



AOL LLC

Public Safety & Criminal Investigations

22000 AOL Way

Dulles, VA 20166

Law Enforcement Manual

(703) 265-COPS (2677)

Or

(703) 265-1933

Fax: (703) 265-2305



Please Direct Legal Process for Any of AOL's Brands to:

In the United States:

AOL LLC Legal Department
Public Safety & Criminal Investigations
22000 AOL Way
Dulles, VA 20166

Attn: Custodian of Records

703-265-1933

703-265-2305 (fax)

650-937-2305 (fax) (California State & Local Agencies Only)

In Canada:

AOL Canada Inc.
55 St. Clair Avenue West
7th Floor
Toronto, ON M4V 2Y7

Attn: Karen Sorbara

416-960-6616

416-960-6560 (fax)

AOL's International Portals

AOL has portals in 19 countries, and plans to launch portals in several more over the course of 2008 and 2009.

North America



[U.S.A.](#)
www.aol.com



[Canada](#)
www.aol.ca



[Mexico](#)
www.aol.com.mx

Europe



[Austria](#)
www.aol.at



[Belgium](#)
www.aol.be



[France](#)
www.aol.fr



[Germany](#)
www.aol.de



[Italy](#)
www.aol.it



[The Netherlands](#)
www.aol.nl



[Poland](#)
www.aol.pl



[Spain](#)
www.aol.es



[Sweden](#)
www.aol.se



[Switzerland](#)
www.aol.ch



[UK](#)
www.aol.co.uk

Asia Pacific



[Australia](#)
www.aol.com.au



[India](#)
www.aol.in



[Hong Kong](#)
www.aol.hk



[New Zealand](#)
www.aol.com.au



[Taiwan](#)
www.aol.tw

AOL Email Domains

Some of the international portals offer email addresses to subscribers that share the same name space as AOL.com. Others offer Country Specific Name Space identifiers that are (as the name implies) unique to that international portal.

AOL's My eAddress feature also permits subscribers to create email addresses in any one of our "affinity" domains, including (for example) switched.com or moviefan.com, or in a unique domain name of the subscriber's choice. For a complete list, see:

domains.aol.com

All AOL email, whether from U.S. or international subscribers, is stored in and processed through AOL's email servers in its data centers in Northern Virginia.

Sample Subpoena Language

18 U.S.C. § 2703(c)(2)

Searches by Name or Screen Name:

The broadest possible language will *not* be workable for persons with relatively common names, since a firstname lastname combination could yield dozens or hundreds of different AOL account holders, and many if not most of those accounts would identify persons entirely unrelated to the investigation.

At least one additional parameter, such as a physical address, telephone number, or credit card number & type, must be included for AOL to locate the screen name.

For the account of (firstname) (lastname) using AOL and/or AIM screen name (screen name) , and for any other screen names associated with this account, and for all other accounts and screen names associated with (firstname) (lastname) , residing at (complete physical address or other additional identifying data) , the following records maintained by AOL LLC (“AOL”) for each account:

All subscriber information, including:

- a. names, email addresses, and screen names;
- b. addresses;
- c. detailed billing records or records of session times and durations;
- d. length of service (including start date) and types of service utilized;
- e. telephone or instrument number or other subscriber number or identity, including most recent temporarily assigned network address [or, alternatively, you may specify a particular date, time, and time zone]; and
- f. the means and source of payment for such service (including any credit card or bank account number).

Searches by IP Address:

If you have only an IP address that appears to be an AOL Member IP or “IPT,” or an AOL Proxy IP (see explanation on page 13, “Types of IP Addresses Logged by AOL”), and you need subscriber information for the corresponding screen name, in place of the first paragraph above you must include the following instead:

IP Address: _____

Exact Date: _____

Exact Time: _____

Time Zone: _____

(Proxy IPs Only) **Complete** headers of the email message sent during the proxy session; or
The **entire** URL of the Web page visited, including **all** fields after .com, .org, .net, etc.:

Disk Subpoena Format Requirements

For any subpoenas with more than 10 screen names

Do's

- Save it on the following media: **two** (2) CD-Roms
- Save the file as a plain text file
- Include *only* the list of screen names
- Include only *one* screen name per line
- Single-spaced lines
- List all screen names on the subpoena (or on an attachment incorporated by reference)
- Provide contact information (name, phone number, and mailing address, but *not* a Post Office box) to which AOL's response should be delivered (Do not include this on this disk)

Do Not's

- Put spaces between characters in screen names
- Include @aol.com or any other domain name after a screen name
- Include screen names containing extraneous characters such as -, *, #, + (screen names can only be alphanumeric)
- Include a letter or copy of the subpoena on the disk
- Include screen names that begin with a number (AOL screen names never begin with a number)
- Number the list

This is how the information on your disk should appear:

John388Doe
JaneDoe388
Johndoe388

Please mail both CDs, and a copy of the subpoena to:

AOL LLC Legal Department
Public Safety & Criminal Investigations
22000 AOL Way
Dulles, VA 20166

If we have provided you with an AOL Legal file #, please include it with your subpoena.

