

# PRISM/US-984XN Overview

OR

# The SIGAD Used **Most** in NSA Reporting Overview

PRISM Collection Manager, S35333

April 2013

Derived From: NSA/CSSM 1-52 Dated: 20070108

Declassify On: 20360901

### TOP SECRET//SI//ORCON//NOFORN















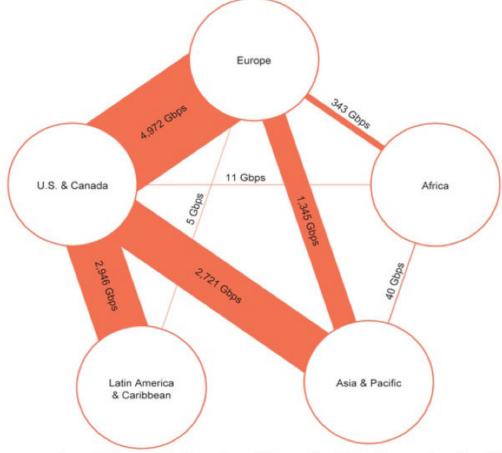


### (TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the cheapest path, not the physically most direct path - you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research



















### (TS//SI//NF) FAA702 Operations

Two Types of Collection



### Upstream

 Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should **Use Both** 



### **PRISM**

 Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

















Why Use Both: PRISM vs. Upstream



	PRISM	Upstream
DNI Selectors	9 U.S. based service providers	Worldwide sources
DNR Selectors	Coming soon	Worldwide sources
Access to Stored Communications (Search)		0
Real-Time Collection (Surveillance)		
"Abouts" Collection	0	
Voice Collection	✓ Voice over IP	
Direct Relationship with Comms Providers	Only through FBI	<b>✓</b>



















