(S//SI//REL) Tracking Targets on Online Social Networks

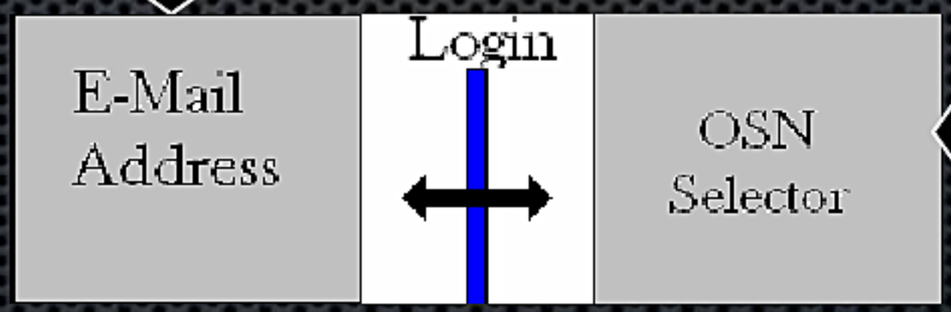
The overall classification of this briefing to TOP SECRET//COMINT//REL TO USA, FVEY

[redacted]
Online Social Networks SME
September 2009

Derived From
NSA/CSSM 1-52
Dated 20070108
Declassify on: 20320108

(U//FOUO) OSN Overview





(S//SI//REL TO USA, FVEY) OSN Selectors are usually invisible to the user and are only used internally.

(U)Fanbox



(TS//SI//REL TO USA, FVEY) Suppose you sign up for Fanbox with the address **terror.bomber@live.com**, and you also sign up for Fanbox email.

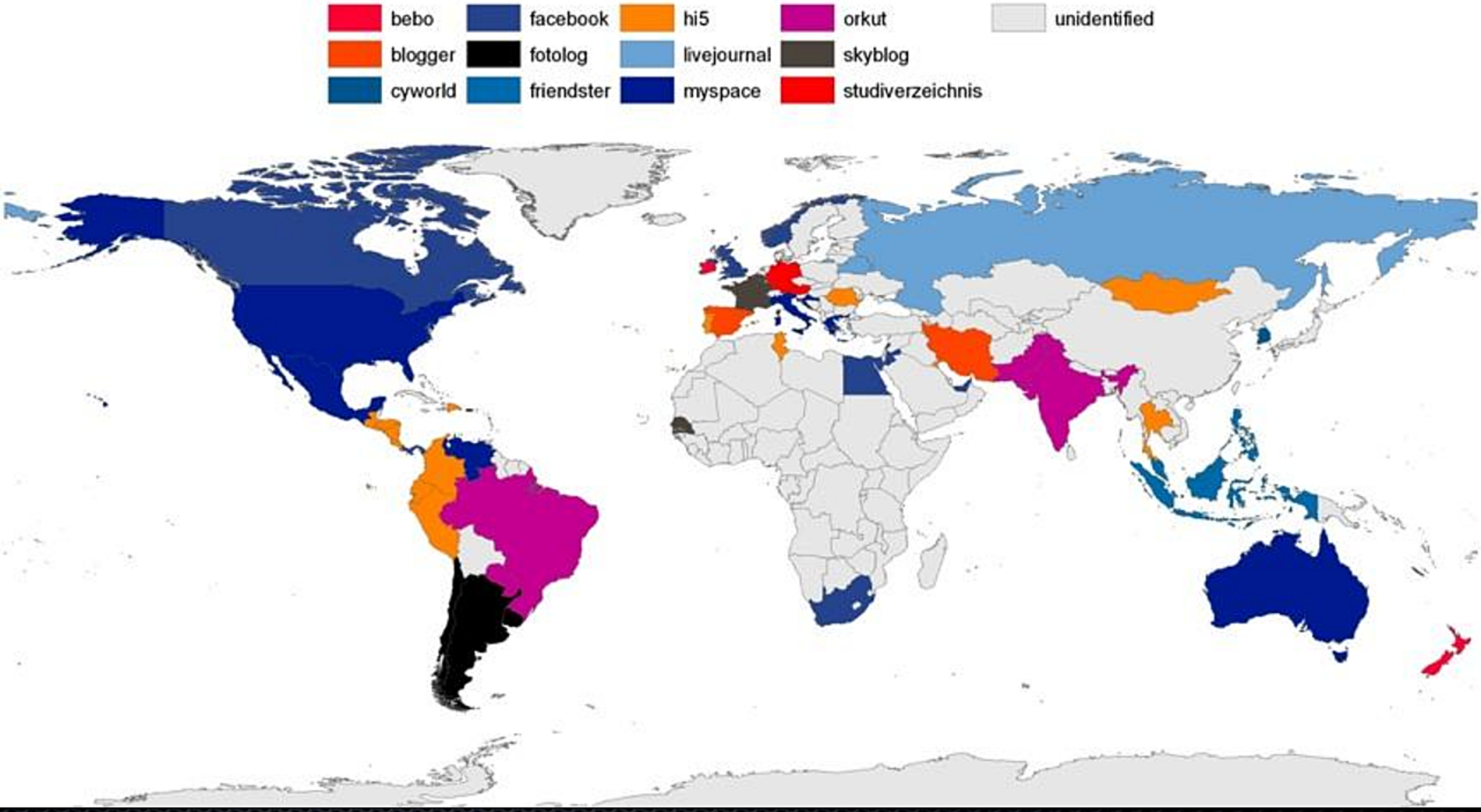
(TS//SI//REL TO USA, FVEY) Here's what your identifiers will look like:

