Privacidad en Internet

Rafael Bonifaz- rafael@asle.ec

Si tu vecino te espía

- ¿Te molestarías?
- ¿Sentirías tu intimidad invadida?
- ¿Qué tanto puede saber de ti al mirar por la ventana?
- ¿Estarías de acuerdo en dejarte espiar por tu vecino por seguridad?

¿Si tu vecino entra a tu computadora?

- ¿Qué tanto podría saber tu vecino al revisar tu computadora o celular?
- Correos, chats, redes sociales, contraseñas, cámara web, micrófono, historiales de búsqueda, fotos, videos, etc...
- ¿Estas de acuerdo que se metan en tu computador por tu seguridad?

Privacidad

- Definición RAE:
  - "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"
- El Artículo 12 de la Declaración Universal de los Derechos Humanos:
  - *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*

La Nube

No existe la nube

Existe la computadora de otra persona

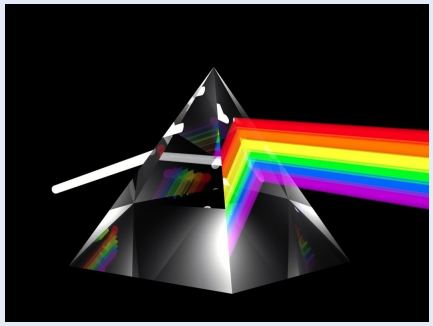
Imagen tomada de revista Wire online:
http://www.wired.com/politics/security/news/2007/10/domestic_taps

Existe computadora de otra persona

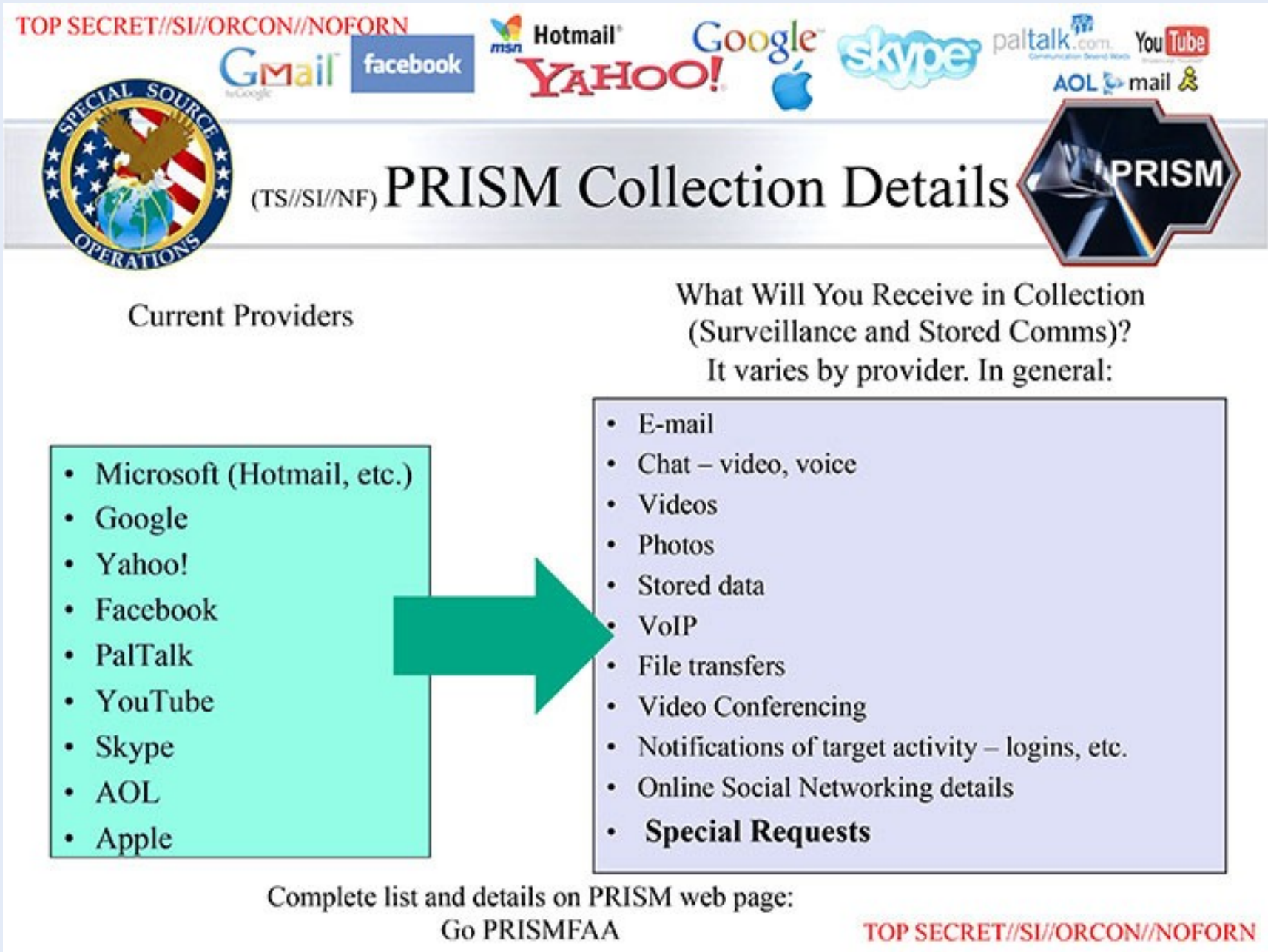
- ***“Si no pagas por el servicio, eres el producto”***
- Cuando usas servicios en Internet, compartes tu información los proveedores:
  - Google, Microsoft, Facebook, Dropbox, etc...
- Si la información no viaja cifrada puede ser leída por terceros