AOL Legal File # _____ - _____ - _____

*The screen names used in the above example are fictitious.

Sample Search Warrant Language

18 U.S.C. § 2703(a)

ATTACHMENT A

Provide the following information as printouts, or on compact disc or DVD:

For the account of _____ (firstname) (lastname) _____ at _____ (physical address, if known) using AOL and/or AIM screen name _____ (screen name) _____ ,

[*add, if there is probable cause:*]

“and for any other screen names associated with this account,”

[*add, if there is probable cause:*]

“and for all other accounts and screen names associated with _____ (firstname) (lastname) _____ ,”

the following records maintained by AOL LLC (“AOL”) for each account:

1. All subscriber information, including:
 - a. names, email addresses, and screen names;
 - b. addresses;
 - c. detailed billing records or records of session times and durations;
 - d. length of service (including start date) and types of service utilized;
 - e. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
 - f. the means and source of payment for such service (including any credit card or bank account number).

2. For the period of _____ (date) _____ to the date this warrant is acted upon by AOL, all transactional information, including:
 - a. logs of Internet Protocol (“IP”) address connections, including dates, times, and time zones, and any ANI information made available to AOL;
 - b. address books;
 - c. buddy lists; and
 - d. account history, including contacts with AOL support services and records of actions taken online by the subscriber or by AOL support staff in connection with the service.

3. For the period of _____ (date) _____ to the date this warrant is acted upon by AOL, the contents of electronic or wire communications held in accounts of the persons assigned the screen names identified in paragraph 1, including:
 - a. all electronic or wire communications (including e-mail text, attachments, and embedded files) in electronic storage by AOL, or held by AOL as a remote computing service, within the meaning of the Stored Communications Act;
 - b. all photos, files, data, or information in whatever form and by whatever means they have been created or stored
[*if probable causes exists, include Xdrive:*
“including files maintained in an Xdrive account”]; and
 - c. all World-Wide Web profiles or homepages.

Serving Search Warrants in the United States

State or Local Agencies

Except as noted below, when the search warrant calls for producing AOL email or other content (see paragraph 3 of the Sample Search Warrant Language), state or local agencies must domesticate warrants through Loudoun County, Virginia, so that they may be issued by the Loudoun County Circuit Court.

Please contact the Loudoun County Sheriff's Office at (703) 777-0493 for details. Sheriff's Investigator Ron Colantonio is currently assigned to process these search warrants.

Search warrants that do not call for producing content, but only subscriber information or transactional records (see paragraphs 1 and 2 of the Sample Search Warrant Language), may be faxed directly to AOL's Legal Department at (703) 265-2305.

California

Pursuant to California Penal Code § 1524.2, AOL accepts California search warrants by fax to (650) 937-2305.

Florida

Pursuant to Florida Statute § 92.605, AOL accepts Florida search warrants by fax to (703) 265-2305.

Minnesota

Pursuant to Minnesota Statute § 626.18, AOL accepts Minnesota search warrants by fax to (703) 265-2305.

State of Washington

Pursuant to 2008 Washington Advance Legislative Service 21, AOL accepts Washington search warrants by fax to (703) 265-2305.

New York

New York search warrants may be faxed to (703) 265-2305.

Federal

Federal search warrants may be faxed to (703) 265-2305.

Sample Preservation Request
18 U.S.C. § 2703(f)

(Your Agency Letterhead)
(Date)

Via Facsimile to 703-265-2305

AOL LLC Legal Department
Public Safety & Criminal Investigations
22000 AOL Way
Dulles, VA 20166

Re: Preservation Request

Dear Custodian of Records:

I am writing to request the preservation of records for the following account, pending the issuance of legal process:

Name: John X. Doe
Address: 1234 Any Street, Anytown, USA 12345
Telephone: (123) 456-7890

Screen Names: John388Doe, JaneDoe388, JohnDoe388
AOL Account #: _____
Credit Card # & Type: _____

{ *or* }

IP Address: _____
Exact Date: _____
Exact Time: _____
Time Zone: _____

(Proxy IPs Only) **Complete** headers of the email message sent during the proxy session; or
The **entire** URL of the Web page visited, including **all** fields after .com, .org, .net, etc.:

You are requested to preserve, for a period of 90 days, the records described below currently in your possession for this account. You are also requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request.