- (TS//SI//REL TO USA, FVEY) Username: terrorbomber378691622
- (TS//SI//REL TO USA, FVEY) UserId: 217440283
- (TS//SI//REL TO USA, FVEY) Email: terrorbomber@fanbox.com (if it's available)
- (TS//SI//REL TO USA, FVEY) Email: terrorbomber18246@fanbox.com (if the above address is already taken)
- (TS//SI//REL TO USA, FVEY) **Note** that if your sign up email address already exists as a Fanbox email address, Fanbox will simply append a few random digits to make it a unique Fanbox email address.

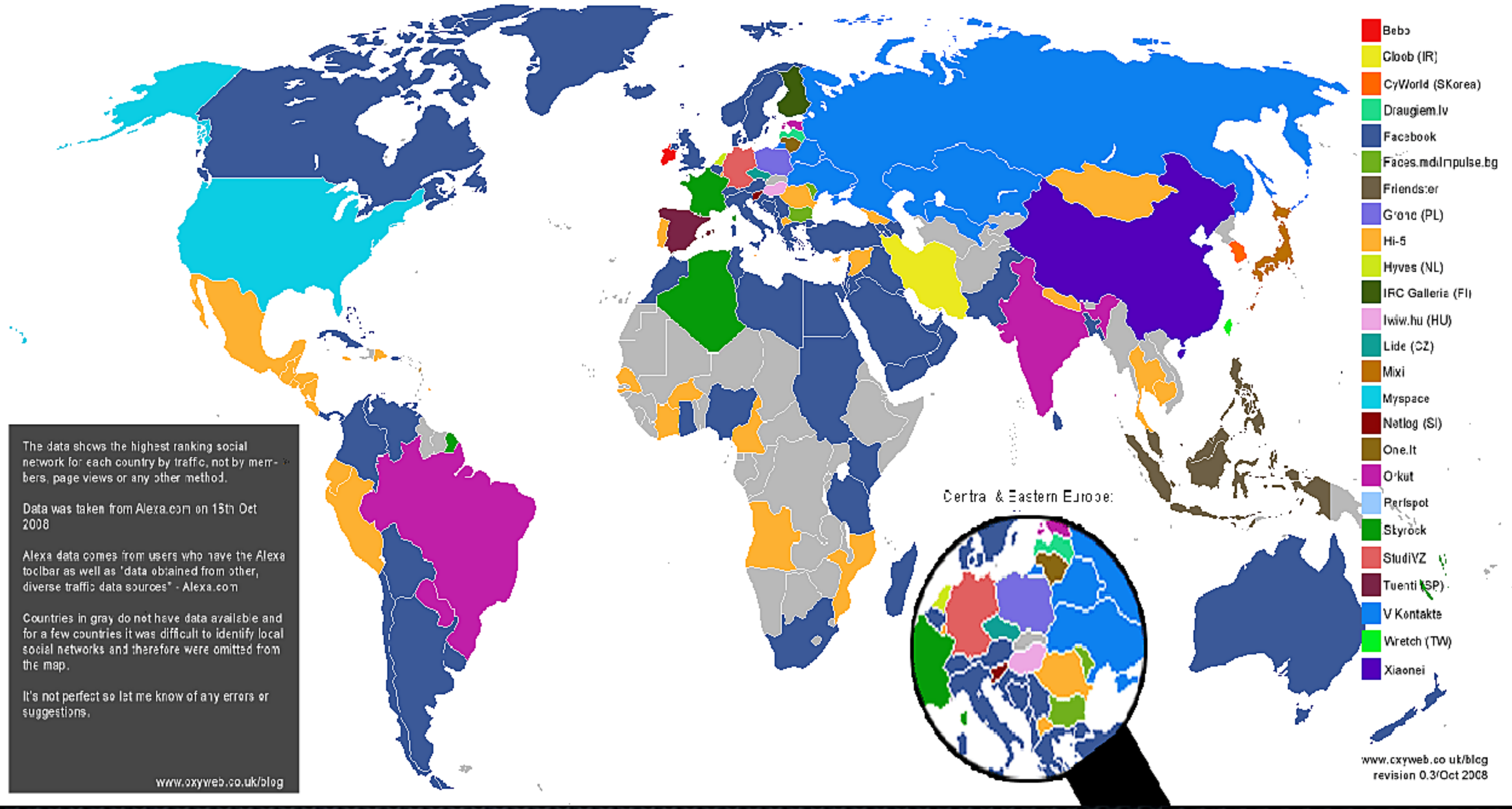
What intelligence do OSN's provide to the IC?