Snowden y la NSA

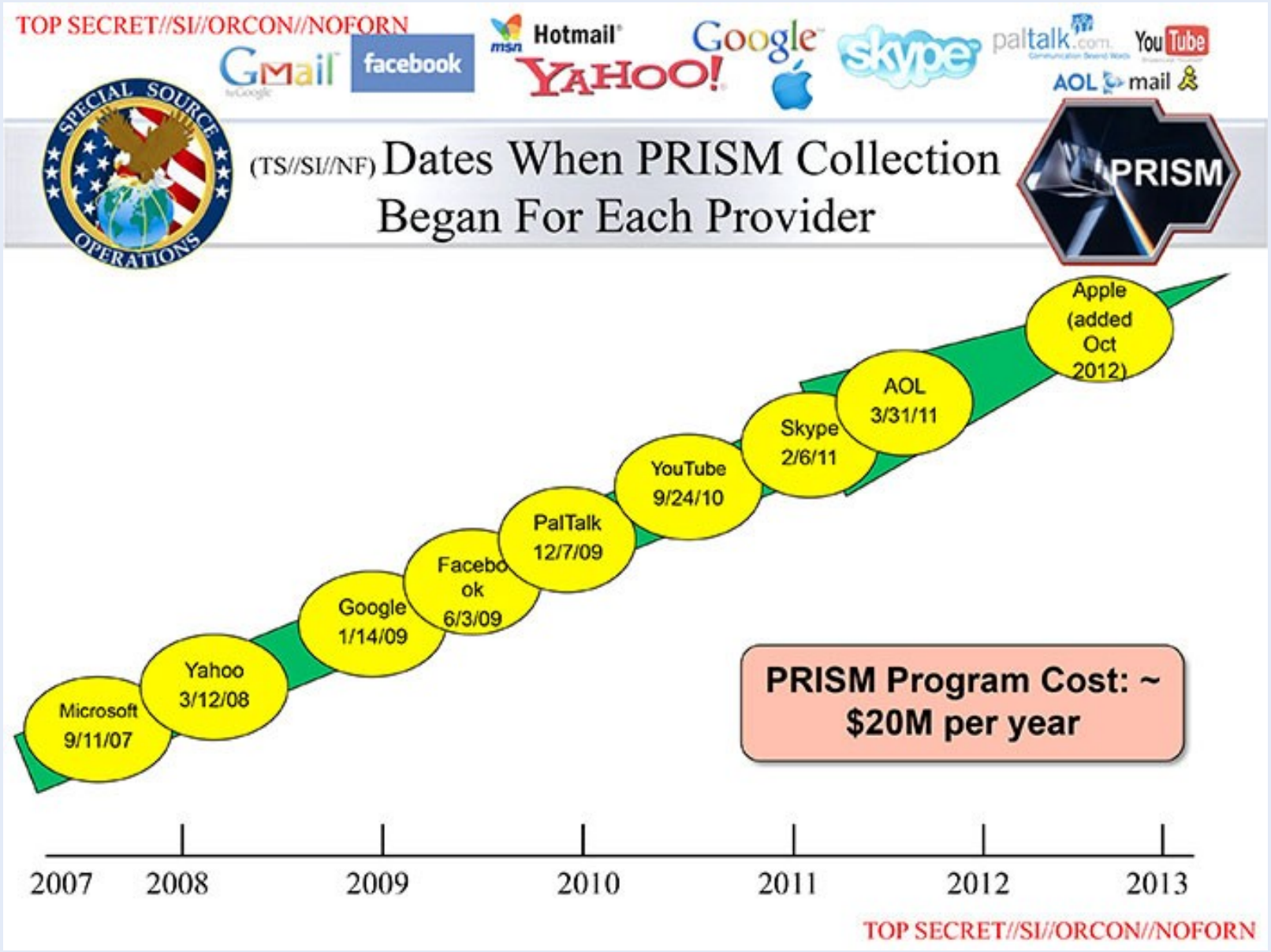
- NSA: Agencia de Seguridad Nacional (EEUU)
- Alianza de los 5 ojos: EEUU, Reino Unido, Canadá, Australia y Nueva Zelanda
- Snowden: Trabajó para la NSA y filtró documentos secretos
- Algunos programas de Espionaje: PRISM, X-KEYSCORE, TAO y otros



PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Details
PRISM
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
TOP SECRET//SI//ORCON//NOFORN

PRISM


TOP SECRET//SI//ORCON//NOFORN
Hotmail
Google
YAHOO!
skype
paltalk.com
YouTube
Gmail
facebook
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

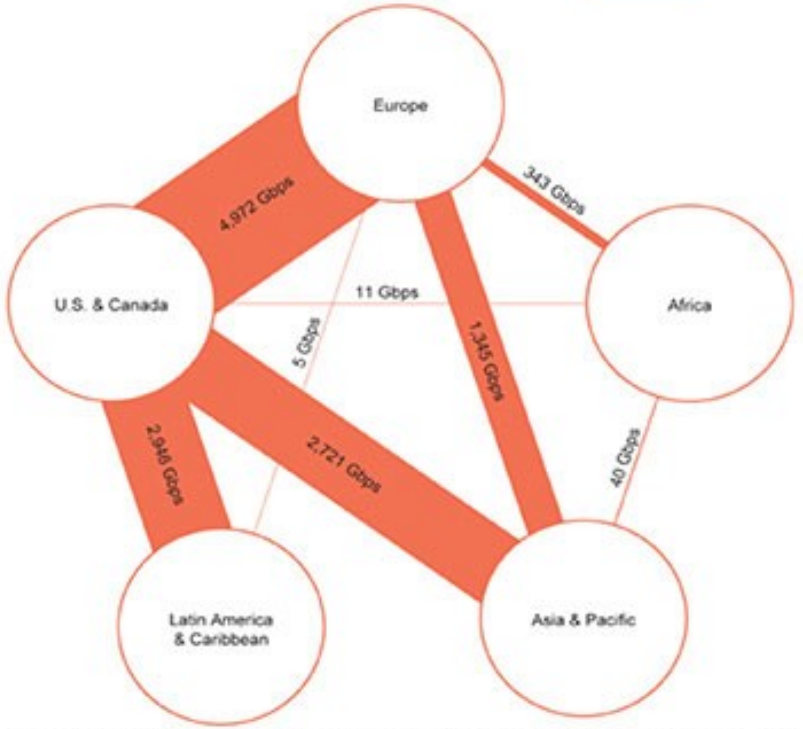
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

