

Facebook Law Enforcement Guidelines

This guide describes the procedure for requesting data from Facebook, Inc. and its corporate affiliates ("Facebook") along with the types of data available.

This guide is **CONFIDENTIAL** and contains Facebook proprietary information. This guide cannot be redistributed without the express written permission of Facebook. It is intended for law enforcement use only and is not intended to create any enforceable rights against Facebook.

Facebook is continuously changing and reserves the right to change any of the policies described below without notice. However, Facebook will do its best to inform law enforcement of any significant changes in the policies and/or procedures in this Guide or by other means.

If this guide is more than 6 months old, please contact Facebook at subpoena@facebook.com for any updates.

Table of Contents

FACEBOOK LAW ENFORCEMENT GUIDELINES	1
ACCEPTABLE USE POLICY	3
NON-CONTENT AND CONTENT DATA	3
HOW TO LOCATE THE UNIQUE FACEBOOK I.D. NUMBER.....	3
HOW TO SUBMIT A REQUEST	4
DESCRIPTION OF AVAILABLE DATA	6
<i>User Basic Subscriber Information (BSI)</i>	6
<i>User Neoprint</i>	6
<i>User Photoprint</i>	7
<i>Group Contact Info</i>	7
<i>Private Messages</i>	7
<i>IP Logs</i>	7
EMERGENCY DISCLOSURES	8
USER CONSENT	8
INTERNATIONAL REQUESTS	8
SPECIAL REQUESTS	9
FACEBOOK EMERGENCY DISCLOSURE FORM	10
SAMPLE FACEBOOK USER CONSENT LETTER	11

Acceptable Use Policy

Privacy and Integrity are cornerstones of the Facebook application and company philosophy. Our privacy settings allow an individual to control access to their data on the site. We actively monitor the site for accounts that try and circumvent our privacy features, either by technical means or by providing false profile information. In accordance with our terms of service (see <http://www.facebook.com/terms.php>), we will disable any and all accounts, **including accounts that may belong to law enforcement**, which supply false or misleading profile information and/or attempt to technically or socially circumvent our privacy measures.

Non-Content and Content Data

Facebook is bound by federal laws, including the Electronic Communication Privacy Act, Title 18 U.S.C. § 2701, et seq. (ECPA).

Generally, a **subpoena** will provide you **non-content** related data. Non-content data is the basic subscriber information (described below) of the Facebook profile. Depending on the availability, the remaining data is considered content and is subjected strictly to ECPA. Generally, a court order under §2703(d) will provide limited content, for example, messages over 180 days, and a **search warrant** will provide you with the remaining content. Further description of the available data is found below.

How to locate the unique Facebook I.D. Number

In general, data retrieval is based upon a Facebook user ID or group ID and/or the associated user name or group name. When the Facebook ID and associated name are not available, an e-mail address(s) associated with the account is often the most useful information for locating an account.

While Facebook may accept requests without these types of information, the additional time required to identify a particular user account will delay response substantially. In some cases, we may not correctly identify an account without additional information. We may purge data as part of our normal operations before we are able to identify a particular user or group if a user ID or group ID and associated name are not provided.

Facebook IDs are intrinsic in our URLs. If you have a subject's profile page URL, you can find the ID by looking for the string "id" in the URL and passing along the number immediately following.

For instance, the user ID for the following profile is “29445421”:

<http://www.facebook.com/profile.php?id=29445421>***

Group IDs follow a similar pattern, but the string to look for is “gid”. The group ID of the following URL is 2204894392:

<http://www.facebook.com/group.php?gid=2204894392>

***Please note that our product continuously changes with new features. In 2009, we launched “**vanity URLs**”. Instead of a UID in the URL, a user may have a unique “vanity name” to identify him/herself. Providing the vanity name will also help identify the Facebook profile.

How to submit a request

Please contact our Security Department at subpoena@facebook.com to inform us that a request may be coming, this is especially important if you are interested in a specific IP log(s) and wish to preserve the account.

Requests may be faxed to +1 (650) 644-3229, sent via e-mail to subpoena@facebook.com OR mailed to:

Facebook, Inc.
Attn: Security Department/Custodian of Records
1601 S. California Avenue
Palo Alto, CA 94304
U.S.A.

