PRISM/US-984XN Overview

OR

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

[redacted] PRISM Collection Manager, S35333

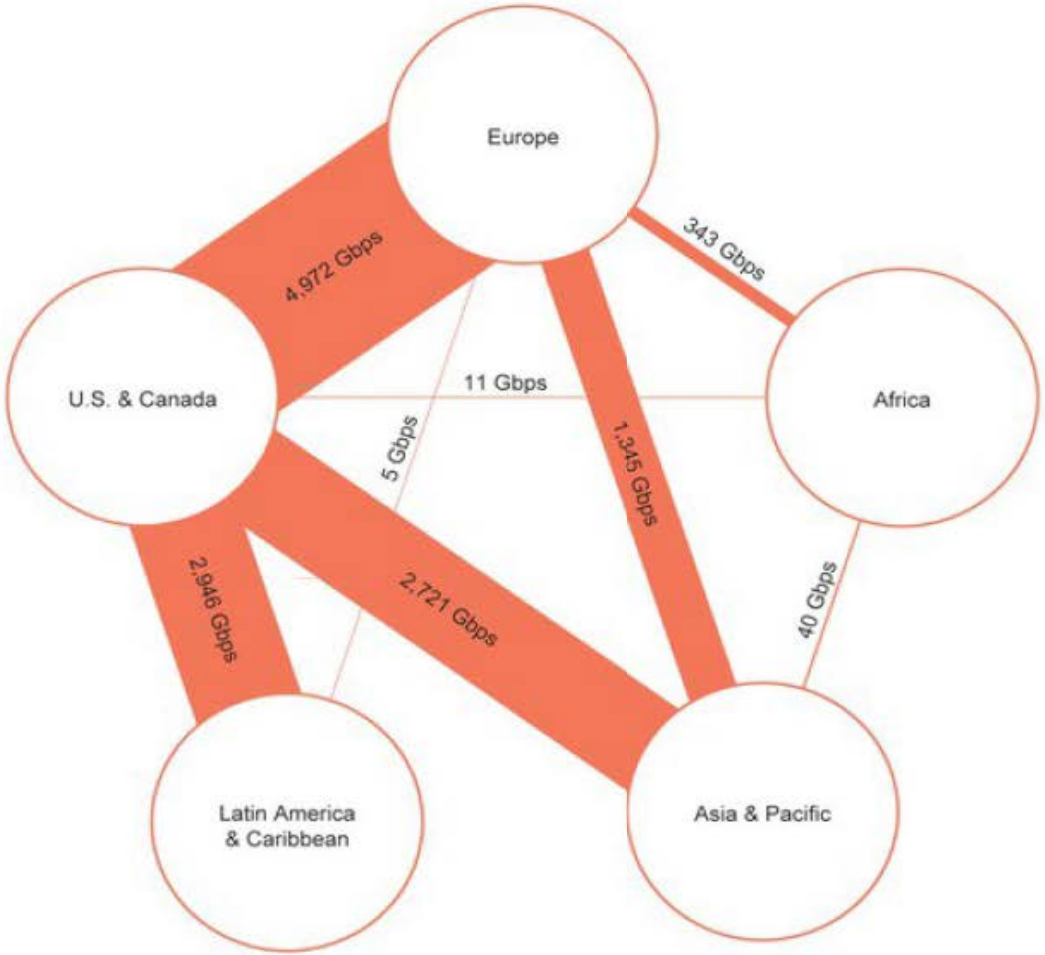
April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

(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.

