

Appendix A

Sample Network Banner Language

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions. First, banners may eliminate any Fourth Amendment “reasonable expectation of privacy” that users might otherwise retain in their use of the network. Second, banners may generate consent to real-time monitoring under Title III. Third, banners may generate consent to the retrieval of stored files and records pursuant to the SCA. Fourth, in the case of a non-government network, banners may establish the network owner’s common authority to consent to a law enforcement search.

CCIPS does not take any position on whether providers of network services should use network banners, and, if so, what types of banners they should use. Further, there is no formal “magic language” that is necessary. Banners may be worded narrowly or broadly, and the scope of consent and waiver triggered by a particular banner will in general depend on the scope of its language. Here is a checklist of issues to consider when evaluating a banner:

a) Does the banner state that a user of the network shall have no reasonable expectation of privacy in the network? A user who lacks a reasonable expectation of privacy in a network will not be able to claim that any search of the network violates his Fourth Amendment rights. *See Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

b) Does the banner state that use of the network constitutes consent to monitoring? Such a statement helps establish the user’s consent to real-time interception pursuant to 18 U.S.C. § 2511(2)(c) (monitoring by law enforcement agency) or § 2511(2)(d) (provider monitoring).

c) Does the banner state that use of the network constitutes consent to the retrieval and disclosure of information stored on the network? Such a statement helps establish the user’s consent to the retrieval and disclosure of such information and/or records pursuant to 18 U.S.C. §§ 2702(b)(3) and 2702(c)(2).

d) In the case of a non-government network, does the banner make clear that the network system administrator(s) may consent to a law enforcement search? Such a statement helps establish the system administrator's common authority to consent to a search under to *United States v. Matlock*, 415 U.S. 164 (1974).

e) Does the banner contain express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring?

f) Does the banner state which users are authorized to access the network and the consequences of unauthorized use of the network? Such notice makes it easier to establish knowledge of unauthorized use and therefore may aid prosecution under 18 U.S.C. § 1030.

g) Does the banner require users to "click through" or otherwise acknowledge the banner before using the network? Such a step may make it easier to establish that the network user actually received the notice that the banner is designed to provide.

Network providers who decide to banner all or part of their network should consider their needs and the needs of their users carefully before selecting particular language. For example, a sensitive government computer network may require a broadly worded banner that permits access to all types of electronic information.

Broad Banners

Here are three examples of broad banners:

(1) You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: you have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system; at any time, and for any lawful government purpose, the Government may monitor, intercept, search, and seize any communication or data transiting or stored on this information

system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

(2) **WARNING!** This computer system is the property of the United States Department of Justice and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. The Department may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit.

(3) You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose, including criminal prosecution.

Narrower Banners

In other cases, network providers may wish to establish a more limited policy. Here are three examples of relatively narrow banners that will generate consent to access in some situations but not others:

(4) This computer network belongs to the Grommie Corporation and may be used only by Grommie Corporation employees and only for work-related purposes. The Grommie Corporation reserves the right to monitor use of this network to ensure network security and to respond to specific allegations of employee misuse. Use of this network shall constitute consent to monitoring for such purposes. In addition, the Grommie Corporation reserves the right to consent to a valid law enforcement request to search the network for evidence of a crime stored within the network.

(5) **Warning:** Patrons of the Cyber-Fun Internet Café may not use its computers to access, view, or obtain obscene materials. To ensure compliance with this policy, the Cyber-Fun Internet Café reserves the right to record the names and addresses of World Wide Web sites that patrons visit using Cyber-Fun Internet Café computers.

(6) It is the policy of the law firm of Rowley & Yzaguirre to monitor the Internet access of its employees to ensure compliance with law firm policies. Accordingly, your use of the Internet may be monitored. The firm reserves the right to disclose the fruits of any monitoring to law enforcement if it deems such disclosure to be appropriate.

counsel, respectfully submits under seal this ex parte application for an Order pursuant to 18 U.S.C. § 2703(d) to require ISPCompany, an Internet Service Provider located in City, State, which functions as an electronic communications service provider and/or a remote computing service, to provide records and other information and contents of wire or electronic communications pertaining to the following email account: sample@sample.com. The records and other information requested are set forth as an Attachment to the proposed Order. In support of this application, the United States asserts:

LEGAL AND FACTUAL BACKGROUND

1. The United States government is investigating [crime summary]. The investigation concerns possible violations of, inter alia, [statutes].

2. Investigation to date of these incidents provides reasonable grounds to believe that ISPCompany has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because ISPCompany functions as an electronic communications service provider (provides its subscribers access to electronic communication services, including email and the Internet) and/or a remote computing service (provides computer facilities for the storage and processing of electronic communications), 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information it is seeking.

3. Here, the government seeks to obtain the following categories of information: (1) records and other information (not including the contents of

communications) pertaining to certain subscribers of ISPCompany; and (2) the contents of electronic communications held by ISPCompany (but not in electronic storage for less than 181 days).