{ *continued on next page* }

Sample Preservation Request
18 U.S.C. § 2703(f)
(cont'd)

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 preservation request applies to the following records:

{ *See Sample Search Warrant for Comprehensive List* }

If you have any questions concerning this request, please contact me at _____.

Signature
Printed Name / Date

Preservation Requests for IP Connection Logs

The above letter may be used to request preservation of IP connection logs for specific accounts across a range of dates, or to pinpoint an IP address on a specific date, time, and time zone, or to preserve the last known IP login on a given account as of the specific date of the preservation request.

A court order issued under 18 U.S.C. § 2703(d) is required to compel disclosure of a range of IP connection logs.

Emergency Voluntary Disclosures

18 U.S.C. § 2702(b)(8)

18 U.S.C. § 2702(c)(4)

The Stored Communications Act permits an Internet service provider to disclose the contents of electronic or wire communications or customer records to law enforcement "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or records] relating to the emergency."

In the event of an emergency, please telephone AOL's Public Safety and Criminal Investigations unit at 703-265-1933, and provide us with specific facts concerning the emergency that you believe requires immediate disclosure of communications or records relating to the emergency.

The specific facts should include:

- Description of the emergency, including facts demonstrating the danger of death or serious physical injury;
- Explanation that the danger is imminent, and that a subpoena, court order, or search warrant cannot be obtained in time; and
- What specific records or communications you seek from AOL that relate to the emergency.

Types of IP Addresses Logged by AOL

Source IP (or "Login IP")

The Source IP is the IP address assigned by an AOL dialup provider or the subscriber's broadband ISP upon initiating a connection to the Internet.

What Whois Shows:

When a Whois query is performed on a Source IP, typically it will show that it has been allocated to an Internet service provider that is *not* AOL.

In addition to any subscriber information available from AOL, a subpoena served on the AOL dialup provider or the subscriber's broadband ISP may reveal identifying information.

Member IP (or "IPT")

When a subscriber actually logs into AOL's service, the member IP or "IPT" is the IP address assigned by AOL that enables the subscriber to navigate throughout AOL's online content.

When a subscriber logs into AOL and navigates on the World Wide Web *without* using the built-in Web browser within the AOL client software, the Web servers logging the subscriber's IP address will show the IPT assigned by AOL.

When a WHOIS query is performed on an IPT, the hostname always ends in **ipt.aol.com**.

Proxy IP

When a subscriber uses AOL's built-in Web browser to navigate the World Wide Web (outside of AOL's online content), the subscriber's Web traffic passes through an AOL proxy server. Therefore, the Websites visited by the subscriber can detect (and log) only the proxy server's IP address. Proxy servers are used to implement AOL's Parental Controls and to speed up Web surfing for subscribers.

When a WHOIS query is performed on a proxy IP, the hostname always ends in **proxy.aol.com**.

Web servers logging visits by AOL subscribers in those circumstances will show the proxy IP assigned to the server – not the Member IP ("IPT") assigned to the individual subscriber. Many AOL subscribers are assigned the same proxy IP at the same time.

Therefore, AOL **cannot** search for a unique Screen Name assigned to a given proxy IP unless law enforcement provides **one** of the following, in addition to the exact date, time, and timezone the proxy IP address was logged:

- **Complete** headers of the email message sent during a proxy session; or
- The **entire** URL of the Web page visited during the proxy session, including all fields to the right of .com, .net, .org, etc.

Understanding AOL IP Connection Logs

```
START 46483bf 2007-05-14 06:37:45EDT 1058 69.228.44.5 123456789 John388Doe
START 46483bf 2007-05-14 06:37:45EDT 1058 69.228.44.5 123456789 John388Doe
FINISH 46483bf 2007-05-14 07:09:08EDT
START 4648d8eb 2007-05-14 17:47:23EDT 1058 69.228.44.5 123456789 JaneDoe388
FINISH 4648d8eb 2007-05-14 17:47:57EDT
START 4648d9 2007-05-14 17:48:32EDT 1058 69.228.44.5 123456789 John388Doe
FINISH 4648d9 2007-05-14 17:50:20EDT
START 4648de 2007-05-14 18:12:03EDT 1058 69.228.44.5 123456789 John388Doe
START 4648de 2007-05-14 18:12:03EDT 1058 69.228.44.5 123456789 John388Doe
FINISH 4648de 2007-05-14 18:47:40EDT
START 464905c9 2007-05-14 20:58:49EDT 1058 69.228.44.5 123456789 JaneDoe388
FINISH 464905c9 2007-05-14 20:59:59EDT
```

This example illustrates the following:

1. There may be duplicate START or FINISH lines representing the same session.
2. Dates, times, and time zones are always included in the logs.
3. To avoid confusion, look for START and FINISH times for a given session with the same hexadecimal number (in the above example, each of the lines that includes 46483bf represents the same session).
4. The number 123456789 in the above example represents the subscriber's AOL account number.
5. The user in this example was not assigned a specific AOL IP address (often but not always beginning with "172") – therefore, the only IP address written to the logs is the user's source IP address, 69.228.44.5. This is typical of connection logs generated by a subscriber with broadband (as opposed to dialup) Internet service.