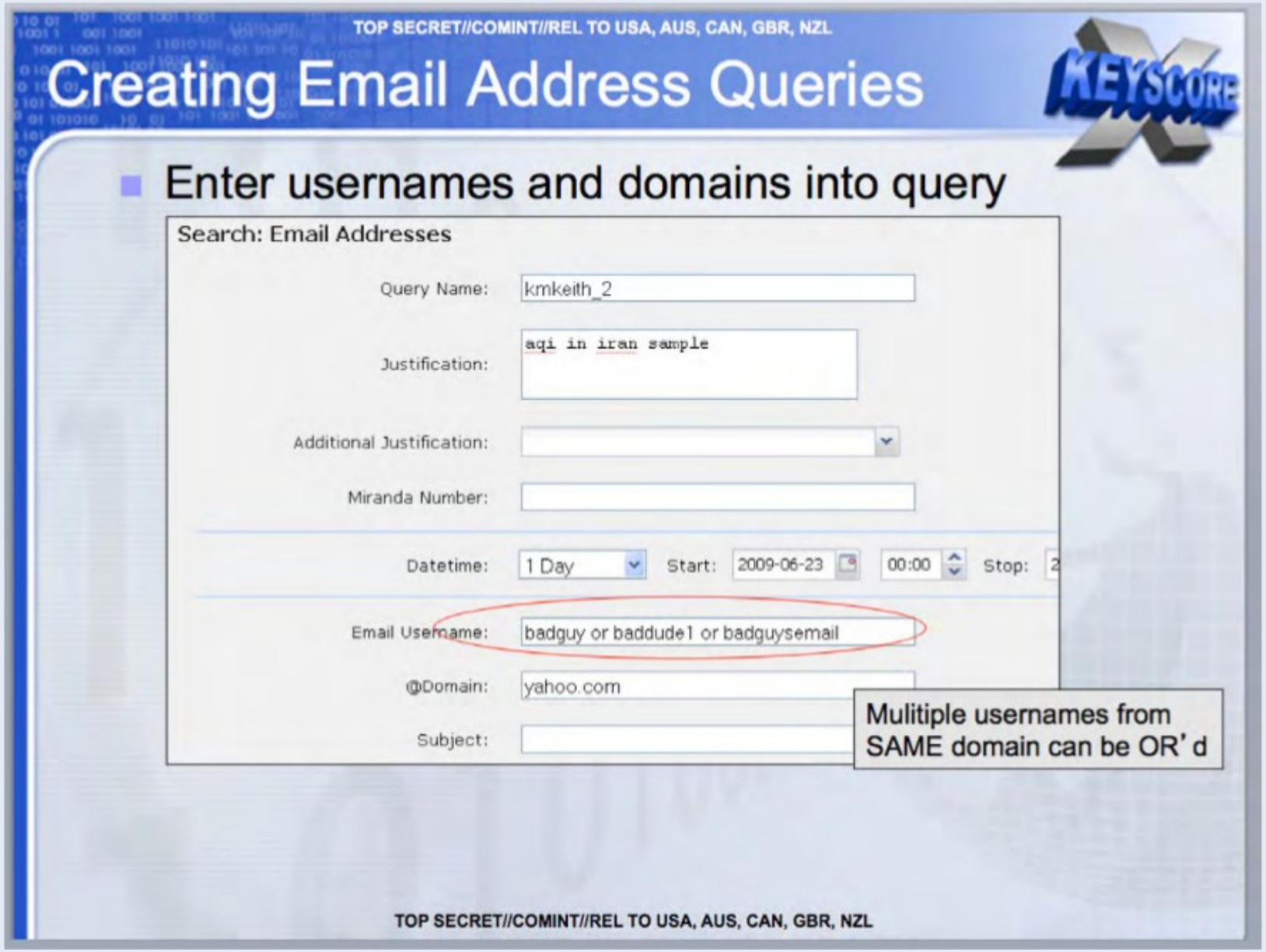
- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

X-KESCORE


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Creating Email Address Queries
KEYSCORE
Enter usernames and domains into query
Search: Email Addresses
Query Name: kmkeith_2
Justification: aqi in iran sample
Additional Justification:
Miranda Number:
Datetime: 1 Day Start: 2009-06-23 00:00 Stop:
Email Username: badguy or baddude1 or badguysemail
@Domain: yahoo.com
Subject:
Mulitiple usernames from SAME domain can be OR'd
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Partners Estratégicos

Espionaje a Presidentes

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Spyfiles y Hacking Team

- Spyfiles: Filtraciones publicadas entre 2011 - 2014
- Espionaje en Internet, celulares, computadoras
- Base del libro Cryptopunks
- http://wikileaks.org/spyfiles
- Hacking Team es una de las empresas en Spyfiles
  - En julio 2015 se filtraron 400G
  - https://www.wikileaks.org/hackingteam/emails/
  - http://ht.transparencytoolkit.org/

Hacking Team

Tomado de http://wikileaks.org/spyfiles/list/document-type/video.html

Filtración Hacking Team

http://hipertextual.com/2015/07/los-paises-iberoamericanos-que-usaron-a-hacking-team-para-espiar

Filtración Hacking Team

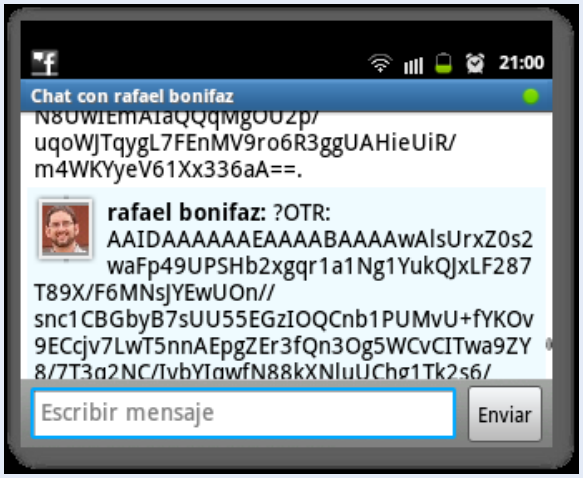
- Varios países de América Latina
- México el país que más compró a Hacking Team
- Buscar correos acá:
  - https://www.wikileaks.org/hackingteam/emails/
- Toda la información:
  - http://ht.transparencytoolkit.org/