4. To obtain records and other information (not including the contents of communications) pertaining to subscribers of an electronic communications service provider or remote computing service, the government must comply with 18 U.S.C. § 2703(c)(1), which provides, in pertinent part:

A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

....

(B) obtains a court order for such disclosure under subsection (d) of this section.

5. Under 18 U.S.C. § 2703(a)(1) and 18 U.S.C. § 2703(b)(1), to obtain the contents of a wire or electronic communication in a remote computing service, or in electronic storage for more than one hundred and eighty days in an electronic communications system, the government must comply with 18 U.S.C. § 2703(b)(1), which provides, in pertinent part:

A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

....

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

....

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

6. Section 2703(b)(2) states that § 2703(b)(1) applies with respect to any wire or electronic communication that is held or maintained in a remote computing service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

7. Section 2703(d), in turn, provides in pertinent part:

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction¹ and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually

¹ 18 U.S.C. § 2711(3) states that “the term ‘court of competent jurisdiction’ has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.” Section 3127 defines the term “court of competent jurisdiction” to include “any district court of the United States (including a magistrate judge of such a court).” 18 U.S.C. § 3127(2)(A).

voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

8. [Factual paragraph(s) here]

9. The conduct described above provides reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

10. Records of customer and subscriber information relating to this investigation that are available from ISPCCompany, and the contents of electronic communications that may be found at ISPCCompany, will help government investigators to identify the individual(s) who are responsible for the events described above and to determine the nature and scope of their activities. Accordingly, the government requests that ISPCCompany be directed to produce all records described in Attachment A to the proposed Order. Part A of the Attachment requests the account name, address, telephone number, email address, billing information, and other identifying information for sample@sample.com.

11. Part B requests the production of records and other information relating to sample@sample.com through the date of this Court's Order. As described in more detail in that section, this information should include connection

information, telephone records, non-content information associated with any communication or file stored by or for the account(s), and correspondence and notes of records involving the account.

12. Part C requests the contents of electronic communications (not in electronic storage) in ISPCompany's computer systems in directories or files owned or controlled by the accounts identified in Part A. These stored files, covered by 18 U.S.C. § 2703(b)(2), will help ascertain the scope and nature of the activity conducted by sample@sample.com from ISPCompany's computers. Pursuant to 18 U.S.C. § 2703(a), Part C also requests the contents of electronic communications that have been in electronic storage in ISPCompany's computer systems for more than 180 days.

13. The information requested should be readily accessible to ISPCompany by computer search, and its production should not prove to be burdensome.

14. The United States requests that this application and Order be sealed by the Court until such time as the Court directs otherwise.

15. The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), ISPCompany be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Order for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence,

change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

16. The United States further requests, pursuant to the delayed notice provisions of 18 U.S.C. § 2705(a), an order delaying any notification to the subscriber or customer that may be required by § 2703(b) to obtain the contents of communications, for a period of ninety days. Providing prior notice to the subscriber or customer would seriously jeopardize the ongoing investigation, as such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

WHEREFORE, it is respectfully requested that the Court grant the attached Order (1) directing ISPCCompany to provide the United States with the records and information described in Attachment A; (2) directing that the application and Order be sealed; (3) directing ISPCCompany not to disclose the existence or content of the Order or this investigation, except to the extent necessary to carry out the Order; and (4) directing that the notification by the government otherwise required under 18 U.S.C. § 2703(b) be delayed for ninety days; and (5) directing that three certified copies of this application and Order be provided by the Clerk of this Court to the United States Attorney's Office.

Executed on _____

Assistant United States Attorney

UNITED STATES DISTRICT COURT
FOR THE _____

)
IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR)
AN ORDER PURSUANT TO)
18 U.S.C. § 2703(d))
_____)

MISC. NO.

Filed Under Seal

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing ISPCo, an electronic communications service provider and/or a remote computing service, located in City, State, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information and the contents of wire or electronic communications sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that ISPCo will, within seven days of the date of this Order,

turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that ISPCCompany shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

IT IS FURTHER ORDERED that the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for a period of ninety days.

United States Magistrate Judge

Date

ATTACHMENT A

You are to provide the following information, if available, as data files on CD-ROM or other electronic media or by facsimile:

- A. The following customer or subscriber account information for each account registered to or associated with sample@sample.com for the time period [date range]:
 1. subscriber names, user names, screen names, or other identities;
 2. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;
 3. local and long distance telephone connection records, or records of session times and durations;
 4. length of service (including start date) and types of service utilized;
 5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
 6. means and source of payment for such service (including any credit card or bank account number) and billing records.
- B. All records and other information relating to the account(s) and time period in Part A, including:
 1. records of user activity for any connections made to or from the account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
 2. telephone records, including caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or

- ESN);
3. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
 4. correspondence and notes of records related to the account(s).
- C. [Before seeking to compel disclosure of content, give prior notice to the customer or subscriber *or* comply with the delayed notice provisions of 18 U.S.C. § 2705(a).] The contents of electronic communications (not in electronic storage²) in ISPCompany’s systems in directories or files owned or controlled by the accounts identified in Part A at any time from [date range]; and the contents of electronic communications that have been in electronic storage in ISPCompany’s electronic communications system for more than 180 days [and within date range].

