41 search warrant. See 18 U.S.C. § 2703(b)(1).

2. With notice to the subscriber/customer, the government can use:

   a. An administrative or trial or grand jury subpoena. See 18 U.S.C. § 2703(b)(1)(B)(i);

   b. A Rule 41 search warrant. See 18 U.S.C. § 2703(c)(1)(B)(ii); or

   c. A disclosure court order. See 18 U.S.C. § 2703(d).

To obtain a disclosure court order, the government submits an application which shows that the contents sought are relevant to a law enforcement inquiry. The court must so find. The carrier may also move to quash or modify the court order if it can show that the data are unusually voluminous or that compliance would cause an undue burden. See 18 U.S.C. § 2703(b) and (d). Only relevancy, not probable cause, is required in an application for the disclosure court order. The application must show that the information sought is relevant to a legitimate law enforcement inquiry.

The statute also covers situations where the government seeks access to general information about a subscriber or customer, not the contents of their communications. This information, commonly referred to as transactional information, includes data such as the customer's schedules (times and days) of transmissions; the length and frequency of transmissions; billing address; toll records; and unlisted numbers. Such information can be obtained by:

1. An administrative or trial or grand jury subpoena. See 18 U.S.C. § 2703(c)(1)(B)(i).

2. A search warrant pursuant to Fed. R. Crim. P. 41. See 18 U.S.C. § 2703(c)(1)(B)(ii).

3. A disclosure court order issued on relevancy. See 18 U.S.C. § 2703(d).

4. Consent from the customer or subscriber of the service. See 18 U.S.C. § 2703(c)(1)(B)(iv).

C. Notice.

To balance law enforcement interests with privacy concerns, 18 U.S.C. § 2705 addresses notification. Generally, an electronic communications service can give notice to a customer or subscriber about entities who want access to their accounts.

However, 18 U.S.C. § 2705 further provides that a government entity can delay notification to a subscriber or customer for a ninety (90) day interval when it is seeking a subpoena or a disclosure court order. If a court order is granted, the court must certify that notice is delayed. If a subpoena is issued, a supervisory official certifies that notice is delayed. See 18 U.S.C. § 2705(a)(1)(A), (B), and (a)(6).

With certification, under 18 U.S.C. § 2705(a)(2), there must be a reasonable belief that notice will have an adverse result such as:

1. Endangering the life or physical safety of a person;

2. Causing a target to flee;

3. Causing the destruction of evidence; or,

4. Jeopardizing an investigation or unduly delaying a trial.

Upon expiration of the delayed period of notification, 18 U.S.C. § 2705(a)(5) requires that notice be sent to the customer or subscriber. However, extensions can be obtained in appropriate cases. See 18 U.S.C. § 2705(a)(4). The government

entity can physically serve the notice or deliver it by registered or first-class mail. The notice must state the nature of the inquiry with reasonable specificity, 18 U.S.C. § 2705(5)(A), and must provide the following information:

1. The name of the computing service involved; the information sought; and the date that supplying occurred. See 18 U.S.C. § 2705(5)(B)(i).

2. That notification was delayed pursuant to certification. See 18 U.S.C. § 2705(5)(B)(ii).

3. Which entity or court made the certification. See 18 U.S.C. § 2705(5)(B)(iii).

4. Which adverse result was alleged to permit the delay. See 18 U.S.C. § 2705(5)(B)(iv).

D. Cost Reimbursement.

Electronic service providers must be reimbursed for their costs of searching for, assembling, and reproducing electronic communications as well as the costs due to the disruption of their normal business operations. The expenses must be directly incurred by the request/warrant/subpoena, and must be reasonably necessary. See 18 U.S.C. § 2706(a).

The amount must be mutually agreed to or the court will set an amount. See 18 U.S.C. § 2706(b). Cost reimbursement for routine searches of telephone toll records and telephone listings are not permitted unless the information is unusually voluminous or caused an undue burden on the provider. See Michigan Bell Telephone Company v. Drug Enforcement Administration, 693 F.Supp. 542 (E.D.Mich. 1988), in which the court ruled that the provision did not allow compensation for costs of compliance for routine search requests for toll or subscriber information, and 18 U.S.C. § 2706(c).