- (S//SI//REL TO USA, FVEY) Insight into the personal lives of targets MAY include:
  - (U) Communications
  - (U) Day to Day activities
  - (U) Contacts and social networks
  - (U) Photographs
  - (U) Videos
  - (U) Personnel information (e.g. Addresses, Phone, Email addresses)
  - (U) Location and Travel Information

(U) Popular Online Social Networks as of 2007



(U)Popular Online Social Networks as of October 2008



MiGente.com
THE POWER OF LATINOS

Buddy Fetch

Collective
groups that work™

twitter

facebook

opensocial

Ning

IRANIAN VIRTUAL SOCIETY
CLOOB.COM

Windows Live Spaces

SKYROCK
Free People Network™

Recruiting Grounds
Gaming Network

Überme
BETA

bebo

orkut
beta

friendfeed

hi5

FanBox

myspace.com
a place for friends

friendster

TAGGED

NETLOG

Google
Friend Connect
BETA

1.5 beta
CYWORLD

腾讯网
qq.com

(TS//SI//REL TO USA, FVEY) CT Targets have been observed using more than 50+ OSNs as of late 2008

(TS//SI//REL TO USA, FVEY) Types of OSN Activity

(TS//SI//REL TO USA, FVEY) Type I: Operational Communication

(TS//SI//REL TO USA, FVEY) Type II: Technological Operational Communication

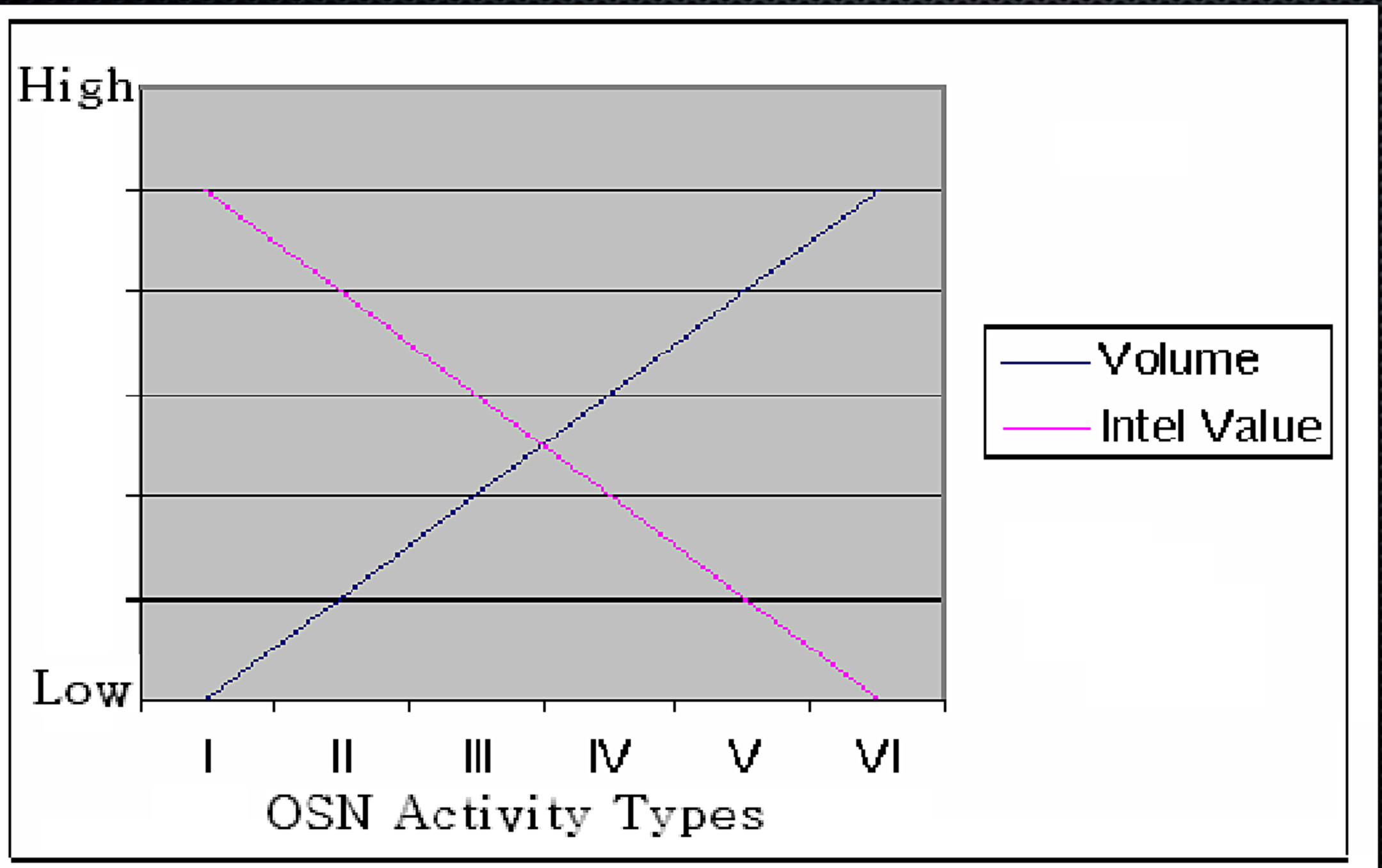
(TS//SI//REL TO USA, FVEY) Type: III: Extremist/ Propaganda OSN Users (Overt)

