

**INVESTIGATIVE GUIDE FOR OBTAINING
ELECTRONIC EVIDENCE FROM THE UNITED STATES**

*Preface and
Acknowledgements*

The purpose of this guidance is to provide foreign investigators and prosecutors with a tool for understanding the laws relating to the collection and disclosure of electronic evidence within the U.S. This guidance is intended as assistance, not authority. The analysis and conclusions herein reflect current thinking on difficult and dynamic areas of the law; as such, they may not represent the most current official position of the Department of Justice or any other agency.¹

This guidance is a product of the Criminal Division of the United States Department of Justice and is a joint effort of the Computer Crime & Intellectual Property Section (“CCIPS”) and the Office of International Affairs (“OIA”).

¹ This guidance has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive.

1. Overview of Electronic Evidence in the United States

There are two basic categories of electronic evidence that are routinely requested by law enforcement: (1) **stored information** (e.g., subscriber information, previously sent emails or voicemails and records of when an individual logged into her account) and (2) **real-time communications** (e.g., information gathered while the communication is still occurring). The U.S. legal framework classifies records based upon how sensitive they are in terms of the account holder's privacy. Generally, the more invasive of the individual's privacy, the greater the legal burden on the government to secure those records. Obtaining basic subscriber information (account holder's name and address), for example, is generally less invasive than obtaining the content of an undelivered email message, and therefore the legal burden needed to secure subscriber information is less onerous than that needed to secure undelivered email content. Likewise, obtaining stored information is considered less invasive than capturing communications in real-time. When electronic evidence is sought, investigators and prosecutors must consider the various classifications set out below in Section 4 and provide the necessary predicate information, depending upon the data sought.

PRACTICAL TIP – Ask only for what is really needed; the more that is sought, the longer it may take to obtain, and the higher the standard of proof a U.S. court may require to obtain it. If it turns out that additional information is needed, another request can be made.

2. Emergency Situations

In emergency situations, U.S. law allows law enforcement to engage in certain investigative activities without securing prior court approval. This applies to emergency situations in either the U.S. or abroad, and the information can often be provided without a formal request. Examples of such emergencies might include a kidnapping case where the kidnapper is communicating with the victim's family using an email account; a terrorism case where the terrorist is using an email account to plan an imminent attack; or an ongoing denial of service attack (DOS) against a hospital's internal computer servers, interfering with ongoing patient care.

In emergency situations, law enforcement authorities from the U.S. or foreign countries may seek disclosure of information from an Internet service provider (herein "ISP") without prior court approval. (Note: This is an "extraordinary" request and can be used only in true emergencies.) The ISP may voluntarily provide any of the three types of data related to stored information discussed below (i.e., subscriber information, transactional information, and content). Note, however, that the emergency disclosure authority only allows the content of communications to be disclosed to a U.S. law enforcement agency. In order to use this emergency procedure, the law requires that the ISP satisfy itself that:

- i) there is an emergency involving "immediate danger of death or serious physical injury to any person" (hypothetical possibilities of danger will not meet this test); and
- ii) this danger requires disclosure of the information without delay.

Keep in mind, however, that compliance by providers is not mandatory. If the ISP refuses to “voluntarily” produce the requested data, there is still the option of using legal process to require the disclosure.

3. Preliminary Issues

a. Data Retention/Preservation

In non-emergency situations, the first step in any investigation involving electronic evidence is to preserve the evidence before it is permanently deleted. Time is of the essence. Once deleted, these messages generally can never be retrieved from an ISP. Most ISPs routinely and permanently delete transactional records from their servers; there is no law in the U.S. requiring maintenance or destruction of this data. ISPs often delete this data within days or weeks after the communication was sent. Requests for electronic communications records older than six months will rarely produce positive results.

This is a simple procedure. Some ISPs will accept requests for preservation directly from foreign law enforcement authorities. Because this is voluntary practice by the ISPs, however, the procedures and practices regarding foreign preservation requests vary; countries are encouraged to verify directly with the ISP in question. In other cases, your country’s representative of the 24/7 Hi-Tech Crime Network (described below) can transmit the request. Be prepared to provide the very basic facts of the investigation and the specific account/Internet Protocol (IP) address/website that is to be preserved, as well as all associated dates and times (including time zones used). If additional guidance is necessary, or if your country is not a member of the 24/7 network, help can be obtained by contacting a number of sources, including U.S. law enforcement attachés located at the U.S. Embassy in your country or the U.S. Department of Justice (CCIPS or OIA).