E. Backup Preservation.

A government agency may also include in its subpoena or court order a requirement that the service provider create a backup copy of the electronic communications' contents in order to preserve it. A provider must make the copy within two business days after receipt of the subpoena or court order and must confirm to the agency that the backup copy has been made. See 18 U.S.C. § 2704(a)(1) and (5).

JG

The provider cannot notify the subscriber about the backup copy request but, notice shall be made by the government agency within three (3) days of the provider's confirmation unless a delayed notification (for a 90 day period) is in effect. See 18 U.S.C. § 2704(a)(1) and (2).

The service provider shall not destroy the backup copy until the later of:

1. The delivery of the information; or

2. The conclusion of any proceedings regarding the government's subpoena or court order, 18 U.S.C. § 2704(a)(3)(A) and (B).

The Service provider must give a copy of the information to the government agency fourteen (14) days after the agency notifies the customer/subscriber. However, the provider does not need to give a copy if the subscriber or customer has challenged the government's request or if the provider intends to challenge the request. See 18 U.S.C. § 2704(a)(4)(A) and (B).

Within 14 days of notification, a subscriber or customer can challenge a government request by filing a motion to quash a subpoena or a motion to vacate a court order. See 18 U.S.C. § 2704(b)(1) requires an affidavit in which the customer swears he is the subscriber and sets forth his reasons why the request should be denied.

The statute also provides for a hearing and, if the court denies the subscriber's motion, the denial is not deemed a final order and no interlocutory appeal may be taken. See 18 U.S.C. § 2704(b)(3) and (4) and (5).

F. Offenses/Penalties.

18 U.S.C. § 2701 creates a criminal offense for anyone who either intentionally accesses (without authority) an electronic communications service; intentionally exceeds an access authorization; or obtains, alters, or prevents authorized access to such a facility. See 18 U.S.C. § 2701(a)(1) and (2) and Steven Jackson Games Inc v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

The penalties for such violations depend upon the motive. If the offense was committed for commercial advantage; private commercial gain; or malicious destruction/damage, there is a $250,000 fine and/or one year imprisonment for a first-time offender. A repeat offender faces a $250,000 fine and/or two years imprisonment. See 18 U.S.C. § 2701(b)(1)(A) and (B). In all other cases, the offender faces a $5,000 fine and/or 6 months imprisonment. See 18 U.S.C. § 2701(b)(2).

A subscriber or customer aggrieved by a provider's violation may file a civil action for relief. 18 U.S.C. § 2707 establishes the amounts of damages which may be recovered and provides a statute of limitations of two years from the date of discovery. The Second Circuit in Organizacion Jd Ltda and Manufacturas Jd, Ltda. v. United States, 18 F.3d 91 (2d Cir. 1994), held that government "entities" could be subject to liability under Section 2707(a).

18 U.S.C. § 2707(d) sets forth the defenses available to a service provider who is sued by his customer or subscriber. They include:

1. A good faith reliance on a court order; search warrant; subpoena; certification; or legislative or statutory authorization; or

2. A good faith reliance on a request for an emergency interception under 18 U.S.C. § 2518(7); or

3. A good faith belief that 18 U.S.C. § 2511(3) permitted the conduct in question.

There is no statutory exclusionary rule. Only constitutional violations will permit a judge to exclude evidence gathered in violation of the statute. See 18 U.S.C. § 2708.

G. ECPA Interface With Privacy Statutes

In the case of Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), ECPA was deemed to interact with a privacy statute, and the challenged searches and seizures were determined to be illegal. The plaintiff was a remote computer service which offered various electronic bulletin board services to the public and its users, in addition to publishing assorted computer games, books, and magazines.

During the course of its investigation into a Bell South computer hacking incident, the Secret Service erroneously concluded that the plaintiff was involved. It failed to determine if there was any link between a computer hacker and the plaintiff. The Secret Service obtained a search warrant for the plaintiff's premises and seized over 300 disks, assorted computer equipment, and all the data stored therein, including all backup materials. The seizure occurred on March 1, 1990. The plaintiff's employees had informed the agents that they were seizing data that was being prepared for publication. Despite repeated requests from the plaintiff's attorneys for the backup data, the Secret Service did not return any of the data until late June 1990. Some of the data had also been deleted without the plaintiff's consent.