### (TS//SI//NF) PRISM Collection Details



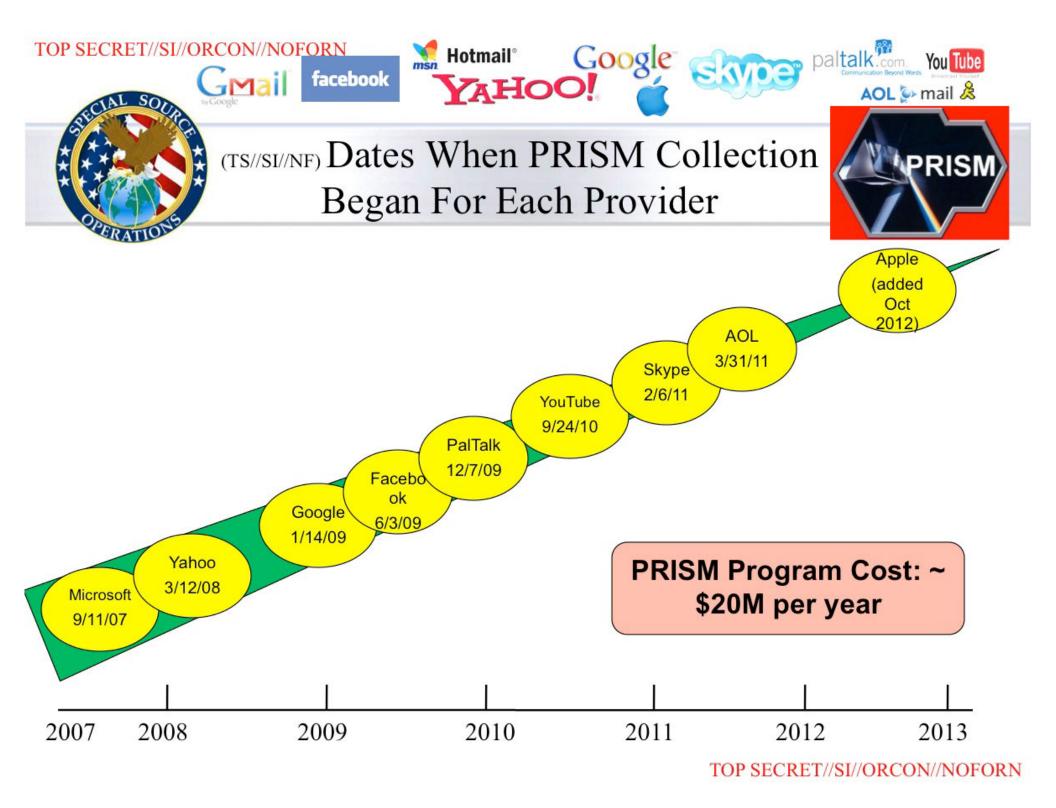
**Current Providers** 

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

- E-mail
- Chat video, voice
- Videos
- Photos
- · Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity logins, etc.
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page:



TOP SECRET//SI//ORCON//NOFORN



facebook





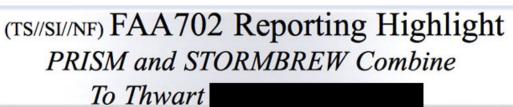








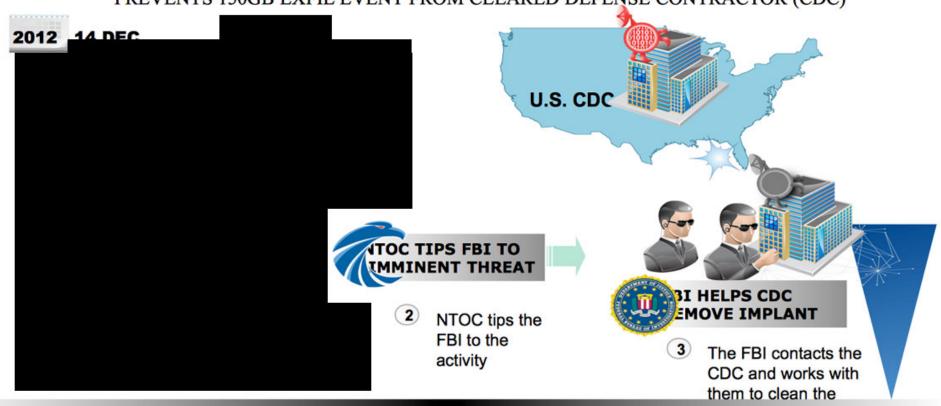






### SAME-DAY NTOC/FBI COLLABORATION

PREVENTS 150GB EXFIL EVENT FROM CLEARED DEFENSE CONTRACTOR (CDC)



The victim performed comprehensive actions on the infected network, thus PREMOTENTING EXFILTRATION on the SAME DAY NTOC DISCOVERED ADVERSARY INTENT