² “Electronic storage” is a term of art, specifically defined in 18 U.S.C. § 2510(17) as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” The government does not seek access to any communications in “electronic storage” for less than 181 days. [The following sentence may not be included in the Ninth Circuit; see the discussion of “electronic storage” in Chapter 3.C.3.] Communications not in “electronic storage” include any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

Appendix C

Sample Language for Preservation Requests under 18 U.S.C. § 2703(f)

ISPCompany
Address

Re: Request for Preservation of Records

Dear ISPCompany:

Pursuant to Title 18, United States Code Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the following email address pending further legal process: sample@sample.com (hereinafter, “the Account”).

I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account, or otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. This request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

2. All records and other information relating to the Account and any associated accounts including the following:
 - a. subscriber names, user names, screen names, or other identities;
 - b. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;
 - c. length of service (including start date) and types of service utilized;
 - d. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
 - e. telephone records, including local and long distance telephone connection records, caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or ESN);
 - f. telephone or instrument number or other subscriber number or identity, including temporarily assigned network address;
 - g. means and source of payment for the Account (including any credit card or bank account numbers) and billing records;
 - h. correspondence and other records of contact by any person or entity about the Account, such as “Help Desk” notes; and
 - i. any other records or evidence relating to the Account.

If you have questions regarding this request, please call me at [phone number].

Sincerely,

[NAME]

[GOVERNMENT ENTITY]

Appendix D

Sample Pen Register/Trap and Trace Application and Order

The sample pen/trap application and order below are designed (1) to collect email addresses to which the account owner sends email and from which the account owner receives email and (2) to collect IP addresses associated with the transmission of email and the account owner's access to the email account. Investigators may edit the application in order to remove requests for information that will not be needed in a particular case.

UNITED STATES DISTRICT COURT
FOR THE [DISTRICT]

IN RE APPLICATION OF THE)	
UNITED STATES OF AMERICA FOR)	MISC. NO. _____
AN ORDER AUTHORIZING THE)	
INSTALLATION AND USE OF PEN)	
REGISTER AND TRAP AND)	
TRACE DEVICES)	
)	Filed Under Seal

APPLICATION

The United States of America, moving by and through [AUSA name], its undersigned counsel, respectfully submits under seal this ex parte application for an Order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen/trap devices”) on the [service provider] email account [target email address] whose

listed subscriber is [subscriber name]. In support of this application, the United States asserts:

1. This is an application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.

2. Under 18 U.S.C. § 3122(b), such an application must include three elements: (1) “the identity of the attorney for the Government or the State law enforcement or investigative officer making the application”; (2) “the identity of the law enforcement agency conducting the investigation”; and (3) “a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.” 18 U.S.C. § 3122(b).

3. The attorney for the Government making the application is the undersigned, [AUSA name], who is an “attorney for the government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the [law enforcement agency].

5. The applicant hereby certifies that the information likely to be obtained by the requested pen/trap devices is relevant to an ongoing criminal investigation being conducted by [law enforcement agency].

ADDITIONAL INFORMATION

6. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use

of pen/trap devices specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court’s authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

7. A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.” 18 U.S.C. § 3127(3). A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.” 18 U.S.C. § 3127(4).

8. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

9. The Internet is a global network of computers and other devices. Every device on the Internet is identified by a unique number called an Internet Protocol, or “IP” address. This number is used to route information between devices. Two computers must know each other’s IP addresses to exchange even the smallest amount of information. Accordingly, when one computer requests information from a second computer, the requesting computer specifies its own IP address so that the responding computer knows where to send its response.

An IP address is analogous to a telephone number and can be recorded by pen/trap devices, and it indicates the online identity of the communicating device without revealing the communication's content.

10. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discreet packets. Generally, a single communication is sent as a series of packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet's source and destination IP addresses and the packet's size.

11. An email message has its own routing header, in addition to the source and destination information associated with all Internet data. The message header of an email contains the message's source and destination(s), expressed as email addresses in "From," "To," "CC" (carbon copy), or "BCC" (blind carbon copy) fields. Multiple destination addresses may be specified in the "To," "CC," and "BCC" fields. The email addresses in an email's message header are like the telephone numbers of both incoming and outgoing calls, because they indicate both origin and destination(s). They can be recorded by pen/trap devices and can be used to identify parties to a communication without revealing the communication's contents.

