



America Online

Compliance & Investigations

22000 AOL Way
Dulles, VA 20166

Law Enforcement Training Manual

(703) 265-COPS (2677)

Or

(703) 265-1933

Fax: (703) 265-2305



Contact Information

AOL United States – See cover sheet for contact info

AOL Canada Inc.

Diane Singer
55 St. Clair Avenue West
7th Floor
Toronto, ON M4V 2Y7
416-960-6540
416-960-6560 (fax)

CompuServe

CompuServe
Custodian of Records
22000 AOL Way
Dulles, VA 20166
(703) 265-1933
(703) 265-2305 Fax

ICQ

Custodian of Records
22000 AOL Way
Dulles, VA 20166
703-265-1933
703-265-2305 (fax)

Netscape

Frances Soto
501 E. Middlefield Rd., Bldg.5
Mountain View, CA 94043
650-937-5898
650-937-5544 (fax)

Current AOL Retention Periods

- Basic Subscriber Information: 6 months (including log on/off times)
- Unread and Sent Mail: 28 Days
- Read Mail: 2 days
- Member Internet Protocol (IP) Addresses: 60 - 90 days
- Proxy Server IP: up to 7 days max (Sometimes 1 or 2 days)
- IP connection Log Data: approx. 90 days (specific date and time required)
- ICQ
 - UIN Required for search
 - Can not search on real name
 - Can not search on nicknames as they are not unique
- AIM
 - IP Connection Log Data: 14 days (specific date and time required)

* All retention periods are approximate and can vary depending on system usage.

Sample Subpoena Wording

Any and all AOL and/or AIM records regarding the identification of "XYZ" to include real name, screen names, status of account, detailed billing logs, date account opened and closed, method of payment and detailed billing records (log on & log off times).

Sample Search Warrant Wording

Any and all AOL and/or AIM accounts for XYZ or screen name "xyz", to include all email, histories, buddy lists, profiles, subscriber information, method of payment, detailed billings records (log on & log off times)..

- ❖ If you are a state or local agency, your warrant must be served through Loudoun County, VA. Please contact Eddie Fant 703-777-0493.(US Law Enforcement Only, for AOL Canada please contact Dianne Singer @ 416-960-6540)
- ❖ California Search Warrants requesting AOL e-mail content must be faxed to Frances Soto at Netscape (650) 937-4366.
- ❖ Federal Search Warrants can be faxed directly AOL Legal. Our fax # is (703) 265-2305.

Sample Preservation Request Letter

(Your Department Letterhead)

Custodian of Records
America Online, Inc.
22000 AOL Way
Dulles, Virginia 20166
ATTN: Compliance and Investigation Unit
Fax: (703)265-2305
Re: Preservation Request

Dear Custodian of Records:

The below listed account is the subject of an ongoing criminal investigation at this agency, and it is requested that said account and all e-mail, and any other information contained herein, be preserved pending the issuance of a search warrant. (Specify any information you may want, i.e. unread, read, sent email, account histories, buddy lists, profiles, detailed billing (log on and log off times) payment method, etc...)

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

Screen Names: Johndoe, JohnXYDoe, XYZDoe
Possible AOL Account #: _____
Credit Card #: _____

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

(Your Signature)
(Your Name Typed)

❖ If you are a state or local agency, your warrant must be served through Loudoun County, VA. Please contact Inv. Eddie Fant at 703-777-0493.

Sample IP Preservation Request Letter

(Your Department Letterhead)

Custodian of Records
America Online, Inc.
22000 AOL Way
Dulles, Virginia 20166
ATTN: Compliance and Investigation Unit
Fax: (703) 265-2305
Re: Preservation Request

Dear Custodian of Records:

The below listed IP address (addresses are) is the subject of an ongoing criminal investigation at this agency, and it is requested that **subscriber information** pertaining to the identity of the member who used the below listed IP address (addresses) at the below listed time be preserved pending the issuance of a subpoena.

IP #:
Date:
Time:
Time Zone:
URL (where applicable):

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

Signature/Printed Name

- ❖ **Specific DATE, TIME and TIME Zone required on all IP lookups.**
- ❖ When doing a search on a Proxy IP address, the URL and or the email are required.
- ❖ Whenever possible, please include the following:
 - ❖ URL
 - ❖ Header Information and copy of email
 - ❖ Copy of Message board posting

Information required for IP address requests (via a subpoena etc.)