(TS//SI//REL TO USA, FVEY) Type IV: Direct Non-operational OSN Users

(TS//SI//REL TO USA, FVEY) Type V: Self-Provided Personal Data on OSN

(TS//SI//REL TO USA, FVEY) Type VI: Close Associate Information or Communication ("The Super Sloth Method")

(TS//SI//REL TO USA, FVEY) Types of OSN Activity



(S//SI//REL TO USA, FVEY)
OSN Selectors expand SIGDEV opportunities

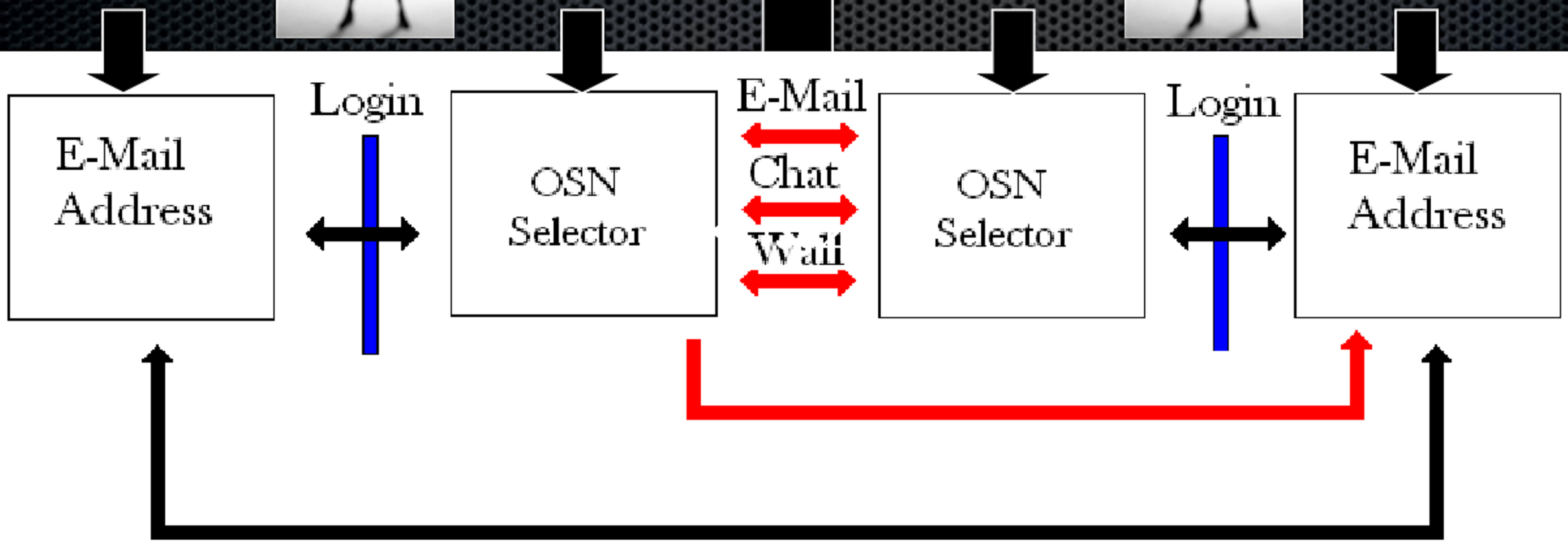


Leverage initial selector seeds to build a better picture of the target's online persona and the selectors involved