THE RELEVANT FACTS

12. The United States government, including the [law enforcement agency], is investigating [crime facts]. The investigation concerns possible violations by unknown individuals of, inter alia, [statutes].

13. [***OPTIONALLY INSERT FACTUAL PARAGRAPH(S) HERE. Please note that additional facts are not required by statute, but some districts include them in applications anyway. For example, some districts will include a fact paragraph like this one: “The investigation relates to the purchase and sale of stolen credit cards and other unauthorized access devices, which are then used to perpetrate mail and wire fraud. Investigators believe that matters relevant to the offenses under investigation have been and continue to be discussed using jjones007992@isp.com. Investigators believe that the listed subscriber for this email address number is John Jones, a target of the investigation, ...”]

14. The conduct being investigated involves use of the email account [target email address]. To further the investigation, investigators need to obtain the dialing, routing, addressing, and signaling information associated with communications sent to or from that email account.

15. The pen/trap devices sought by this application will be installed at location(s) to be determined, and will collect dialing, routing, addressing, and signaling information associated with each communication to or from the [service provider] email account [target email address], including the date, time,

and duration of the communication, and the following, without geographic limit:

- IP addresses, including IP addresses associated with access to the account;
- Headers of email messages, including the source and destination network addresses, as well as the routes of transmission and size of the messages, but not content located in headers, such as subject lines;
- the number and size of any attachments.

GOVERNMENT REQUESTS

16. For the reasons stated above, the United States requests that the Court enter an Order authorizing installation and use of pen/trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication to or from the [service provider] email account [target email address], along with the date, time, and duration of the communication, without geographic limit. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8), pursuant to the proposed Order.

17. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days, pursuant to 18 U.S.C. § 3123(c)(1).

18. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order [service provider] and any

other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to install the pen/trap devices, including installation and operation of the pen/trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by [law enforcement agency], pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in providing facilities and assistance in furtherance of this Order.

19. The United States further requests that the Court order [service provider] and any other person or entity whose assistance may facilitate execution of this Order to notify [law enforcement agency] of any changes relating to the email account [target email address], including changes to subscriber information, and to provide prior notice to the [law enforcement agency] before terminating service to the email account.

20. The United States further requests that the Court order that the [law enforcement agency] and the applicant have access to the information collected by the pen/trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

21. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order [law enforcement agency] and any other person or entity whose assistance facilitates execution of this Order, and their

agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this application and Order, the resulting pen/trap devices, or this investigation, except as necessary to effectuate the Order, unless and until authorized by this Court.

22. The United States further requests that this application and any resulting Order be sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

23. The United States further requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this application and Order, and provide copies of this Order to [law enforcement agency] and [service provider] upon request.

24. The foregoing is based on information provided to me in my official capacity by agents of [law enforcement agency].

I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____.

[AUSA name]

[AUSA title]

[address]

UNITED STATES DISTRICT COURT
FOR THE _____

IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR) MISC. NO.
AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF PEN)
REGISTER AND TRAP AND)
TRACE DEVICES)
_____) Filed Under Seal

ORDER

[AUSA name], on behalf of the United States, has submitted an application pursuant to 18 U.S.C. §§ 3122 and 3123, requesting that the Court issue an Order pursuant to 18 U.S.C. § 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen/trap devices”) on the [service provider] email account [target email address], whose listed subscriber is [subscriber name].

The Court finds that the applicant is an attorney for the government and has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation being conducted by [law enforcement agency] of unknown individuals in connection with possible violations of [statutes].

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 3123, that pen/trap devices may be installed and used to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each

communication to or from the [service provider] email account [target email address], including the date, time, and duration of the communication, and the following, without geographic limit:

- IP addresses, including IP addresses associated with access to the account;
- Headers of email messages, including the source and destination network addresses, as well as the routes of transmission and size of the messages, but not content located in headers, such as subject lines;
- the number and size of any attachments.

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123(c)(1), that the use and installation of the foregoing is authorized for sixty days from the date of this Order;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that [service provider] and any other person or entity providing wire or electronic communication service in the United States whose assistance may, pursuant to 18 U.S.C. § 3123(a), facilitate the execution of this Order shall, upon service of this Order, furnish information, facilities, and technical assistance necessary to install the pen/trap devices, including installation and operation of the pen/trap devices unobtrusively and with minimum disruption of normal service;

IT IS FURTHER ORDERED that [law enforcement agency] reasonably compensate [service provider] and any other person or entity whose

assistance facilitates execution of this Order for reasonable expenses incurred in complying with this Order;

IT IS FURTHER ORDERED that [service provider] and any other person or entity whose assistance may facilitate execution of this Order notify [law enforcement agency] of any changes relating to the email account [target email account], including changes to subscriber information, and to provide prior notice to [law enforcement agency] before terminating service to the email account;