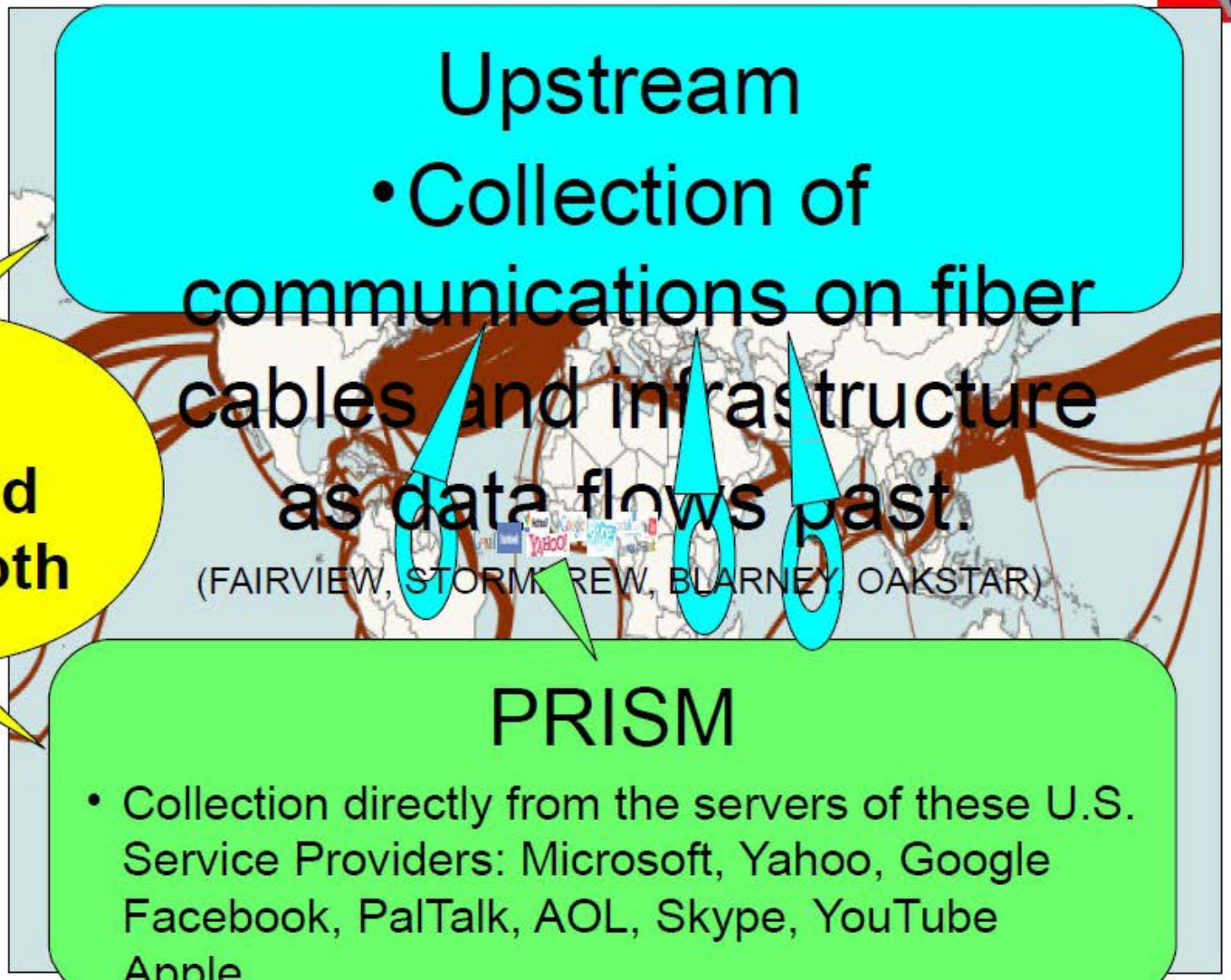


International Internet Regional Bandwidth Capacity in 2011

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.

(TS//SI//NF) FAA702 Operations

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)	✓	⊘
Real-Time Collection (Surveillance)	✓	✓
"Abouts" Collection	⊘	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	⊘ Only through FBI	✓