(U) OSN Comms Flow







(TS//SI//REL TO USA, FVEY) TWO individuals communicating seamlessly through at least FOUR independent selectors

(TS//SI//REL TO USA, FVEY)
User Activity Possible Queries

User Activity

Datetime: 1 Day | Start: 2009-09-21 00:00 | Stop: 2009-09-22

Search For: username

Search Value: 12345678910

Realm: facebook

Datetime: 1 Day | Start: 2009-09-21 00:00 | Stop: 2009-09-22

Search For: username

Search Value: My_Username

Realm: netlog

(TS//SI//REL TO USA, FVEY) Pros and Cons of User Activity Queries

Pros:

Hard Selector query

Easy to pull/automate

Email Addresses in the Username can lead to new leads

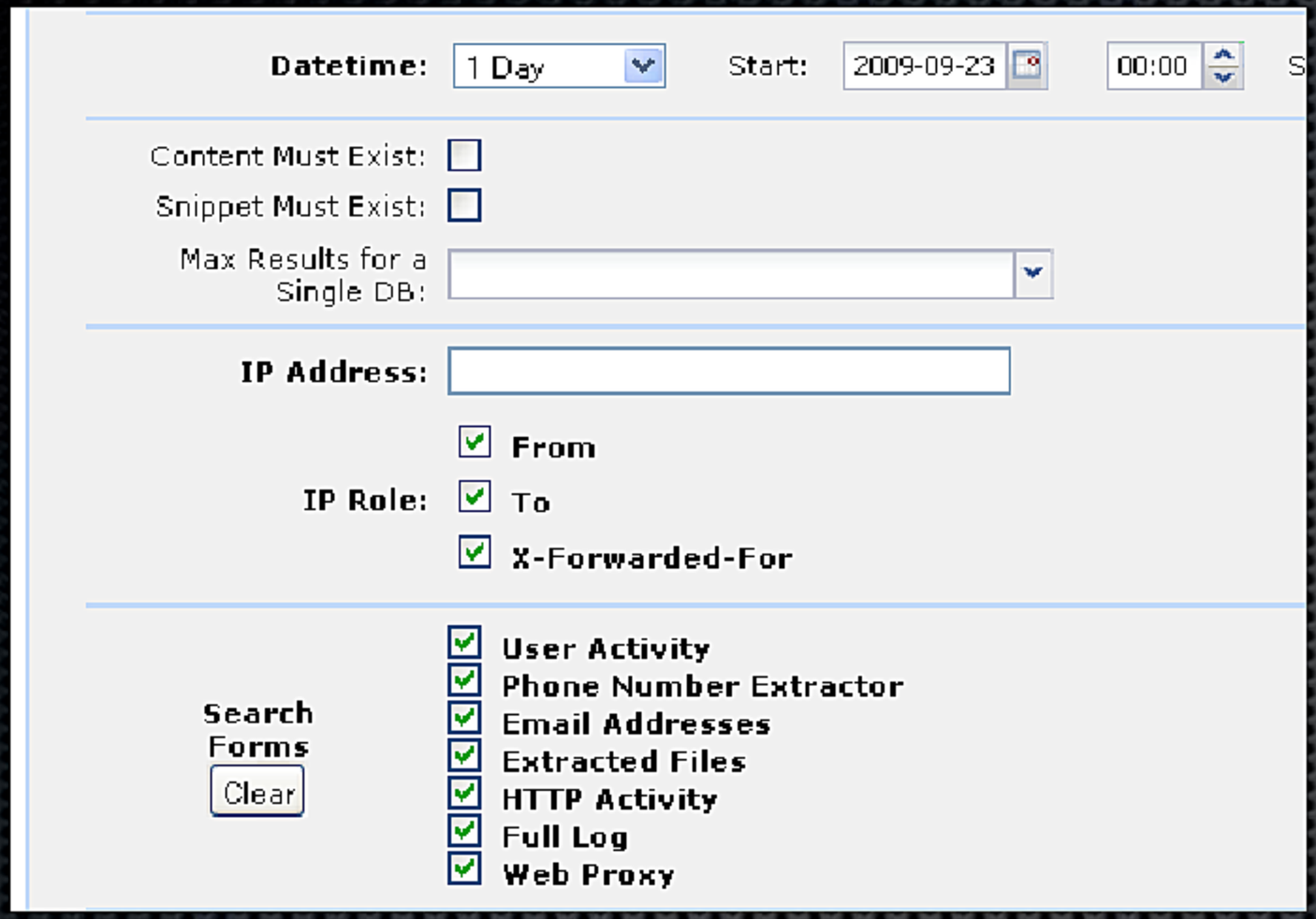
Cons:

