IMVU User Information Request Guidelines
IMVU CONFIDENTIAL
For distribution to and use by law enforcement only

IMVU, Inc. promotes a safe and fun environment where people can meet and interact in 3D. IMVU trusts our users to act in a responsible (and legal) manner; however, should this trust be violated, IMVU is ready and willing to assist law enforcement with any investigations stemming from inappropriate or illegal behavior. This document provides guidance for agencies seeking information on IMVU users, and highlighting the manner as well as documentation (subpoena, search warrant, court-ordered demand, or ID Theft statement) that allows the most efficient response from IMVU.

Available Data

Basic account information provided in response to a subpoena will include an Avatar name, e-mail address, customer ID (all unique), as well as the IP address used to register the account and any device fingerprints on file. The device fingerprint(s) IMVU provides do not actually contain information about the device connected to our service (e.g. MAC address, computer name, etc.), they are merely a fingerprint confirming a specific device was using the IMVU service. Additionally, this fingerprint can be used to positively identify other accounts that used the same device(s) to connect to the IMVU service.

If account communications are requested, IMVU will provide the text of web-based messages and a summary of real-time chats (via IMVU's 3D client) that will include the accounts participating in chats but not the actual text of the chat.

IMVU does not have a policy for the regular purging or removal of account records but communication data may be missing or incomplete after 6 months.

Please note that IMVU does not verify customer data, which creates the possibility that the data produced by IMVU may result in limited data or data that was falsified by the person of interest.

Details of Request

For IMVU to look-up account data we will need either the Avatar name, the e-mail address associated with the account, the account number, or a payment identifier (e.g. credit card #, PayPal transaction #/email address, etc.). In some cases an IP address may be used, but because IMVU primarily tracks the most recent IP address used and because many network providers change IP assignments or use proxies, this is not always reliable.

When requesting the account data, please have the subpoena or search warrant request:

> "Account data for the account(s) matching the Avatar name, e-mail or IP addresses *[insert known data here]* and for any account(s) that appears to be controlled by the same person."

This will allow IMVU to provide a more comprehensive data set without the need for you to request an additional legal documentation (subpoena, search warrant, etc.).

In the legal documentation please be specific if the account should remain enabled. If IMVU becomes aware of an account with suspicious or illegal activity it will likely be disabled. If leaving an account enabled will assist in an investigation, please make sure this is stated when submitting the subpoena, search warrant, or other court-ordered demand.

In the event the account(s) of interest are the result of ID Theft. If the account(s) in question are related to ID Theft, your victim(s) can request information from IMVU without the need of a subpoena or summons. Please have the victim fill out and submit to IMVU the California Office of Information Security and Privacy Protection (form 3A) located at: http://www.privacy.ca.gov/cis3aenglish.htm

Delivery of Legal Documentation

To expedite collection of data, please send a copy of the subpoena, search warrant, court-ordered demand or ID Theft statement via fax.

Fax:

b6

Mail:

IMVU, Inc.

b6

164 Hamilton Ave
Palo Alto, CA 94301