Subpoena should be made out to:

Custodian of Records
America Online, Inc.
22000 AOL Way
Dulles, Virginia 20166
ATTN: Compliance and Investigation Unit
Fax: (703)265-2305

Retention Periods for IP addresses.

- Member Internet Protocol (IP) Addresses: Approximately 90 days
- Proxy Server IP: up to 7 days max (sometimes 1 or 2 days)

You **MUST** include the following information in reference to the IP address usage:

IP Address

Date

Time

Time Zone - of where the servers are that captured the IP address (this information is sometimes contained in the timestamp of an email)

Most IP lookups can not be processed without the following information:

If the information you have came from an email, please include a copy of the email, including, and most importantly, **the header information**.

If the information you have came from a website, please include the exact URL (web address) of the *purchase page* (not just the main web address).

Please consult the following website to see if an IP address is assigned to AOL.

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

If you have any further questions, please contact our Law Enforcement Help-Line @ 703-265-COPS.

Sample IP Connection Log Data Preservation

(Your Department Letterhead)

Custodian of Records
America Online, Inc.
22000 AOL Way
Dulles, Virginia 20166
ATTN: Compliance and Investigation Unit
Fax: (703)265-2305
Re: IP Connection Log Data Preservation

Dear Custodian of Records:

The below listed account is the subject of an ongoing criminal investigation at this agency, and it is requested that the IP connection log data be preserved pending the issuance of a court order or search warrant. Please specify whether this is in reference to an AOL or AOL Instant Messenger account.

Screen Names: Johndoe, JohnXYDoe, XYZDoe
Date: (Required) 03/22/01
Time: (Required) 16:35:12
Time Zone: (Required) EST

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

(Your Signature)
(Your Name Typed)

- *Please note that AOL IP connection Log Data is only available for 90 days.
- *Please note that AOL Instant Messenger (AIM) IP connection Log Data is only available for 14 days.
- *Please note that once this information is preserved, a Subpoena, Court Order or Search Warrant is necessary for the release of the information.

Information required for requests on IP Connection Log Data for a screen name on a Subpoena, Court order or Search Warrant

Please provide subscriber information and IP Connection Log Data for the following AOL or AOL Instant Messenger Account (Please specify weather it is AOL or AIM)

<u>Required Information</u>	<u>Examples</u>
Screen Names:	Johndoe388
Date:	03/22/01
Time:	16:35:12
Time Zone:	EST

*If you do not know the date/time/time zone, you can request the most recent login.

*Please note that AOL IP connection Log Data is only available for 60 - 90 days.

*Please note that AOL Instant Messenger (AIM) IP connection Log Data is only available for 14 days.

Sample Consent Wording

(Your Agency Letterhead)

I, "XYZ", being duly sworn, do hereby state the following:

I am the primary account holder of America Online account bearing the screen names "XYZ".

I understand that the "ABC" agency is conducting an official criminal investigation and has requested that I grant my consent to authorize the "ABC" agency to receive, review, copy and otherwise utilize, as they deem appropriate, all information of any kind held by America Online, Inc. relative to my AOL account and any alternate screen names or subaccounts.

I hereby authorize AOL to provide to any agent of the above referenced agency, any and all records relating to my AOL account, including: Basic Subscriber Information, Payment Information, Log on and Log Off Times, Buddy List Information and All Email Content. (Please list each type of information you are requesting.)

Pursuant to this Authority to Release, I do hereby agree to hold harmless and do forever hold harmless America Online for the disclosure of such information and do forever waive on my behalf and on behalf of all my heirs or assigns, any and all claims arising, in whole or in part, as a result of AOL's disclosure of information related to my account(s) pursuant to this authorization.

I do hereby indemnify America Online against any claims or cause of actions arising in whole or in part, out of AOL's disclosure of information related to my account(s) pursuant to this authorization.