Only certain OSN's usernames that can be queried

No content that doesn't have a selector associated with it

No Web-Browsing

(TS//SI//REL TO USA, FVEY)
HTTP Activity and IP Multisearch Queries

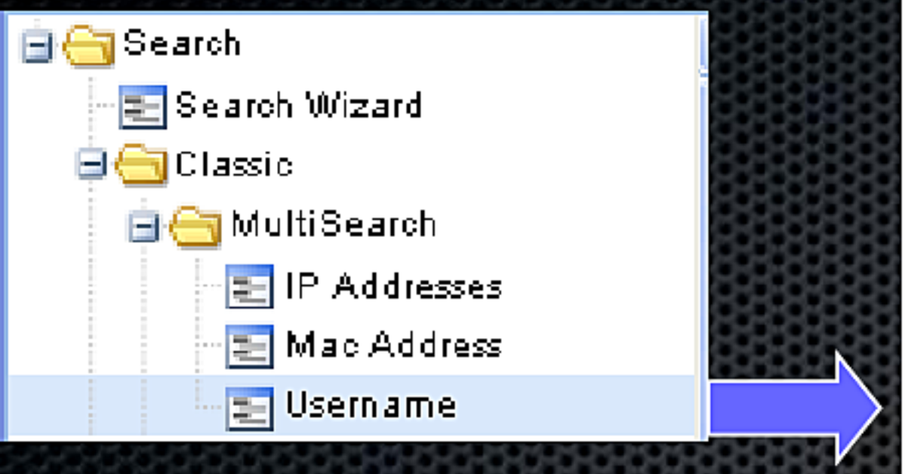


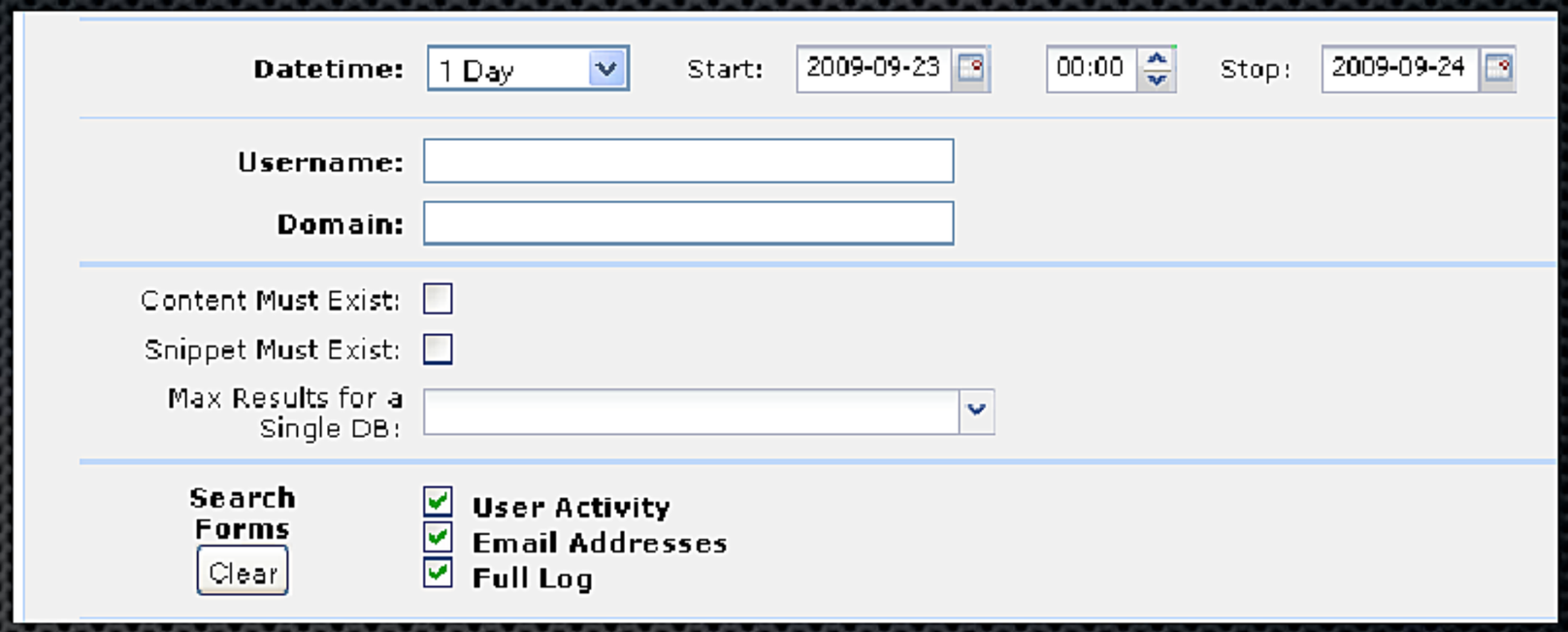


HTTP Activity Queries usually require some other piece of technical information to query while leveraging the OSN appIDs to be legally compliant