Most ISPs will maintain data for 90 days once a preservation request is received, and it can be renewed for an additional 90 days upon written request. Regardless of the method chosen, as soon as preservation has been requested, the requesting country should begin pursuing one of the methods available for obtaining disclosure of the data (for example, through informal law enforcement to law enforcement information sharing as part of a bilateral or parallel U.S. investigation, or the filing of an official request, including a request made pursuant to a Mutual Legal Assistance Treaty (MLAT)). The reference number provided by the ISP at the time of preservation, or date and time preservation was sought, should be included in the subsequent request for disclosure of the data.

i. 24/7 Hi-Tech Network (Points of Contact)

A group of more than 60 countries has designated high-tech investigative units devoted to handling computer related crimes on a 24-hour, 7-days a week basis. If your country is a member of the 24/7 Network, your country representative will work directly with the U.S.’s official Network contact to preserve the electronic evidence with minimal delay.

b. Special Considerations

i. Notice to subscribers

When a preservation request is submitted, there is a possibility that the account holder may learn of the inquiry, either because of the provider's technical design built into their servers or because the provider makes a notification, as Twitter may. Under U.S. law, there is no legal prohibition on this. Generally, however, the execution of a preservation request will not be apparent to customers of the larger, more well-known ISPs.

ii. Is the ISP reputable?

When making preservation or production requests to ISPs, keep in mind that not all ISPs are reputable. Significantly, there is no licensing requirement of ISPs in the U.S., and there is very little regulation of the ISP industry. There are occasions, for example, when an ISP is actually run by a criminal enterprise, in which case a preservation request could alert the person being investigated. Therefore, before making a request directly to an unknown ISP, consider contacting U.S. authorities to seek guidance on whether the provider is a known and reputable provider.

iii. Foreign affiliates of U.S. ISPs

In some cases, U.S.-based ISPs have established affiliate companies in other countries. In such cases, assuming there is no impediment under domestic law, and where consistent with any applicable international agreements, the foreign affiliate of a U.S. ISP may be able to directly provide some forms of assistance described in this guidance to foreign law enforcement authorities, without the need for a formal request to the United States. Since ISPs operate under different organizational, legal and policy structures, and since those policies and practices may change over time, ISP foreign affiliates should be consulted directly on this point.

c. The United States' Process for Reviewing and Executing International Requests

Following preservation, the foreign MLAT request should be made promptly. When a foreign request for assistance is received, an OIA attorney reviews the request to determine whether it is sufficient under applicable treaties and laws, and, if so, how best to execute the request. If all or part of the request is deemed insufficient, OIA may seek further information from the requesting country before a final decision on execution is reached.

d. Special Considerations in Terrorism Cases

Special factors may be taken into consideration when obtaining electronic evidence in terrorism-related investigations. In these cases, it is imperative to coordinate closely with OIA and the U.S. law enforcement attachés located at the U.S. Embassy in your country before submitting a request; such consultation will assist in the expeditious and appropriate handling of your request.

4. Stored Information – Three Types

There are three types of stored information available from ISPs that may be helpful to an investigation:

*a. **Subscriber Information** – Lowest Level of Process*

What is it?

Subscriber information is information that describes who a person is (*e.g.*, the name and address of the subscriber), and includes basic information about the person's use of an online service (ISP) on a specific date and time (for example, times of logging into the account, how long the subscriber has used that specific service, etc.).

Legal Standard

In order to obtain subscriber information, you need only establish that the evidence sought is relevant and related to the criminal investigation. It is not enough to show that the accused had an email account; the account must have something to do with the crime being investigated. This is the lowest legal standard required of all investigative processes.

Examples where subscriber information may be important

Hypothetical #1 (child exploitation)

Victoria, aged 12 years, receives an email including attached photographs of children engaged in sexual acts from a suspected adult using Joe@us-ISP.com. In the email, Joe suggests that they meet at a specified location. Investigator wants to know who is registered to the email account (and therefore does not need the content of the email account).

Hypothetical #2 (extortion)

ABC Corporation receives an email in which the sender threatens to release sensitive information about ABC's clients if he does not receive \$100,000. Sender provides a link to a password-protected website containing sensitive information about ABC's clients as proof, as well as the password that ABC Corporation will need to view the information and verify the threat. Investigator wants to know who owns the email account, who owns or was assigned the IP address used by the Sender to log into the email account, and who registered the website.

Hypothetical #3 (phishing)

Granny receives an email informing her that she needs to update her account information with her online bank, www.onlinebank.com, by providing personal information. Three days after doing so, all money from her bank account is removed. Granny supplies the original email that she received to Investigator

who determines that the link is not the actual bank's website but rather a third-party's website. Investigator wants to know who set up the website, how they paid for the website, how long the website has been hosted, and where it is hosted.