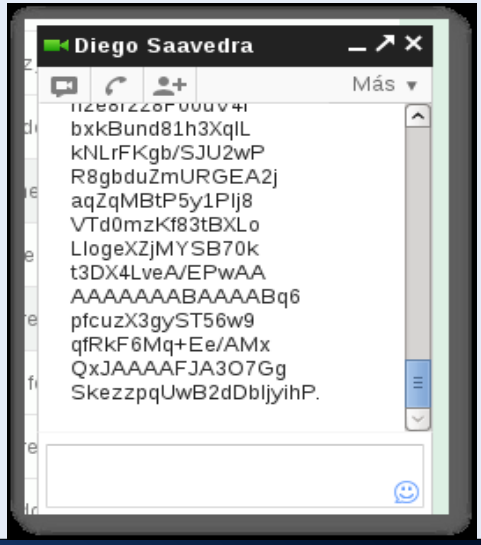
Software Libre

- Se construye de forma colaborativa en grandes mingas del conocimiento en Internet
- Se sabe como funciona y por tanto es auditable
- Se confía en una comunidad y no se tiene fe ciega en una corporación
- La comunidad esta dispuesta a ayudar
- La comunidad se une para crear el mejor software posible para solucionar su problema común
- En seguridades significa crear los sistemas más seguros posibles
- Normalmente son comunidades abiertas a las que nos podemos unir, opinar y colaborar
- Necesitamos formar talento humano capaz de controlar y apropiarse de la tecnología
- Solo con software libre es posible

Criptografía

- Permite que la información sea accesible solo por los interesados.
- La información se debe cifrar en la computadora antes de ser enviada
- Existe herramientas libres para:
- Chat cifrado: OTR
- Correo cifrado: PGP
- Gestión de contraseñas: KeepassX
- Voz/Ip cifrado (remplazo Skype): Jitsi
- Navegación anónima y privada: Tor
- Transacciones monetarias (Bitcoin y derivados)
- Alternativas al correo como Pond





Infraestructura propia y descentralizada

- Infraestructura propia y descentralizada
- Hardware libre
- Páginas web y servicios dentro del país
- Servidores propios de comunicaciones
- Correo postfix, exim, etc..
- Chat con XMPP, IRC
- VOZ/IP: Elastix, Asterisk, FreeSwitch
- Nube: Owncloud, Alfresco
- Celular: CyanogenMod, Firefox OS, Replicant OS, ¿cryptophone?
- Servicios ocultos con Tor

Software Libre, Criptografía y Privacidad

- Información relevante:
  - “Cryptopunks”, Julian Assange, Jacob Appelbaum, Jérémie Zimmerman y Andy Muller-Maguhn (2012)
    - http://assange.rt.com/es/episodio-8--assange-y-los-criptopunks/
    - http://assange.rt.com/es/episodio-9--assange-y-los-criptopunks/
- “1984” de George Orwell (1949)
- Los Spyfiles: http://wikileaks.org/spyfiles
- “Sin un Lugar Donde Esconderse” de Glen Greenwald (2014)
- Filtraciones de Snowden:
  - https://search.edwardsnowden.com/
  - http://glenngreenwald.net/#BookDocuments
- “Cuando Google Conocío Wikileaks”, Julian Assange 2014
- Libros de Cory Doctorow (Marcus Yallow)
  - Pequeño Hermano
  - Homeland

Una reflexión

“Si quieres construir un barco, no empieces por buscar madera, cortar tablas o distribuir el trabajo, sino que primero has de evocar en los hombres el anhelo de mar libre y ancho.”

Antoine de Saint-Exupéry

Infraestructura propia y descentralizada

- Rafael Bonifaz
  - rafael@asle.ec
  - PGP ID: 5310523C
- Twitter:
  - @rbonifaz @asle_ec
- http://rafael.bonifaz.ec http://www.asle.ec

- Hecha con Software Libre: Debian, LibreOffice, Shutter, Iceweasel
- ¡Copien y mejoren esta presentació!