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

Current Providers

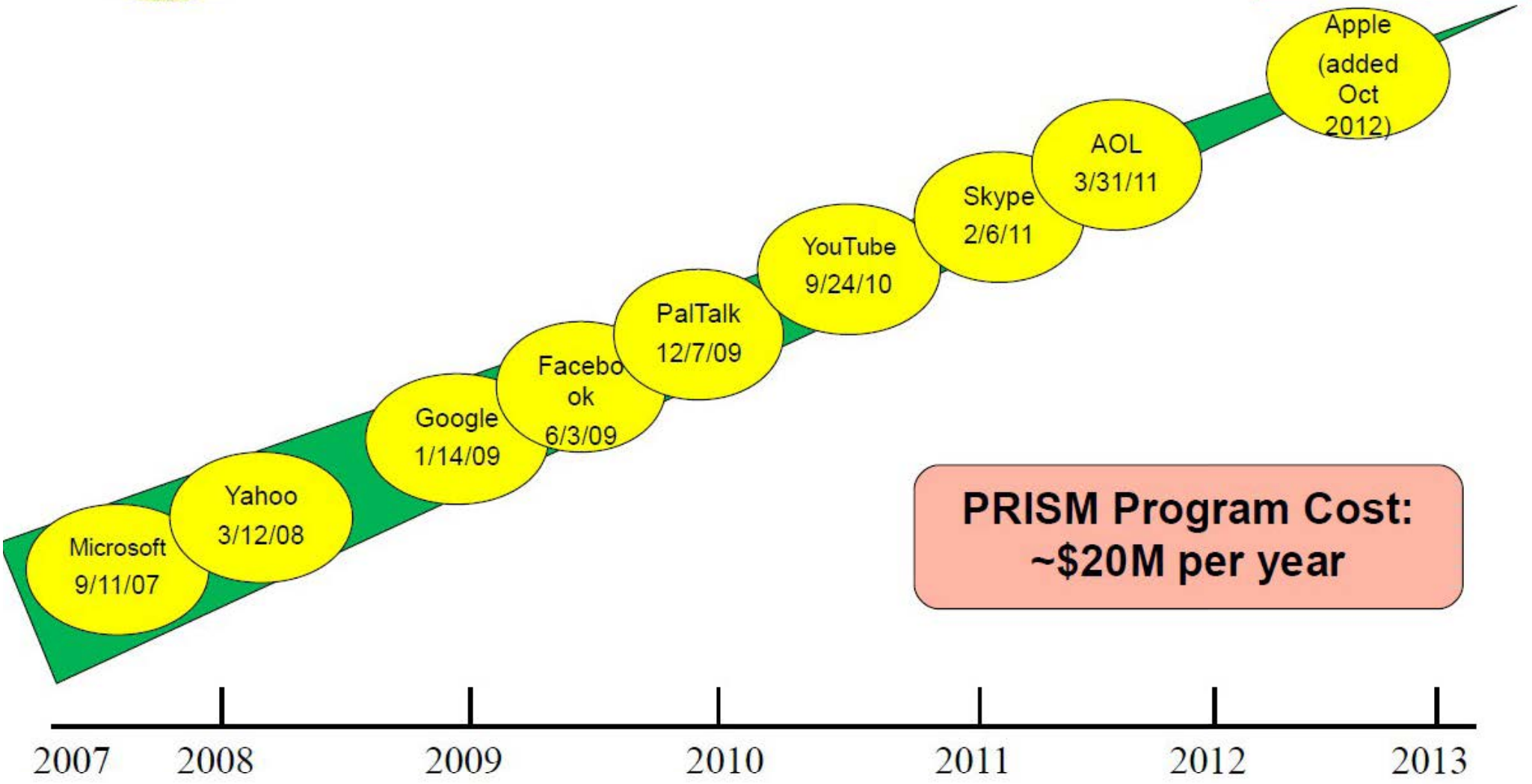
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

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

- 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:
Go PRISMFAA

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~$20M per year

(TS//SI//NF) FAA702 Reporting Highlight

PRISM and STORMBREW Combine

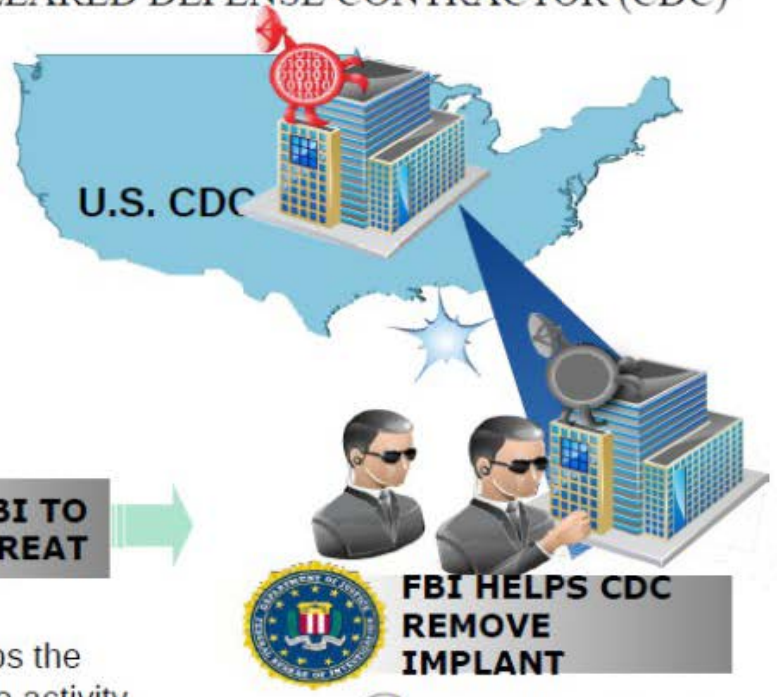
To Thwart [redacted]