In order to help assist us in identifying the requesting agency and the Facebook profile(s) of interest, please provide the following:

1. Your contact information:

The following contact information is required for every request:

- Requesting Agency Name
- Requesting Individual (RI)
- RI Employer-Issued E-mail Address***
- RI Phone Contact, including the extension
- RI Mailing Address (P.O. Box will not be accepted)
- Response Due Date (Please allow at least 2 – 4 weeks for processing)

***Most of our communication is processed via e-mail. In addition, if permissible, the returned data is also sent via e-mail. You will receive a case number upon

receipt of an e-mail and/or data. Please always include the case number in any future correspondence.

2. Facebook User Information:

Please have as much of the following information as possible available, in order to enable us to identify the proper accounts. Facebook user IDs are preferred.

- Facebook User ID/Group ID/Vanity URL
- User's Full name
- Full URL to Facebook profile
- School/Networks
- Date of Birth
- All known e-mail address(s)
- All known phone number(s)
- Full address
- Period of activity (specific information and date(s) of interest may expedite your request)

Note Regarding Disabling Account: Pursuant to its terms of use, Facebook will disable an account if the account is in violation of said terms. If disabling or restricting user access to the user's profile will jeopardize your current investigation, you must clearly specify **"DO NOT DISABLE UNTIL XX/XX/XXXX"** on all requests submitted to Facebook. If permitted, a further description of the investigation is also requested.

Facebook generally returns data via e-mail, however if the volume of returned data is larger than a few megabytes, Facebook will respond via read only media (CDrom or DVDrom). Responses will be in PDF or text formats.

Facebook reserves the right to charge reasonable fees, where permissible, to cover our costs in replying to user data requests.

Preservation of Records

Pending the issuance of your legal document (i.e. subpoena, search warrant), Facebook will preserve information in accordance with 18 U.S.C. § 2703(f) but will not produce data until a valid legal request is received. Information required for Preservation Requests are described as above, and may be submitted by fax, mail, or e-mailed.

Please note that Facebook will preserve information for 90 days, however based on the necessity for the case in question, an extension can be made.

Description of available data

User Basic Subscriber Information (BSI)

BSI is the basic information of a given user profile. It may include the following, depending on the availability at the time of processing your request:

- User Identification Number
- E-mail address
- Date and Time Stamp of account creation date displayed in GMT
- Most Recent Logins (generally captures the last 2-3 days of logs prior to processing the request) in GMT
- Registered Mobile Number
- Verification on whether publicly viewable

BSI is delivered in XML format.

User Neoprint

The Neoprint is an expanded view of a given user profile. A request should specify that they are requesting a "Neoprint of user ID XXXXXX"

The Neoprint may contain the following elements:

- Profile Contact Information
- Mini-Feed
- Status Update History
- Shares
- Notes
- Wall Postings
- Friend Listing, with Friends Facebook ID's
- Groups Listing, with Facebook Group ID's
- Future and Past Events
- Video Listing, with filename

If a profile is changed or updated, deleted content is not retained, and cannot be produced. Any messages deleted by the user are not retained and cannot be produced. Wall postings deleted by the user may not be retained and may not be produced.

Neoprints are delivered in PDF format.

User Photoprint

The Photoprint is a compilation of all photos uploaded by the user that have not been deleted, along with all photos uploaded by any user which have the requested user tagged in them. A request should specify that they are requesting a "Photoprint of user ID XXXXXX". Deleted photos are not retained.

Photoprints are delivered in PDF format.

Group Contact Info

Where a group is known, we generally provide the creator BSI and/or administrator BSI. We will also provide a PDF of the current status of the group profile page. A request should specify that they are requesting "Contact information for group ID XXXXXX". No historical data is retained.

Group contact info is delivered as a PDF format.

Private Messages

Private Messages are saved based on user discretion, if the user has deleted any messages at any point during their activity, Facebook does not keep records of those messages.

Private messages info is delivered as a PDF format.

IP Logs

The system described in our previous Law Enforcement Guidelines regarding the IP logs data is no longer functional. We now have a limited capacity of retrieving specific logs and are technically limited in providing "everything" within a requested date range. We are unable to testify to the completeness of the data.

Requests for specific log(s) of interest are now required in order to individually extract them from a separate tool. The IP logs contain content and will be subjected accordingly to ECPA.

IP logs can be produced for a given user ID or IP address. A request should specify that they are requesting the "IP log of user ID XXXXXX" or "IP log of IP Address xxx.xxx.xxx.xxx"

The log contains the following information:

- [Column One] **Script** – Script executed. For instance, a profile view of the url “http://www.facebook.com/profile.php?id=29445421” would populate script with “profile.php”
- [Column Two] **Scriptget** – Additional information passed to the script. in the above example, scriptget would contain “id=29445421”
- [Column Three] **Userid** – The Facebook user ID of the account active for the request
- [Column Four] **Viewtime** – Date of execution, in PACIFIC TIME ZONE.
- [Column Five] **IP** – Source IP address

IP Logs are delivered as a tab delimited text file.