IT IS FURTHER ORDERED that [law enforcement agency] and the applicant have access to the information collected by the pen/trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to [law enforcement agency], for the duration of the Order;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123(d)(2), that [service provider] and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, shall not disclose in any manner, directly or indirectly, by any action or inaction, the existence of the application and this Order, the pen/trap devices, or the investigation to any person, except as necessary to effectuate this Order, unless and until otherwise ordered by the Court;

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three certified copies of this application and Order, and shall provide copies of this Order to [law enforcement agency]

and [service provider] upon request;

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

Date

United States Magistrate Judge

Appendix E

Sample Subpoena Language

The SCA permits the government to compel disclosure of the basic subscriber and session information listed in 18 U.S.C. § 2703(c)(2) using a subpoena. This information is specified in Part A below, and the government is not required to provide notice to the subscriber or customer when using a subpoena to compel disclosure of this information.

When the government either gives prior notice to the customer or subscriber or complies with the delayed notice provisions of 18 U.S.C. § 2705(a), it may use a subpoena to compel disclosure of “the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days” and “the contents of any wire or electronic communication” held by a provider of remote computing service “on behalf of . . . a subscriber or customer of such remote computing service.” 18 U.S.C. §§ 2703(a), 2703(b)(1)(B)(i), 2703(b)(2). This information is specified in Part B below. As discussed in Chapter 3.C.3, there is disagreement among courts on whether previously retrieved communications fall within the scope of communications in “electronic storage.”

The information requested below can be obtained with the use of an administrative subpoena authorized by Federal or State statute or a Federal or State grand jury or trial subpoena or a § 2703(d) order or a search warrant. *See* 18 U.S.C. §§ 2703(b)(1)(B)(i), 2703(c)(2).

Attachment To Subpoena

All customer or subscriber account information for the [choose one: email account, domain name, IP address, subscriber, username] [specify email account, domain name, IP address, subscriber, username], or for any related accounts, that falls within any of the following categories:

1. Name,
2. Address,

3. Local and long distance telephone toll billing records,
4. Records of session times and durations,
5. Length of service (including start date) and types of service utilized,
6. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as an Internet Protocol address, and
7. Means and source of payment for such service (including any credit card or bank account number).
8. [Before seeking to compel disclosure of content, give prior notice to the customer or subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a).] For each such account, the information shall also include the contents of electronic communications (not in electronic storage) held or maintained by your company for the use of the account at any time, up through and including the date of this subpoena; and the contents of electronic communications that have been in electronic storage in your company's electronic communications system for more than 180 days.

“Electronic storage” is defined in 18 U.S.C. § 2510(17) as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” The government does not seek access to any such materials unless they have been in “electronic storage” for more than 180 days.

You are to provide this information, if available, as data files on CD-ROM or other electronic media or by facsimile to [fax number].

Appendix F

Sample Premises Computer Search Warrant Affidavit

This form may be used when a warrant is sought to allow agents to enter a premises and remove computers or electronic media from the premises. In this document, “[[” marks indicate places that must be customized for each affidavit. Fill out your district’s AO 93 Search Warrant form without any reference to computers; your agents are simply searching a premises for items particularly described in the affidavit’s attachment. Consider incorporating the affidavit by reference. See Chapter 2 for a detailed discussion of issues involved in drafting computer search warrants.

UNITED STATES DISTRICT COURT
FOR THE [DISTRICT]

In the Matter of the Search of
[[Premises Address]]

)
) Case No.
)
)
)

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, [[AGENT NAME]], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [[PREMISES ADDRESS]], hereinafter “PREMISES,” for certain things particularly described in Attachment A.

2. I am a [[TITLE]] with the [[AGENCY]], and have been since [[DATE]]. [[DESCRIBE TRAINING AND EXPERIENCE INCLUDING EXPERTISE WITH COMPUTERS]].

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. [[Give facts that establish probable cause to believe that evidence, fruits, or contraband can be found on each computer that will be searched and/or seized, or to believe that the computers may be seized as contraband or instrumentalities.]]

TECHNICAL TERMS

5. [[THIS SECTION MIGHT BE UNNECESSARY; DEFINE ONLY TECHNICAL TERMS AS NECESSARY TO SUPPORT PROBABLE CAUSE.]] Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

COMPUTERS AND ELECTRONIC STORAGE

6. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. I submit that if a computer or electronic

medium is found on the premises, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

d. [[FOR CHILD PORNOGRAPHY CASES]] I know from training and experience that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer’s ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk or computer hard drive can contain many child pornography images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely, if ever, dispose of their sexually explicit materials.

e. [[FOR BUSINESS SEARCH CASES]] Based on actual inspection of [[spreadsheets, financial records, invoices]], I am aware that computer

equipment was used to generate, store, and print documents used in the [[tax evasion, money laundering, drug trafficking, etc.]] scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

7. [[FOR CHILD PORNOGRAPHY OR OTHER CONTRABAND CASES]] In this case, the warrant application requests permission to search and seize [[images of child pornography, including those that may be stored on a computer]]. These things constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware and electronic media that may contain those things if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. [[In this case, computer hardware that was used to store child pornography is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.]]