Type of Subscriber Information Available

The following is the type of subscriber information that should be requested (Note: when requesting information, please provide a specific email address [e.g., Joe@us-ISP.com] or IP address [e.g., IP address 120.128.4.30], or the URL for a web page [e.g., <http://www.onlinebank.com>] as well as the relevant date, time and time zone):

1. The subscriber's account or login name;
2. The subscriber's name and street address;
3. The subscriber's telephone number or numbers;
4. The subscriber's email address;
5. The IP address used by the subscriber to register the account or otherwise initiate service;
6. All IP addresses used by the subscriber to log into the account;
7. Session times, dates and durations; and
8. Any other information pertaining to the identity of the subscriber, including, but not limited to billing information (including type and number of credit cards, student identification number, or other identifying information).

PRACTICAL TIP – Because IP addresses frequently change, it is important to always include the precise time -- up to the second, if available -- as well as the time zone (e.g., Greenwich Mean Time or “GMT”) when asking for IP address information.

PRACTICAL TIP – Be sure to explain how the time frame of the records sought (*i.e.*, the beginning and end dates/times) relates to the investigation. Even though obtaining subscriber information requires the lowest legal standard, law enforcement authorities still need to justify why the evidence sought is relevant to the investigation.

b. Transactional Information – Medium Level of Process

What is it?

Transactional records include records identifying with whom a subscriber communicated, what websites a subscriber visited, and similar information about a user's online activity.

Legal Standard

In order to obtain most types of transactional information, you must provide specific facts detailing how the records or other information sought are relevant and material to a criminal investigation. This is because U.S. law requires prosecutors to provide the court with a factual summary of the investigation and how the records requested will advance that investigation.

This is an intermediate standard, higher than mere relevance, but not as high a legal burden as “probable cause,” as discussed below in (c).

Examples where transactional information may be useful or important

Hypothetical #1 (child exploitation)

In the case where 12-year-old Victoria was asked to travel to meet “Joe,” Investigator wants to identify other minors who may have been victimized. Investigator seeks the email addresses used to communicate with “Joe’s” email account.

Hypothetical #2 (extortion)

In the case where ABC Corporation received the extortion email, Investigator wants to know if the sender of the extortionate email is working with others. Investigator now seeks a log of the email addresses to which that account has sent or from which it has received emails.

Hypothetical #3 (phishing)

In the case where Granny’s bank account was stolen by a phisher, Investigator wants to know if other potential victims received the phishing email. Investigator now seeks a log of all other email addresses to which the phishing email was sent.

Types of Transactional Information Available

When making a request for transactional information and providing a specific email address or the URL of a web page, this is the kind of information to request:

For Email or Web Hosting Accounts:

- Connection information for other systems to which user connected via the email account (or into the web host account) including:
 - a. Connection destination or source of connection, including source port;
 - b. Connection time (within seconds, if possible), time zone, and date;
 - c. Disconnect time (within seconds, if possible), time zone, and date;
 - d. Method of connection to system (*e.g.*, telnet, ftp, http);
 - e. Data transfer volume (*e.g.*, bytes); and
 - f. Any other relevant routing information;
- Source or destination of any electronic mail messages sent from or received by the account (known as the header of the email or the “To” and “From” fields), and the date, time, and length of the message;
- Information pertaining to any image(s) or other documents uploaded to the account (or the website), including the dates and times of uploading, and the sizes of the files but not including the contents of such files; and
- Name and other identifying details of individuals that accessed a specific image/file/web page within a specified period of time, on a specified date.

c. **Content** - *Highest Level of Process*

What is it?

Content is the information sent in an email from the sender to the recipient, which could include written messages, embedded photographs or images, and attached files.

Legal Standard

In order to obtain content in most cases, you must provide information in the formal request that satisfies two legal standards: (1) “probable cause,” and (2) that the facts supporting the request are current.

“Probable cause”: the request must provide specific facts supporting the belief that the evidence (content) sought will be found among the records of the ISP, and that the evidence relates to a crime. This is the same standard that applies to the search of a house or a business in the United States. The request must provide sufficient detail describing: (1) the type of content to be seized (*e.g.*, an email communication); and (2) the reason why the content relates to the criminal offense being investigated.

“Current” or “fresh” information is the second requirement for obtaining the content of electronic communications. This means that at least some of the facts upon which the request is based need to be relatively recent, or indicate the likelihood that the evidence will still be located in the place to be searched. Courts will reject a request if the information presented is old or “stale.” While this is somewhat case-specific (and while not a hard and fast rule), facts that are more than 120 – 180 days old, in the context of electronic evidence, are more likely to be considered stale.

If there was a previous preservation request, however, and the requesting country is now seeking production of those preserved records, it may be possible to avoid a staleness problem because preservation makes it much more likely that the records still exist. Additionally, in certain cases, such as those involving child pornography, U.S. courts tend to find what would otherwise be considered older data to still be “fresh.” If there are concerns about staleness problems in a given case, please contact U.S. authorities before filing a request.