- IP Address
- MAC Address

(TS//SI//REL TO USA, FVEY)
Username Queries are preferable

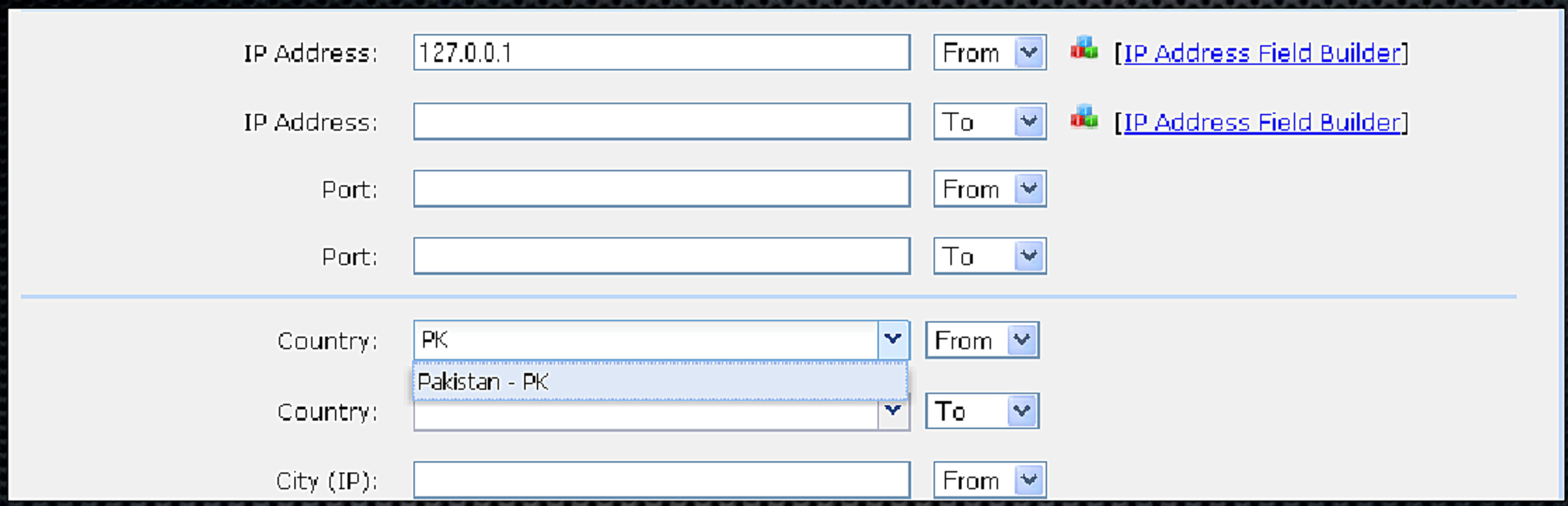




Search For	Search Value	@Domain	Realm	Subject	Attribute Type	Chain	Attribute Value	Activity	Source
username	[redacted]				email_address		[redacted]@yah		bebo
username	[redacted]				email_address		[redacted]@yah		bebo
username	[redacted]				email_address		[redacted]@yah		bebo

- Email address of the user often appears in the "Attribute Value" or other fields when looking at OSNs.

(TS//SI//REL TO USA, FVEY)
HTTP Activity Queries



HTTP Activity Queries usually require some other piece of technical information to query while leveraging the OSN appIDs to be legally compliant

- IP Address
- MAC Address
- Country of Origin

(TS//SI//REL TO USA, FVEY)
Pros and Cons of HTTP Activity Queries

Pros:

OSNs that don't require login are seen

Mobile and other technologies may be seen more easily

Web forms, chat, etc. that may not be collected by normal dictionary selection can be seen and saved off