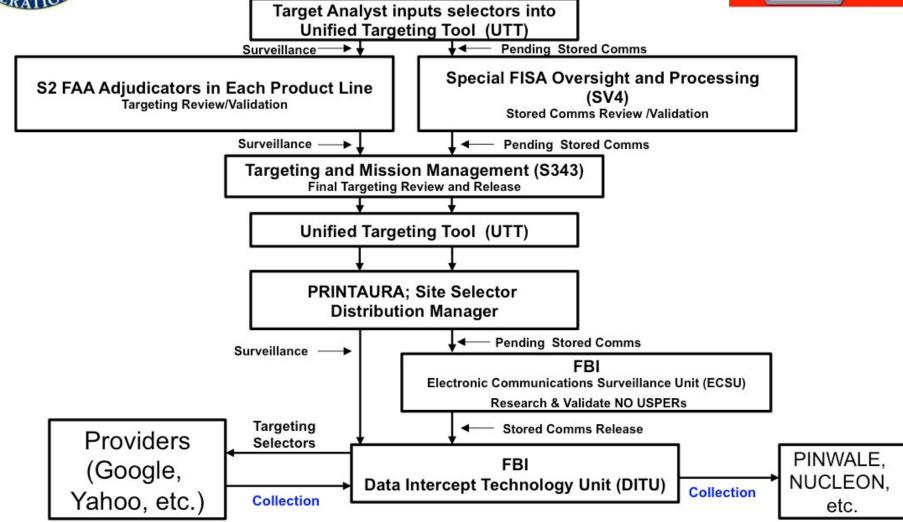


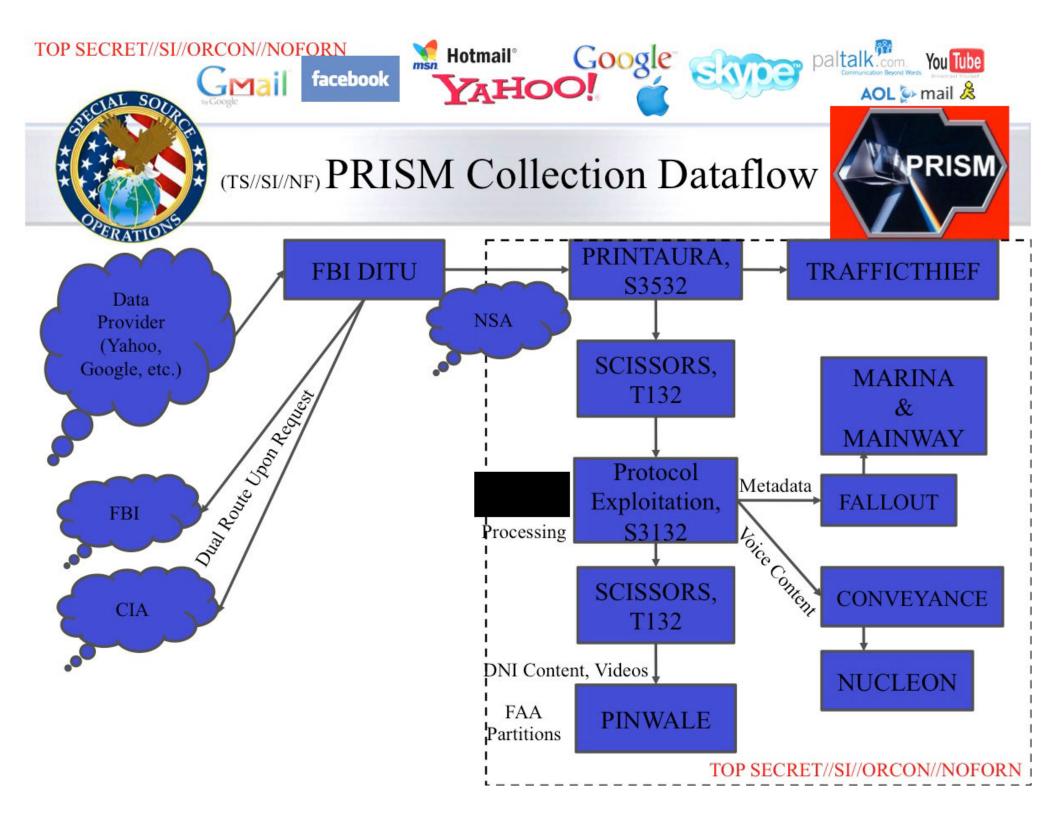




### (TS//SI//NF) PRISM Tasking Process



























### (TS//SI//NF) PRISM Case Notations



## P2ESQC120001234

### PRISM Provider

P1: Microsoft

P2: Yahoo

P3: Google

P4: Facebook

P5: PalTalk

P6: YouTube

P7: Skype

P8: AOI

PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

### Content Type

A: Stored Comms (Search)

B: IM (chat)

C: RTN-EDC (real-time notification of an e-mail event such as a login

or sent message)

D: RTN-IM (real-time notification of a chat login or logout event)

F: F-Mail

F: VoIP

G: Full (WebForum)

H: OSN Messaging (photos, wallposts, activity, etc.)

I: OSN Basic Subscriber Info

J: Videos

. (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN



facebook















### (TS//SI//NF) REPRISMFISA TIPS