Members Signature & Printed Name

Date

Witness Signature & Printed Name

Date

AOL Compliance and Investigation Unit Disk Subpoena Format Requirements

For any subpoenas with more than 10 screen names

1. Plain text file. (save file as text only)
2. List of screen names only.
3. No spaces between characters of screen name.
4. One screen name per line.
5. No extraneous characters (screen names can only be alpha-numeric)
6. Single-spaced lines.
7. Please do not include the file name, a letter or a copy of the subpoena on the disk.
8. Do not number the list.
9. Please note that our screen names can not begin with a number.
10. Disk formats: 3 ½" floppy, CD-Rom, Zip (100 MB)

Below is an example of how the information on your disk should appear:

John388Doe
JaneDoe388
Johndoe388
DoeJane397
Doejohn398

Please mail disk and copy of subpoena to:

America Online
Compliance and Investigation Unit
Attn: Jennifer Sheridan
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 # _____ - _____ - _____ (if applicable)

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

WHOIS Lookups

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

<http://www.arin.net/whois/arinwhois.html>

<http://www.ripe.net/db/whois.html> (Europe)

<http://www.apnic.net/apnic-bin/whois.pl> (Asia Pacific)

<http://www.nsiregistry.com/>

<http://www.registrars.com/static/whois/index.shtml>

<http://www.nic.mil/dodnic/>

Tracing an Internet Email

- When an internet e-mail message is sent, the user **typically** controls only the receipt line(s) (To: and Bcc:) and the Subject: line.
- Mail software adds the rest of the header information as it is processed.

Reading an email header:

Sample Email Header

- - - - Message header follows - - - -

(1)	Return-path: <ambottom@in50210.cc.nps.navy.mil>
(2)	Received: from in50210.cc.nps.navy.mil by nps.navy.mil (4.1/SMI-4.1) id AA08680; Thur, 7 Nov 96 17:51:49 PST
(3)	Received: from localhost by in 50210.cc.nps.navy.mil (4.1/SMI-4.1) id AA16514; Thur, 7 Nov 96 17:50:53 PST
(4)	Message-Id: <9611080150.AA16514@in50210.cc.nps.navy.mil>
(5)	Date: Thur, 7 Nov 1996 17:50:53 -0800 (PST)
(6)	From : "Albert M. Bottoms" <ambottomin50210.cc.nps.navy.mil>
(7)	To: Tim White <ti.white@\$m.ir.lo.COM>
(8)	Cc: Real 3D <real3dQmmc.com, Denny Adams <dadams@idsa.com, Tim Arion <tarion@aol.com>, RAY BALCERAK <RBALCERAK@AR'A.mll>

- **Line (1)** tells other computers who really sent the message, and where to send error messages (bounces and warnings).
- **Lines (2) and (3)** show the route the message took from sending to delivery.
 - ◆ Each computer that receives this message adds a Received: field with its complete address and time stamp; this helps in tracking delivery problems.
- **Line (4)** is the Message-ID, a unique identifier for this specific message. This ID is logged and can be traced through computers on the message route if there is a need to track the mail.
- **Line (5)** shows the date, time, and time zone when the message was sent.
- **Line (6)** tells the name and e-mail address of the message originator (the "sender").
- **Line (7)** shows the name and e-mail address of the primary recipient; the address may be for a:
 - ◆ Mailing list,
 - ◆ System-wide alias,
 - ◆ A personal username.
- **Line (8)** lists the names and e-mail addresses of the "courtesy copy" recipients of the message. There may be "Bcc:" recipients as well; these "blind carbon copy" recipients get copies of the message, but their names and addresses are not visible in the headers.

Understanding AOL IP Log Information

Top line shows:

Login Date/ Time (Eastern)/ SoftwareVersion/ Orig. IP/ AOL Acct Number/ Screen Name/ Normal-Remote Status

Bottom line shows:

Logout Date/ Time (Eastern)/ IPT/ AOL IPT/ AOL Acct. Number/ Screen name/ Duration of Online Session

Example:

Login Date	Login Time	Version	Originating IP	AOL Acct. No.	Screen Name	Norm-Rem. Status
2/25/01	05:42:00	0519	206.115.154.248	098765123	JOHNDoe	NO-R00
2/25/01	08:01:00	IPT	172.132.192.238	098765123	JOHNDoe	02:19:00
Logout Date	Logout Time	IPT	AOL IPT	AOL Acct. No.	Screen Name	Online Duration