The plaintiff sued for damages under Title II and the Privacy Protection Act, 42 U.S.C. § 2000aa et seq., (hereinafter "Act"). The court faulted the Secret Service for their failure to adequately investigate the alleged link between the plaintiff and the computer hacker. In fact, there was no link. The court found that the Secret Service's failure to promptly return the seized items to the plaintiff was unjustifiable and had caused it economic harm.

The court said that the Act prohibited government law enforcement officers from searching for or seizing work product or documentary materials which are intended for dissemination to the public via newspaper, broadcast, or similar format. The court ruled that the seized data was work product and documentary material protected by the Act. By seizing all of the data and, thereafter, failing to promptly return it, the Secret Service violated the Act. The court granted the plaintiff's request for its expenses of $8,781.00 and its economic damages of $42,259.00.

It also ruled that the Secret Service had violated Title II because it had not complied with those provisions that require notice; provide an opportunity to quash; and require backup data preservation (Sections 2703, 2704, and 2705). The court then imposed the statutory damages provision of $1,000.00 (Section 2707).

The court went on to note that most of the problems with the case resulted from the government's ignorance of the pertinent statutes. It stressed that such searches and seizures highlight the traps for the unwary.

HYBRID COMMUNICATIONS INTERCEPTION

Hybrid communications, which are combinations of wire and electronic communications or wire and radio communications, can create special problems. For instance, two parties can converse on a telephone line, then using facsimile machines, send data to each other over the same telephone line, and then return to the voice conversation before terminating it. If there is a wire or oral segment to the communication, then a Title I order is required.

Some of these problems were specifically addressed in ECPA. Others require an analysis of each component part of the transmission with the government following the rules that apply to each part.

I. Cordless Telephones.

A cordless telephone consists of a handset and a base unit wired to a land line and an electrical current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit, the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios.

The interception of radio portion of a hand-held or cordless telephone communication is exempt from Title I. See 18 U.S.C. § 2510(1) and (12). This exemption recognizes that such "backyard" phones are so easily intercepted within their very short range from the base station phone that no true privacy interests can be deemed present. An interception of the wire portion of such a conversation, however, still requires a Title I order, obtained pursuant to 18 U.S.C. § 2518.

II. Cellular Telephones.

All cellular telephone conversations are covered by Title I. A reference to connections in switching stations in 18 U.S.C. § 2510(1) is included so that even radio-to-radio cellular communications that occur between persons using two cellular car phones will come within Title I. Hence, a court order, obtained pursuant to 18 U.S.C. § 2518, is mandatory, unless specifically exempt by the statute.

Including cellular communications within Title I is a congressional recognition that persons using fully mobile car phones or briefcase phones expect their conversations to be private.

III. **Voice Mail**.

Voice Mail is a sophisticated answering system. A person calls another person who subscribes to voice mail. The caller leaves a message (in human voice) and the message is stored on a disk (either a floppy disk, an optical disk, or a hard drive). The message is retrieved by the caller from any touch-tone telephone using a private password. The message is delivered in a computer-generated voice. This transmission is a hybrid because it contains an electronic transmission as well as a wire communication.

Voice Mail may also store the message in human voice and transmit the message in the human voice, rather than in a computer generated voice. These are extremely sophisticated systems and still use wire as part of the transmission.

ECPA's legislative history addresses the potential problem of combining electronic and wire communications into one conversation. The history makes it clear that if any part of the conversation is a wire communication, then for purposes of the Act, Congress expects the conversation to be deemed a wire communication. H. Rep. No. 99-647, 99th Cong., 2d Sess. p. 35 (1986).

Since part of a voice mail transmission involves wire, Title I would govern. Thus, a wire intercept order must be obtained pursuant to 18 U.S.C. § 2518 and the offense involved must be one of the specifically listed predicate offenses of 18 U.S.C. § 2516.

IV. **Closed Circuit Television**.

Commonly used as a security measure, these are private video transmissions. These transmissions are a hybrid because they may contain an audio or voice portion as well as the video portion.

The interception of the audio portion of the transmission, requires a wire intercept order obtained pursuant to 18 U.S.C. § 2518 for one of the predicate offenses listed in 18 U.S.C. § 2516. Interception of the video portion of the closed circuit television transmission requires an electronic intercept order obtained pursuant to 18 U.S.C. § 2518 for any federal felony, including Title 26 crimes. You may use one affidavit when applying for both orders. See United States v. Falls, 34 F.3d 674 (8th Cir. 1994).