All of the above-described data is continuously under major development. Therefore, the data may be retained for a longer or short period and may be produced in one or more files.

Emergency Disclosures

Facebook will provide data pursuant to Title 18 U.S.C. §2702(b)(6)(C) and § 2702 (c)(4) if Facebook believes in good faith that serious bodily harm or death of a person may occur. An Emergency Disclosure Form is provided in the Guidelines and may only be submitted by a law enforcement agent.

E-mail the Emergency Disclosure Form to subpoena@facebook.com and include “**Emergency Request**” in the subject heading. Facebook will respond within 24 hours to true emergency requests.

User Consent

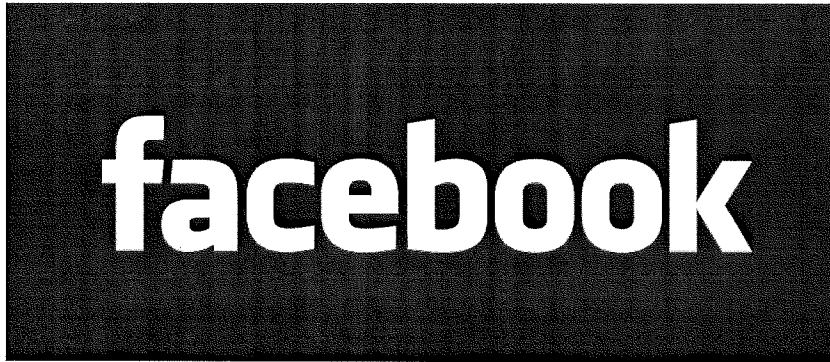
Facebook will provide data pursuant to the voluntary consent of the user (see Title 18 U.S.C. §2702 (b)(3) and § 2702 (c)(2)). A template of a consent letter is provided in the Guidelines. Authentication of the true identity of the user must be provided along with the consent letter. For example, a notarized consent letter will be accepted.

International Requests

Due to the growing popularity of Facebook internationally, we recognize the needs of international Law Enforcement. Please send requests in accordance with our guidelines to subpoena@facebook.com.

Special Requests

The Facebook Security Team may be able to retrieve specific information not addressed in the general categories above. Please contact Facebook if you have a specific investigative need prior to issuing a subpoena or warrant.



EMERGENCY DISCLOSURE FORM

Pursuant to 18 U.S.C. § 2702 (b) (7) and § 2702 (c) and the Facebook privacy policy, Facebook may exercise its discretion in providing relevant data after reviewing the provided information below. Please provide as much information in order to enable the Security team to conduct an appropriate search.

1. Describe the nature of the emergency (i.e. potential bodily harm, crime being committed):

2. Provide the identification of all users involved (Facebook user profile name, ID number and Date of Birth):

3. Provide the exact location(s) of the evidence related to the described emergency:

I, _____, attest that the above-mentioned facts are true and
Printed Name of authorized Officer
accurate to the best of my knowledge.

Signature and Badge #

Date

[SAMPLE]

Consent to Release Private Facebook Information

I, [LEGAL NAME], am an account holder with Facebook, Inc. My account name is [FACEBOOK USERNAME] and my login email address is: _____. I do hereby voluntarily authorize Facebook to release the reasonably available data as check-marked below, from my Facebook account profile for the period of [mm/dd/yyyy to mm/dd/yyyy] or 2 years from present date.

I hereby indemnify Facebook, Inc. against all claims for damages, compensation and/or costs in respect to damage or loss to a third party caused by, or arising out of, or being incidental to release of my data.

My data should be released to:

[CONTACT NAME, PHONE NUMBER, FAX NUMBER, ADDRESS and E-MAIL ADDRESS]

- Profile
- Status Updates
- Notes
- Mini-feed
- Shares
- Wallposts
- Deleted Wallposts
- Old (over 180 days) Wallposts
- Friends List
- Deleted Friends List (deleted by user)
- Groups
- Events
- Videos
- Recent IP Address Logins
- Applications
- Facebook Message Box
- Photos

Affiant's Signature

Date

Notary Public/Individual Duly Authorized to Administer Oath: