

NING, INC. LAW ENFORCEMENT COMPLIANCE GUIDE
04/2009

1. Summary of Services and Description

- Ning, Inc. (“Ning”) is an online service provider that provides a set of technology applications that enable individuals to build their own websites or social networks (“Ning Platform”). Ning is not involved in the decisions relating to content uploaded or published by the creators of these social networks (“Network Creators”) or any of the members of these social networks (“Members”). Additionally, we are not involved in the management of the social networks on the Ning Platform, or in any of the decisions relating to the focus of social networks created on the Ning Platform.
- Ning does not provide any form of internet access or connection for individuals (including Network Creators or Members) that use the Ning Platform.

2. Contact Information at Ning

- **For Law Enforcement Legal Process (subpoena, search warrant, court order, etc.)**

Jon Stueve, Esq.
Director of Legal Affairs
Ning, Inc.
735 Emerson St.
Palo Alto, CA 94301
Email: jstueve@ning.com
Direct Dial: 650-561-7099
Fax: 650-289-0650

We require that any form of legal process be sent both via fax and service via certified mail

- **For NCMEC Reporting**

Erin Mulcrone
Director, Policies and Abuse
Ning, Inc.
735 Emerson St.
Palo Alto, CA 94301
Email: erin@ning.com
Direct Dial: 650-561-7132
Fax: 650-289-0650

3. Legal Process

- **Retention Policy:** To provide law enforcement time to investigate, Ning retains content relating to child pornography for a period of 90 days from the date of Ning’s report via the CyberTipline. Unless a preservation request has been sent by law enforcement, Ning will destroy the content upon expiration of such 90 day period. Ning does not keep log retention files for longer than one year, so if a Member that is discovered to have uploaded child pornography first registered to join the Ning Platform more than a year ago, Ning will no longer have registration IP address information for this Member. When possible, we will provide alternative IP address information that we may have in response to legal process.

- **Ning’s Process:**

1. Upon internal discovery of suspected child pornography on the Ning Platform or when any reports of suspected child pornography are sent to us, we either immediately remove the specific content from that social network, or immediately shut down the entire social network if the social network itself appears to be promoting or otherwise focused on child pornography. At this time, we also disable the account of the Member that uploaded the suspected child pornography and inform the Network Creator and/or Member that we have disabled their account and have reported them to NCMEC.

2. We then report the content to NCMEC via the CyperTipline. We generally report both content that was reported to us as well as additional content we discover after doing our own internal investigation of the entire social network.

3. Upon receipt of legal process, we will promptly gather and produce the information listed below under “***What Information Ning Can Provide to Law Enforcement***”.

If you wish to have any child pornography content mailed in response to your search warrant, please put a direct mandate in your search warrant ordering us to mail the evidence to you. Please note that without a direct mandate under a search warrant to mail the content, we will not do so due to the fact that there is no safe harbor for the transmission of child pornography (even to law enforcement).

If you do not include an order to mail the content in your warrant, we will each need to coordinate with the San Jose, CA ICAC or San Jose, CA FBI office so that they can physically come to our offices to pick-up this content and in turn send this to you.

4. What Ning Can Provide to Law Enforcement

- Ning can provide you with the following information once we receive a subpoena, search warrant or court order (please draft your legal process to specifically include this):

Information Ning Can Provide Pursuant to an 18 U.S.C. §2703(c)(2) Subpoena:

1. **Registration email** of the Network Creator and Members who uploaded the content that we believe is child pornography to the specified social networks*;

2. **Registration IP addresses** of the Network Creators and Members who uploaded the content we believe is child pornography to the specified social networks*;
3. **Usernames** of the Network Creator and Members who uploaded content that we believe is child pornography*; and
4. **Credit Card Information (if any)** of the Network Creator if a Network Creator uploaded suspected child pornography and has purchased premium services (this includes any address provided during the purchase). **Please note that we do not collect any address or telephone information unless a Network Creator purchases premium services using a credit card.**

Additional Information Ning Can Provide Pursuant to an 18 U.S.C. §2703(a) Warrant:

1. All **images and videos** of suspected child pornography on the social network in question*;
2. The **date/time stamped IP addresses** at the time the Member uploaded the content in question;
3. Any and all **messages** sent or received from Network Creators and/or Members (through the Ning Platform) who uploaded the suspected child pornography to the specified Social network, to include READ, UNREAD and SENT MESSAGES. **(Please note that we do not currently keep deleted messages on our servers).** These messages can also be received by a Network Creator or Member to the email address associated with his or her registration email. These messages are sent via email masking.
4. The subject line and date/time stamp of all **automated email notifications** (such as notifications to join a Social network) sent on behalf of the Network Creator or Member by Ning. The content of these automated emails are not kept on our servers.

*(Items marked with an * are provided at the time Ning makes its CyberTipline report if the Member or suspect was reported to NCMEC by Ning)*

AS A REMINDER, FOR IMAGES OR VIDEOS TO BE MAILED IN RESPONSE TO A WARRANT, WE WILL NEED A DIRECT MANDATE IN THE SEARCH WARRANT ORDERING US TO MAIL THE EVIDENCE TO YOU.

5. International Jurisdictions

International law enforcement agencies can obtain the information set forth in “**Information Ning Can Provide Pursuant to an 18 U.S.C. §2703(c)(2) Subpoena**” by providing a properly authorized Regulation of Investigatory Powers Act (“RIPA”) form along with contact information for the person who executes this form. Additionally, Ning can provide the information set forth in “**Additional Information Ning Can Provide Pursuant to an 18 U.S.C. §2703(a) Warrant**” with formal process from the United States or pursuant to the Hague Convention.

Information Ning DOES NOT have Access To:

Ning does not have access to the following types of information. This is information that the Member’s internet service provider is more likely to have.

1. Connection date and time

2. Disconnection date and time
3. Method of connection
4. Data transfer volume
5. Other connection information, such as Internet Protocol address of the source of the connection

6. NCMEC Reporting

- As requested by NCMEC, Ning reports on a per suspect basis – each Member who uploads suspected child pornography to a social network is reported separately. This means that there may be several reports filed on a particular social network.
- Ning provides the following information (in addition to the suspect child pornography content) in a separate document attached to each CyberTipline report:
 1. The name and URL of the social network as well as the total number of all Members.
 2. The username of the Network Creator and whether or not the Network Creator uploaded any suspected child pornography to this social network.
 3. The total number of all images and videos on the social network as well as the number of images and videos that we believe contain suspected child pornography.
 4. The username of the Member that is being reported that uploaded any suspected child pornography. This is the username for the social network in which the Member uploaded the suspected child pornography.
 5. The registration IP address and registration email of the Member that is being reported. This is the registration IP address and registration email at the time the Member joined the Ning Platform.
 6. The total number of all images and videos uploaded by the specific Member of that social network that is being reported as well as the total number of images and videos that we believe contain suspected child pornography.

7. Fulfillment of Legal Process

- **Expected turnaround time:** Ning will generally be able to provide a response within two to three weeks after receipt of legal process requesting the information set forth in “*What Information Ning Can Provide to Law Enforcement*”.