SAME-DAY NTOC/FBI COLLABORATION

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

2012 **14 DEC**

[redacted]



2 NTOC tips the FBI to the activity

3 The FBI contacts the CDC and works with them to clean the network

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

(TS//SI//NF) Some Higher Volume Domains Collected from FAA Passive

In addition to Hotmail, Yahoo, Google, Paltalk, Facebook, Skype, AOL:

Select IP Addresses

[redacted]

[redacted]

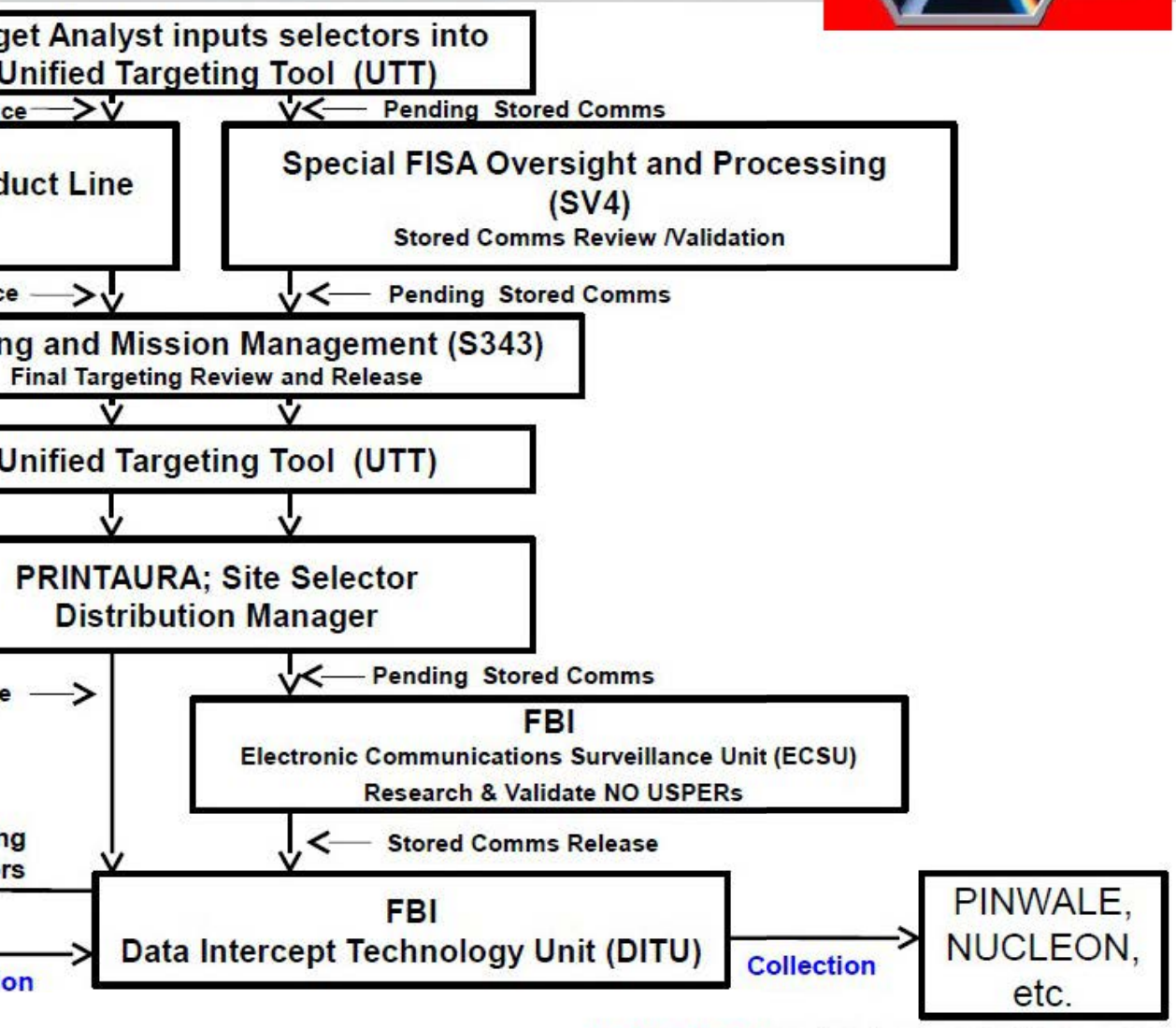
wanadoo.fr

[redacted]

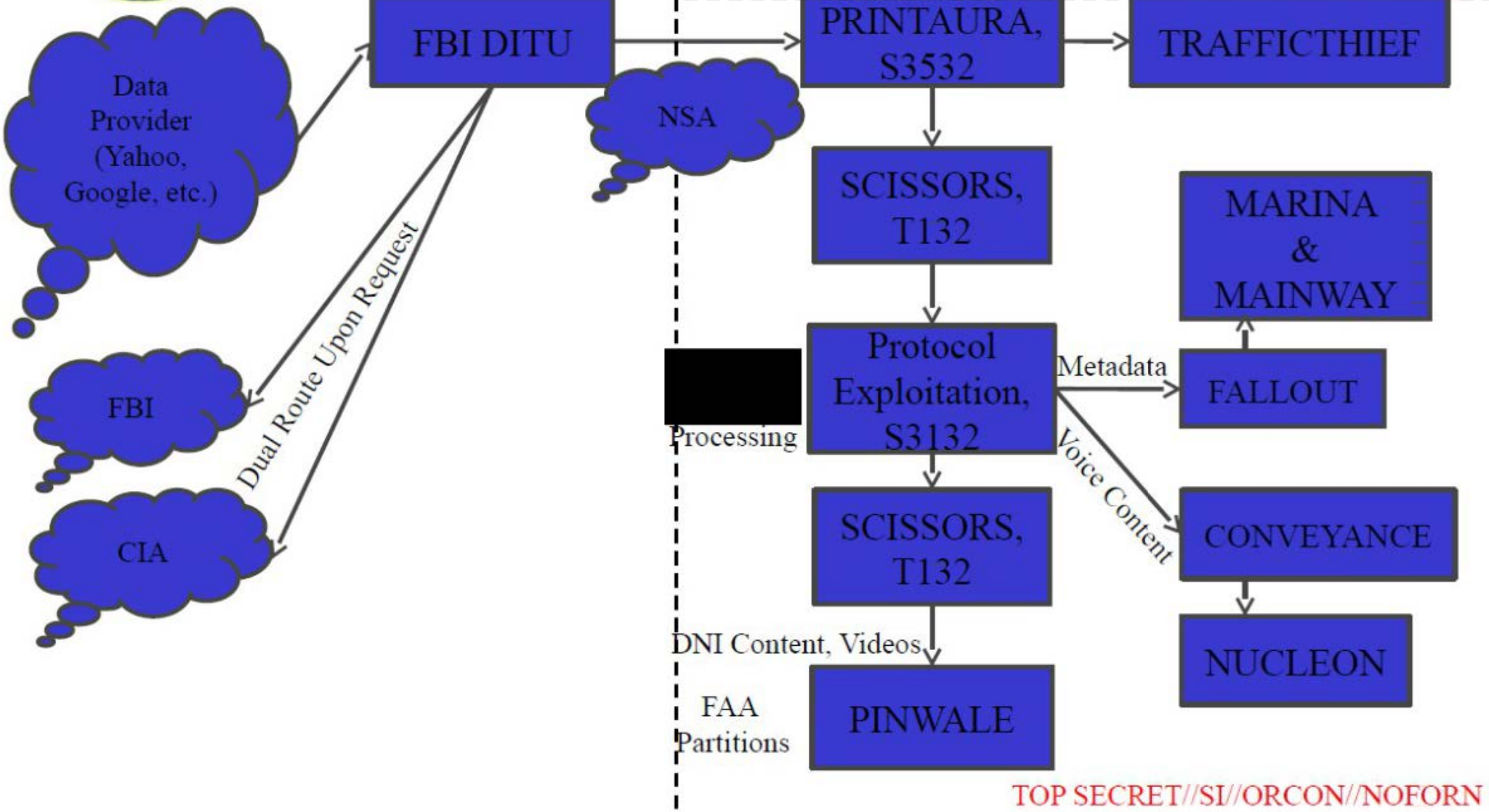
alcatel-lucent.com

[redacted]