8. [[FOR CHILD PORNOGRAPHY PRODUCTION CASES]] I know from training and experience that it is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can have a camera built in, or can be connected to a camera and turn the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

9. [[FOR HACKING OR OTHER INSTRUMENTALITY CASES]] I know that when an individual uses a computer to [[obtain unauthorized access to a victim computer over the Internet]], the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

10. [[FOR CASES WHERE A RESIDENCE SHARED WITH OTHERS IS SEARCHED]] Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

11. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

b. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even “hidden,” erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external

sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment may be necessary to complete an accurate analysis.

12. In light of these concerns, I hereby request the Court’s permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

13. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the [[AGENCY]] intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

14. [[INCLUDE THE FOLLOWING IF THERE IS A CONCERN ABOUT THE SEARCH UNREASONABLY IMPAIRING AN OPERATIONAL, OTHERWISE LEGAL BUSINESS]] I recognize that the Company is a functioning company with many employees, and that a seizure of the Company’s computers may have the unintended effect of limiting the Company’s ability to provide service to its legitimate customers. In response to these concerns, the agents who execute the search anticipate taking an incremental approach to minimize the inconvenience to the Company’s legitimate customers and to minimize the need to seize equipment and data. It is anticipated that, barring unexpected circumstances, this incremental approach will proceed as follows:

a. Upon arriving at the PREMISES, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out paper and electronic copies of the things described in the warrant. The assistance of such an employee might allow agents to place less of a burden on the Company than would otherwise be necessary.

b. If the employees choose not to assist the agents, the agents decide that none are trustworthy, or for some other reason the agents cannot execute the warrant successfully without themselves examining the Company's computers, the agents will attempt to locate the things described in the warrant, and will attempt to make electronic copies of those things. This analysis will focus on things that may contain the evidence and information of the violations under investigation. In doing this, the agents might be able to copy only those things that are evidence of the offenses described herein, and provide only those things to the case agent. Circumstances might also require the agents to attempt to create an electronic "image" of those parts of the computer that are likely to store the things described in the warrant. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The agents or qualified computer experts will then conduct an off-site search for the things described in the warrant from the "mirror image" copy at a later date. If the agents successfully image the Company's computers, the agents will not conduct any additional search or seizure of the Company's computers.

c. If imaging proves impractical, or even impossible for technical reasons, then the agents will seize those components of the Company's computer system that the agents believe must be seized to permit the agents to locate the things described in the warrant at an off-site location. The seized components will be removed from the PREMISES. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

CONCLUSION

15. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and seize the items described in Attachment A.

REQUEST FOR SEALING

[[IF APPROPRIATE: It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.]]

Respectfully submitted,

[[AGENT NAME]]

Special Agent

[[AGENCY]]

Subscribed and sworn to before me on _____:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. All records relating to violations of the statutes listed on the warrant and involving [[SUSPECT]] since [[DATE]], including:

- a. [[IDENTIFY RECORDS SOUGHT WITH PARTICULARITY; EXAMPLES FOR A DRUG CASE FOLLOW]];
- b. lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information);
- d. any information recording [[SUSPECT]]'s schedule or travel from 2008 to the present;
- e. all bank records, checks, credit card bills, account information, and other financial records.

2. [[IF OFFENSE INVOLVED A COMPUTER AS AN INSTRUMENTALITY OR CONTAINER FOR CONTRABAND]] Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including [[receiving images of child pornography over the Internet in violation of 18 U.S.C. § 2252A.]]

3. For any computer hard drive or other electronic media (hereinafter, "MEDIA") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;
- b. passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;
- c. documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

4. [[IF CASE INVOLVED THE INTERNET]] Records and things evidencing the use of the Internet Protocol address [[e.g. 10.19.74.69]]

to communicate with [[e.g. Yahoo! mail servers or university mathematics department computers]], including:

- a. routers, modems, and network equipment used to connect computers to the Internet;
- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Appendix G

Sample Letter for Provider Monitoring

As discussed in Chapter 4.D.3.c of this manual, agents and prosecutors should adopt a cautious approach to accepting the fruits of future monitoring conducted by providers under the provider exception. Furthermore, law enforcement may be able to avoid this issue by relying on the computer trespasser exception. However, in cases in which law enforcement chooses to accept the fruits of future monitoring by providers, this letter may reduce the risk that any provider monitoring and disclosure will exceed the acceptable limits of § 2511(2)(a)(i).

This letter is intended to inform [law enforcement agency] of [Provider's] decision to conduct monitoring of unauthorized activity within its computer network pursuant to 18 U.S.C. § 2511(2)(a)(i), and to disclose some or all of the fruits of this monitoring to law enforcement if [Provider] deems disclosure will assist in protecting its rights or property. On or about [date], [Provider] became aware that it was the victim of unauthorized intrusions into its computer network. [Provider] understands that 18 U.S.C. § 2511(2)(a)(i) authorizes

an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service[.]