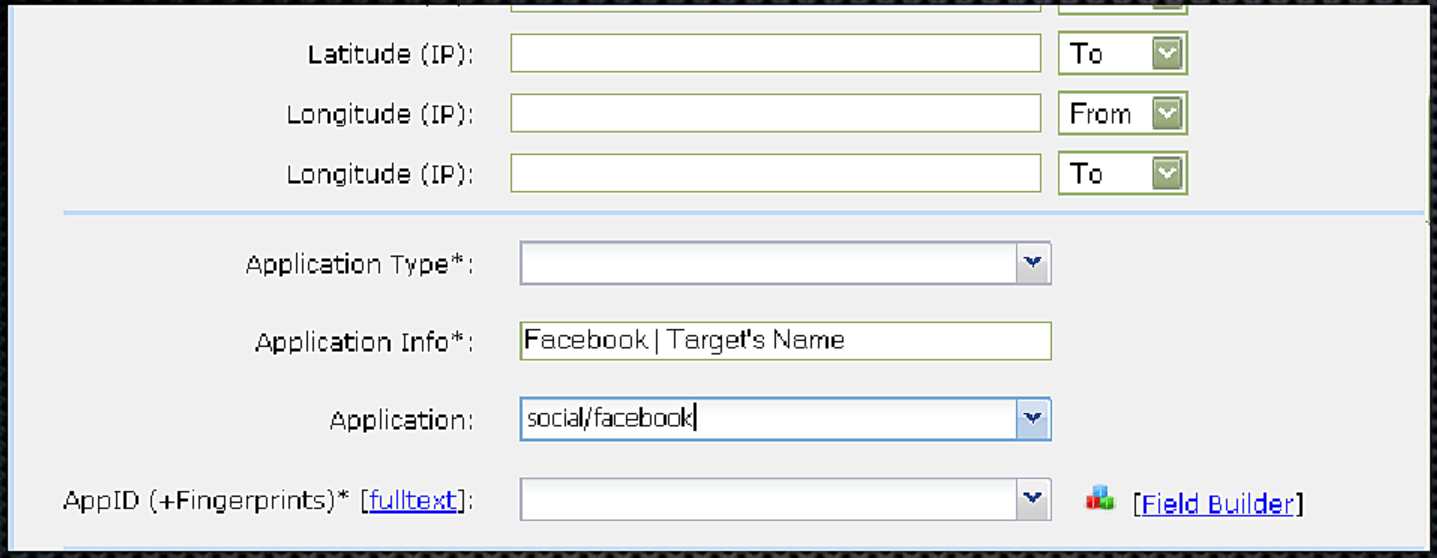
Cons:

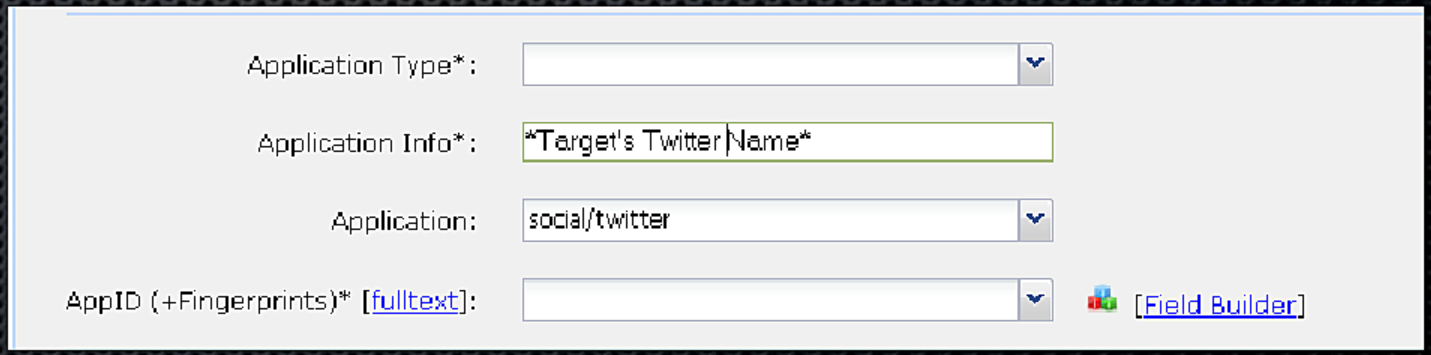
Traffic Overload – Too many results (GET requests etc.)

Proxies and network architecture can obfuscate the target's traffic

Bad presentation – HTTP activity usually needs to be viewed as code

(S//SI//REL TO USA, FVEY) Xkeyscore Server Side Pulls





(TS//SI//REL TO USA, FVEY)
Useful AppIds

Social/* = A great starting point, will show all social traffic on an IP, also an efficient way to see the types of OSN are being used in a geographic area, ISP, region, etc.

Social/YourOSNHere = Great for IP level targeting etc.

Social/Facebook/chat/to_server = Possible to see the recepient of a target's chat and the message that was sent

Social/Facebook/upload/photo = AppID detects the photos being uploaded onto Facebook by your target

(U) Questions or Comments?

- Contact Info

[redacted]

[redacted]@nsa.ic.gov

(U//FOUO) Online Social Networks Working Group

Email: DL OSNwg

Main Page: "Go OSN"
Other Pages: "Go Facebook" "Go Twitter" "Go OSN_Tiger_Team"