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



(TS//SI//NF) PRISM Collection Dataflow



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

P2ESQC120001234

PRISM Provider
- P1: Microsoft
- P2: Yahoo
- P3: Google
- P4: Facebook
- P5: PalTalk
- P6: YouTube
- P7: Skype
- P8: AOL
- PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

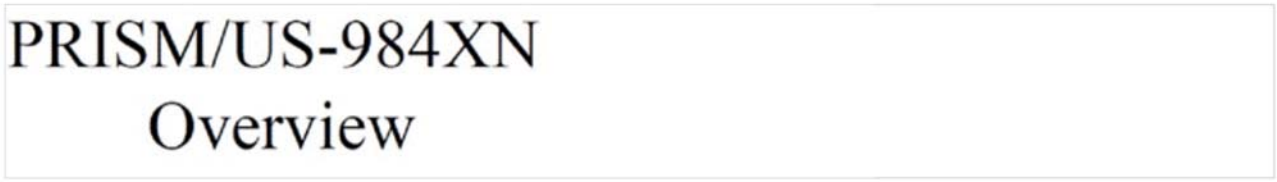
Serial #

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)
- E: E-Mail
- F: VoIP
- G: Full (WebForum)
- H: OSN Messaging (photos, wallposts, activity, etc.)
- I: OSN Basic Subscriber Info
- J: Videos
- . (dot): Indicates multiple types

Prism Entier

11 pages - Contributed by Martin Untersinger , Le Monde - Oct 18, 2013

Notes sur la présentation Prism (p. 1)



"Le Monde" a décidé de rendre public une sélection de documents issus de la présentation de 41 pages décrivant le fonctionnement du programme Prism aux analystes. C'est sur la base de cette présentation, à laquelle "Le Monde" a accès dans son intégralité, que le Guardian et le Washington Post ont révélé l'existence de ce programme. Le Monde a choisi de ne pas reproduire la majorité des documents de la présentation du programme Prism exhumée par Edward Snowden. La plupart sont très techniques et n'apportent que peu d'informations. Certains, sont extrêmement sensibles. Un certain nombre de ces documents ont déjà été publiés par le Washington Post et le Guardian. Deux des documents suivants (p. 4 et 7) sont inédits à ce jour.

Le réseau Internet (p. 2)

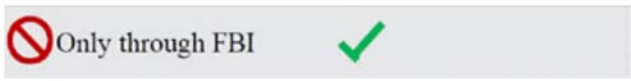
Ce document décrit l'infrastructure générale d'Internet au niveau mondial, et justifie les dispositifs d'interception par la place centrale que les Etats-Unis y occupent.

Il faut utiliser Prism et Upstream (p. 3)

Ce document incite les analystes de la NSA à utiliser à la fois Prism et Upstream, une famille de programmes qui interceptent les données dans les infrastructures d'Internet.

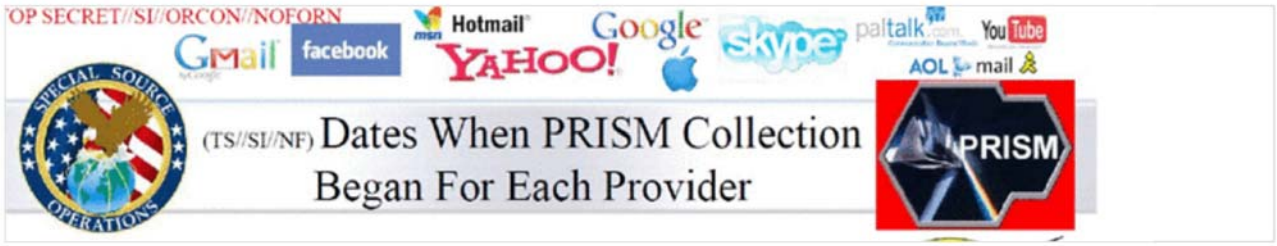
Ce document compare les programmes Prism et Upstream (p. 4)

Le rôle du FBI (p. 4)



Le FBI joue un rôle purement technique, probablement parce que le programme Prism nécessite le déploiement d'infrastructures techniques sur le sol américain, ce qui n'est pas du ressort de la NSA. Dans tous les cas, l'accès des services de renseignement américain aux entreprises est privilégié, et plus direct que ce qui avait été imaginé précédemment.