This statutory authority permits [Provider] to engage in reasonable monitoring of unauthorized use of its network to protect its rights or property and also to disclose intercepted communications to [law enforcement] to further the protection of [Provider]'s rights or property. Under 18 U.S.C. §§

2702(b)(5) and 2702(c)(3), [Provider] is also permitted to disclose customer communications, records, or other information related to such monitoring if such disclosure protects the [Provider]'s rights and property.

To protect its rights and property, [Provider] plans to [continue to] conduct reasonable monitoring of the unauthorized use in an effort to evaluate the scope of the unauthorized activity and attempt to discover the identity of the person or persons responsible. [Provider] may then wish to disclose some or all of the fruits of its interception, records, or other information related to such interception, to law enforcement to help support a criminal investigation concerning the unauthorized use and criminal prosecution for the unauthorized activity of the person(s) responsible.

[Provider] understands that it is under absolutely no obligation to conduct any monitoring whatsoever, or to disclose the fruits of any monitoring, records, or other information related to such monitoring, and that [law enforcement] has not directed, requested, encouraged, or solicited [Provider] to intercept, disclose, or use monitored communications, associated records, or other information for law enforcement purposes.

Accordingly, [Provider] will not engage in monitoring solely or primarily to assist law enforcement absent an appropriate court order or a relevant exception to the Wiretap Act (e.g., 18 U.S.C. § 2511(2)(i)). Any monitoring and/or disclosure will be at [Provider's] initiative. [Provider] also recognizes that the interception of wire and electronic communications beyond the permissible scope of 18 U.S.C. § 2511(2)(a)(i) may potentially subject it to civil and criminal penalties.

Sincerely,

General Counsel

Appendix H

Sample Authorization for Monitoring of Computer Trespasser Activity

I am [Name of Owner/Operator or person acting on behalf of Owner/Operator, Title] of [Name and Address of Organization]. I am the [Owner] [Operator] [person acting on behalf of the Owner or Operator], and own or have the authority to supervise, manage, or control operation of the [relevant part of the] [Organization's] computer system or the data and communications on and through the network. An unauthorized user(s), who I understand has no contractual basis for any access to this computer system, has accessed this computer and is a trespasser(s). I hereby authorize [law enforcement agency] to intercept communications to, through, or from a trespasser(s) transmitted to, through, or from [Organization's] computer system. The general nature of the communications to be monitored are [general description of the identifying characteristics of the communications to be monitored.] [Organization will assist law enforcement agency to conduct such interception under the direction of law enforcement agency.] Such interception may occur at any location on the computer system or network, including at multiple or changed locations, which may facilitate the interception of communications to or from the trespasser.

This authorization does not extend to the interception of communications other than those to, through, or from a trespasser(s). This authorization does not restrict monitoring under any other appropriate exception to the Wiretap Act, 18 U.S.C. § 2510 et seq.

This authorization is valid [for a specified time period] [indefinitely, until withdrawn in writing by me or a person acting for me]. I understand I may withdraw authorization for monitoring at any time, but I agree to do so in writing.

Signature of Owner/Operator

Date

Appendix I

Sample Email Account Search Warrant Affidavit

The sample 2703 search warrant affidavit and attachments below are designed (1) to obtain email messages associated with the target email account that relate to the investigation, and (2) to obtain records relating to who created, used, or communicated with the account. Investigators may edit the affidavit and attachments to remove requests for information that will not be needed in a particular case. In addition, please note that while the facts described in the “background” section of the affidavit are true for most email providers, the affiant should be certain that they are true for the particular email provider that is the subject of the affidavit.

Notes: When filling out the search warrant form, write “See Attachment A” in the section that asks for the location of the search and “See Attachment B” in the section that asks for a description of the items to be seized. Fax the warrant, along with both attachments and the “certificate of authenticity,” to the service provider. The service provider should then give the requested data to the agent, who should cull through the data returned by the provider and isolate material that is not called for by the warrant.

UNITED STATES DISTRICT COURT
FOR THE [DISTRICT]

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[[EMAIL ADDRESSES]] THAT IS STORED
AT PREMISES CONTROLLED BY [[EMAIL
PROVIDER]]

Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, [AGENT NAME], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by [EMAIL PROVIDER], an email provider headquartered at [PROVIDER ADDRESS]. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require [EMAIL PROVIDER] to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the [AGENCY], and have been since [DATE]. [DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS QUALIFICATION TO SPEAK ABOUT THE INTERNET AND OTHER TECHNICAL MATTERS].

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. [Give facts establishing probable cause. At a minimum, establish a connection between the email account and a suspected crime. Also mention whether a preservation request was sent (or other facts suggesting the email is still at the provider)]

TECHNICAL BACKGROUND

5. In my training and experience, I have learned that [EMAIL PROVIDER] provides a variety of on-line services, including electronic mail (“email”) access, to the general public. Subscribers obtain an account by registering with [EMAIL PROVIDER]. During the registration process, [EMAIL PROVIDER] asks subscribers to provide basic personal information. Therefore, the computers of [EMAIL PROVIDER] are likely to contain stored electron-

ic communications (including retrieved and unretrieved email for [EMAIL PROVIDER] subscribers) and information concerning subscribers and their use of [EMAIL PROVIDER] services, such as account access information, email transaction information, and account application information.

6. In general, an email that is sent to a [EMAIL PROVIDER] subscriber is stored in the subscriber's "mail box" on [EMAIL PROVIDER] servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on [EMAIL PROVIDER] servers indefinitely.

7. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to [EMAIL PROVIDER]'s servers, and then transmitted to its end destination. [EMAIL PROVIDER] often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the [EMAIL PROVIDER] server, the email can remain on the system indefinitely.

8. An [EMAIL PROVIDER] subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by [EMAIL PROVIDER]. [NOTE: Consider consulting the provider's law enforcement guide or contacting the provider to identify other types of stored records or files that may be relevant to the case and available from the provider. If there are such records, specifically describe them in the affidavit and list them in Section I of Attachment B.]

9. Subscribers to [EMAIL PROVIDER] might not store on their home computers copies of the emails stored in their [EMAIL PROVIDER] account. This is particularly true when they access their [EMAIL PROVIDER] account through the web, or if they do not wish to maintain particular emails or files in their residence.

10. In general, email providers like [EMAIL PROVIDER] ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

11. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized,

the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via [EMAIL PROVIDER]’s website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

12. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

13. I anticipate executing this warrant under the Stored Communications Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require [EMAIL PROVIDER] to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

14. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of [EMAIL PROVIDER] there exists evidence of a crime [and contraband or fruits of a crime]. Accordingly, a search warrant is requested.

15. This Court has jurisdiction to issue the requested warrant because it is “a court with jurisdiction over the offense under investigation.” 18 U.S.C. § 2703(a).

16. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR NONDISCLOSURE AND SEALING

17. [IF APPROPRIATE: The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), [EMAIL PROVIDER] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution. [Note: if using this paragraph, include a nondisclosure order with warrant.]]

18. [IF APPROPRIATE: It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.]

Respectfully submitted,

[AGENT NAME]

Special Agent

[AGENCY]

Subscribed and sworn to before me on [date]:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with [EMAIL ACCOUNT] that is stored at premises owned, maintained, controlled, or operated by [EMAIL PROVIDER], a company headquartered at [ADDRESS].

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by [EMAIL PROVIDER]

To the extent that the information described in Attachment A is within the possession, custody, or control of [EMAIL PROVIDER], [EMAIL PROVIDER] is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails stored in the account, including copies of emails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between [EMAIL PROVIDER] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed on the warrant involving [SUSPECT] since [DATE], including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. [Insert specific descriptions of the electronic mail which your probable cause supports seizure and copying of; examples: “the sale of illegal drugs” “a threat to bomb a laboratory,” “communications between John and Mary,” “preparatory steps taken in furtherance of the scheme”. Tailor the list to items that would be helpful to the investigation.]

b. Records relating to who created, used, or communicated with the account.

Appendix J

Sample Consent Form for Computer Search

CONSENT TO SEARCH COMPUTER/ELECTRONIC EQUIPMENT

I, _____, have been asked to give my consent to the search of my computer/electronic equipment. I have also been informed of my right to refuse to consent to such a search.

I hereby authorize _____ and any other person(s) designated by [insert Agency/Department] to conduct at any time a complete search of:

All computer/electronic equipment located at _____. These persons are authorized by me to take from the above location: any computer hardware and storage media, including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/electronic hardware or software and related manuals; any other electronic storage devices, including but not limited to, personal digital assistants, cellular telephones, and electronic pagers; and any other media or materials necessary to assist in accessing the stored electronic data.

The following electronic devices:

[Description of computers, data storage devices, cellular telephone, or other devices (makes, models, and serial numbers, if available)]

I certify that I own, possess, control, and/or have a right of access to these devices and all information found in them. I understand that any contraband or evidence on these devices may be used against me in a court of law.

I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize [insert Agency/Department] to make and keep a copy of any information stored on these devices. I understand that any copy made by [insert Agency/Department] will become the property

of [insert Agency/Department] and that I will have no privacy or possessory interest in the copy.

This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form; it has been read to me; and I understand it. I understand the _____ language and have been able to communicate with the agents/officers.

I understand that I may withdraw my consent at any time. I may also ask for a receipt for all things turned over.

Signed: _____ Signature of Witnesses: _____

Date and Time: _____ Date and Time: _____