Note:

IP connection logs for WebMail sessions (on either AOL.com or AIM.com) do **not** include "Finish" or "Logout" times.

Internet and AOL Email Headers

An excellent guide to interpreting Internet email headers is found in the following manual:

Best Practices for Seizing Electronic Evidence, Version 2.0

Federal Law Enforcement Training Center

<http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/downloads/other/>

See "Tracing an Internet Email," on pages 22-23 of the Best Practices guide.

When AOL users send email to one another, however, the headers are reduced to a bare minimum, since email need not be routed through multiple email servers scattered across the globe. Below is the entire set of headers in email sent from secure@aol.com to guilt@aol.com :

AOL to AOL e-mail:

Subject: Hello World

Date: 1/30/2008 3:44:11 P.M. Eastern Standard Time

From: [secure](mailto:secure@aol.com)

To: [guilt](mailto:guilt@aol.com)

Sent on: AOL Webmail 34032-STANDARD sub 0

MapQuest Searches

Search Parameters:

MapQuest searches are labor-intensive and time-consuming. Accordingly, please narrow your requests as much as possible. A request for all data concerning a particular MapQuest search over a 3 to 5 day period is reasonable; a request for data over an entire month (for example) may be unreasonable.

Search terms may include:

- Exact address, e.g., 1234 Any Street, Anytown, USA 12345; or
- Exact intersection, e.g., Any Street & Main Street, Anytown, USA 12345; or
- In the event IP data is your starting point, the

IP Address: _____

Exact Date: _____

Exact Time: _____

Time Zone: _____

used to undertake the search.

Retention Period:

MapQuest search data is retained for approximately 45 days.

ICQ Searches

Search Parameters:

ICQ, an Instant Messaging service popular outside the United States, is based on a numerical UIN (Universal Identification Number). Registration and profile information is user-generated and user-configurable. Email addresses associated with an ICQ UIN, like those used to register for free AOL or AIM.com accounts, are unverified.

ICQ usage generates IP connection logs which are retained for up to 90 days.

AOL Email Retention Periods

AOL E-Mail

(Paid Services, including those converted to free accounts)

- Inbox - Kept as New: Indefinite
- Inbox - Unread: 30 days
- Read: 30 days from the date it is read
- Sent: 30 days
- Deleted: 24 hours
- Spam - Unread: 5 days
- Spam - Read: 1 day

These retention periods are not guaranteed since each mailbox is also subject to a numerical quota (1,000 messages for the Inbox, 550 for all others), which when exceeded results in the deletion of the oldest messages beyond the quota.

- “Saved on AOL”:
Indefinite (with no numerical quota)

AIM.com / My eAddress (“Affinity”) Domains / International Portals

(Free Services)

- Inbox – All read, unread, kept as new: Indefinite
- Sent: Indefinite
- Trash: 7 days
- Spam (Unread): 5 days
- Spam (Read): 1 day
- “Saved Mail” (including any top-level, user-created folders): Indefinite

120 days without “logging in” will result in all e-mail being deleted from the free account. There are no numerical quotas for these accounts.

With the release of the AOL 9.1 client, AOL subscribers have the option to convert their email to the AIM.com retention periods (i.e., indefinite except for Trash and Spam).

Subscribers who use AOL WebMail can also convert their email to the AIM.com retention periods (i.e., indefinite except for Trash and Spam), by selecting “Switch to improved unified inbox” within the General Settings options.

Compuserve2000 E-Mail

- Inbox - Kept as New: 27 days (from deposit)
- Inbox - Unread: 27 days (from deposit)
- Read: 3 to 7 days after it is read, or 27 days from deposit (whichever is less)
- Sent: 27 days
- Deleted: 24 hours

AOL Log Data Retention Periods

Session logs ("Detailed billing")	6 months
Source IP & Member IP ("IPT") connection logs	90 days
Webmail IP connection logs	90 days
Proxy IP connection logs	5 to 7 days
AIM IP connection logs	up to 90 days
ICQ IP connection logs	up to 90 days

All AOL log data retention periods are approximate and subject to change without notice.