Dates d'entrée dans le programme (p. 6)



Ce document montre les dates d'entrées dans le programme Prism des géants du Net américain

Programmes complémentaires (p. 7)

Les deux programmes ont été utilisés, de manière complémentaire, dans le cadre d'une opération de la NSA

NTOC (p. 7)

Il s'agit de la cellule de crise de la NSA.

Un sous-traitant de la défense américaine (p. 7)

Le Monde a choisi de ne pas révéler le pays concerné en raison de la nature très sensible de la question. (p. 7)

La véritable identité du pays n'apporte que peu d'informations complémentaires.

Les domaines surveillés par la NSA (p. 8)

Le document présente les domaines surveillés par la NSA entre le 1er au 31 janvier 2013. La période pendant laquelle cette surveillance a été menée est inscrite au bas du document. Se chevauchant avec certaines adresses devant être masquées, elle n'apparaît pas.

Une partie seulement (p. 8)

Ce document ne mentionne ce qui n'est qu'un extrait des domaines surveillés par l'agence. De même, le document ne précise pas la quantité ou la nature des données éventuellement interceptées.

Upstream (p. 8)

Il s'agit de la famille de programme Upstream, qui intercepte les données lorsqu'elles transitent dans les grandes infrastructures d'Internet, notamment les câbles. FAA (pour FISA Amendment Act) est le cadre juridique qui entoure Prism et une partie d'Upstream.

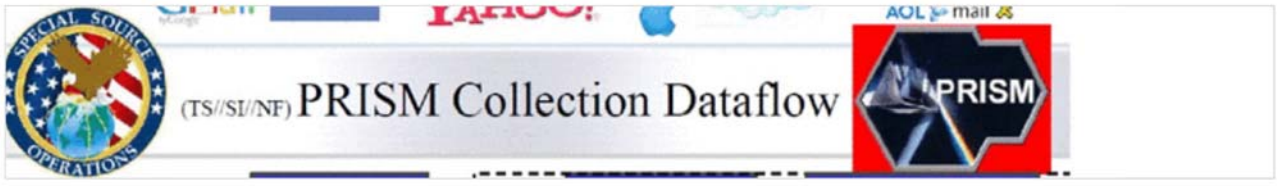
Le Monde a choisi de ne pas révéler les autres domaines surveillés par la NSA (p. 8)

Cette décision s'explique par la volonté de ne pas compromettre des enquêtes en cours des journalistes du "Monde", ainsi que par la nature très sensible de certains domaines.

Le processus (p. 9)

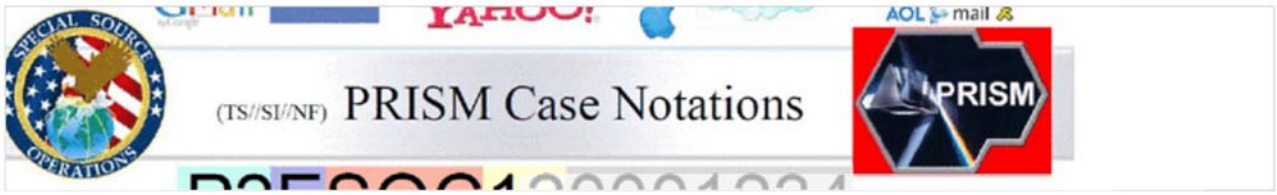
Ce document détaille le processus technique, de l'analyste derrière son ordinateur jusqu'aux bases de données des entreprises du Web. Le rôle du FBI comme intermédiaire technique y apparaît clairement.

Dans les bases de données de la NSA (p. 10)



Une fois les données récupérées, ces dernières cheminent à travers un maillage serré de bases de données qui les trient et les archivent.

Classification (p. 11)



Ce document montre la manière dont la NSA codifie et "range" les données interceptées.