Examples where content may be useful or important

Hypothetical #1 (child exploitation)

In the case where 12-year-old Victoria was asked to travel to meet “Joe,” Joe emails the victim stating that a “friend” of his left him a voice mail asking that Victoria and Joe meet him at a specific location one week from today at 3 PM. Investigator wants the content of the communications in “Joe’s” email account in order to see who Joe is working with and whether Joe and his friend have had any discussions about their plans once Victoria arrives.

Hypothetical #2 (extortion)

In the case where ABC Corporation received the extortion email, Investigator has received the transactional records regarding accesses to the suspect website (where clients' information was posted), and it appears that a number of the IP addresses associated with those accesses originated from within ABC's company network in the United States. Investigator believes that this indicates an insider is working with the extortionist. Investigator now wishes to secure the content of all emails in the extortionist's email account in order to identify the insider, and to verify this relationship. Investigator therefore asks ABC Corporation to retrieve and provide copies of all of the content in the employee's email account.

Hypothetical #3 (phishing)

In the case where the money in Granny's bank account was stolen by a phisher, Investigator learns that a week ago the phisher emailed instructions to the bank on where to transfer the funds in Granny's account. Investigator previously requested that the phisher's email account be preserved and now wants the content of all of the messages in the phisher's account to see if others were victimized in a similar manner, as well as to see if other banks were contacted by the phisher with similar requests.

Types of Content Available

For Email or Web Hosting Accounts

- The content of all emails stored in the account, including copies of emails sent from the account.

For Social Networking Accounts

- All communications and messages made or received by the user, including all private messages and pending "Friend" requests.

PRACTICAL TIP: If a requesting country is able to meet the burden for securing content, transactional records, and/or subscriber information can also be secured through this process, since all of these records require legal process with a lower standard than content.

5. Real-Time Collection of Non-Content Information

What is it?

Real-time collection of non-content information refers to obtaining dialing or routing information (*e.g.*, data that identifies who is sending an email) while the communication is still en route to its destination. (Note: this mechanism will also yield the initial log-in IP address.) This information will not include the content of the email, any attachments that may accompany it, or the subject line.

Legal Standard

In order to obtain non-content information in real-time on behalf of a foreign request, U.S. law enforcement are required to demonstrate specific facts detailing how the records or other information sought are relevant and material to a criminal investigation. In other words, explain how the information requested relates to the investigation for which it is sought. Once a court issues its order, U.S. law enforcement may collect this information in real-time for up to 60 days, and renew this request for another 60 days if needed (and approved by the court). This information may be provided to foreign law enforcement promptly.

Hypothetical where real-time non-content information may be useful

Investigator anticipates that Suspect will be sending an email from a particular Yahoo! account in the next day or two containing a ransom demand. Investigator seeks real-time information about the origin of the email (*i.e.*, the IP address by which the sender accesses Yahoo!) in order to determine the physical location of the Suspect and, ideally, to apprehend the Suspect.

PRACTICAL TIP: This technique is especially useful when targets move around from computer to computer, such as through cyber-café's. An investigator who has the IP address the suspect used and the time when it was used may be able to identify the location of the individual.

6. Real-Time Collection of Content Information

U.S. legal practice precludes prospective real-time collection of content solely on behalf of foreign governments. The United States may share real-time collection of content only if collected in a U.S. investigation.

7. Limitations on Assistance

The United States might postpone assistance in response to a foreign request if execution of the request would interfere with an ongoing U.S. criminal investigation or prosecution. In that situation, the United States might delay execution, or, alternatively, might impose conditions that, if accepted by the foreign country, would protect the integrity of the U.S. case.

Additionally, the United States may have to deny assistance to the extent that execution of the request is contrary to the public interest of the United States. For example, if the conduct at issue is an activity that would be protected under the U.S. Constitution, a request for assistance may be declined. Specifically, the United States may deny a request for assistance if it relates to an individual engaging in expression (written, spoken or other) that falls under the U.S. Constitution's protection of free expression (*e.g.*, "hate" speech is generally protected by the Constitution, even though objectionable), unless facts are provided that indicate the expression goes beyond permissible, protected speech (*e.g.*, hate speech that includes calls for immediate, violent action). Because not all expression is protected by the U.S. Constitution, please consult with U.S. authorities to verify whether or not assistance can be offered in a particular case.

Finally, U.S. authorities generally prioritize foreign requests to those involving serious criminality. As a practical matter, foreign authorities are asked to limit the extent to which they request assistance in cases in which a minor infraction is involved.