Through a PRISM, Darkly

Kurt Opsahl

Deputy General Counsel, EFF

What we'll talk about today

- The Background – History, codenames, spying laws
- The Programs – Facts we know about spying under:
  - FISAAA and the Patriot Act (PRISM, MARINA)
  - Executive Orders (MUSCULAR, BULLRUN)
- Fight Back – What we can do to stop the spying

The Background

- After 9/11, President Bush unleashed the full power of the dark side
- A subset of the President's Surveillance Program was later labeled the TSP
- PSP was without the court-approved warrants ordinarily required for domestic spying

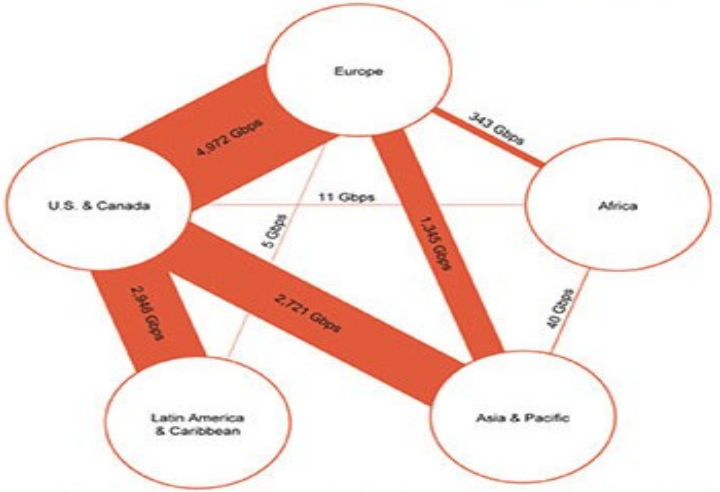
US Companies Sit on Wire

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

PRISM

- 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.



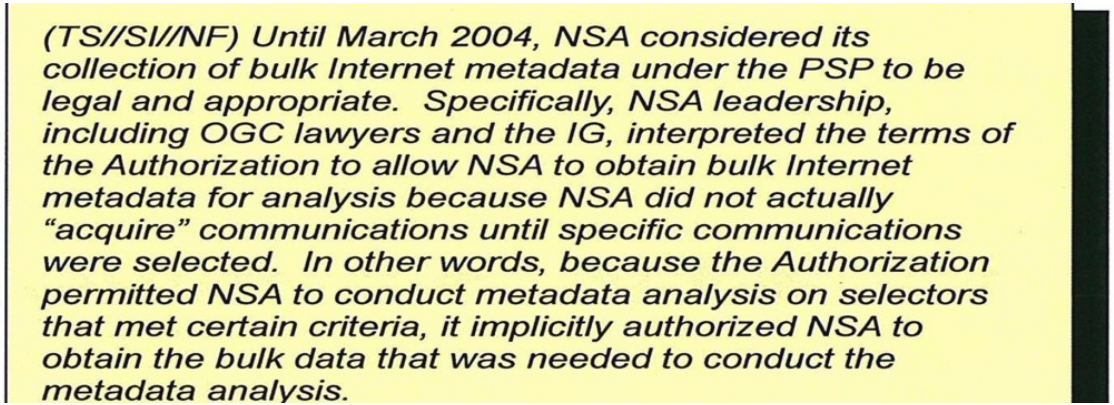
International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

Showdown at the Hospital

- March 2004 – Acting Attorney General Comey refused to sign off on the PSP



- Gonz
- Threats of resignation

Public Disclosure

- 2005: *NY Times* revealed the existence of PSP, focus on content collection
- 2006: *USA Today* revealed telephone call-detail records program
- 2007: Gov't claims program under FISA court;
  - Protect America Act passes
- 2008: FISA Amendments Act
- 2013: Edward Snowden

Know Your Codenames

- *STELLAR WIND* – the original PSP program – has four basic parts:

	Content	Metadata
Telephony	NUCLEON	MAINWAY
Internet	PINWALE/ PRISM	MARINA

- EVILSEED – IP geolocation (IEP)
- FASCIA – Location database

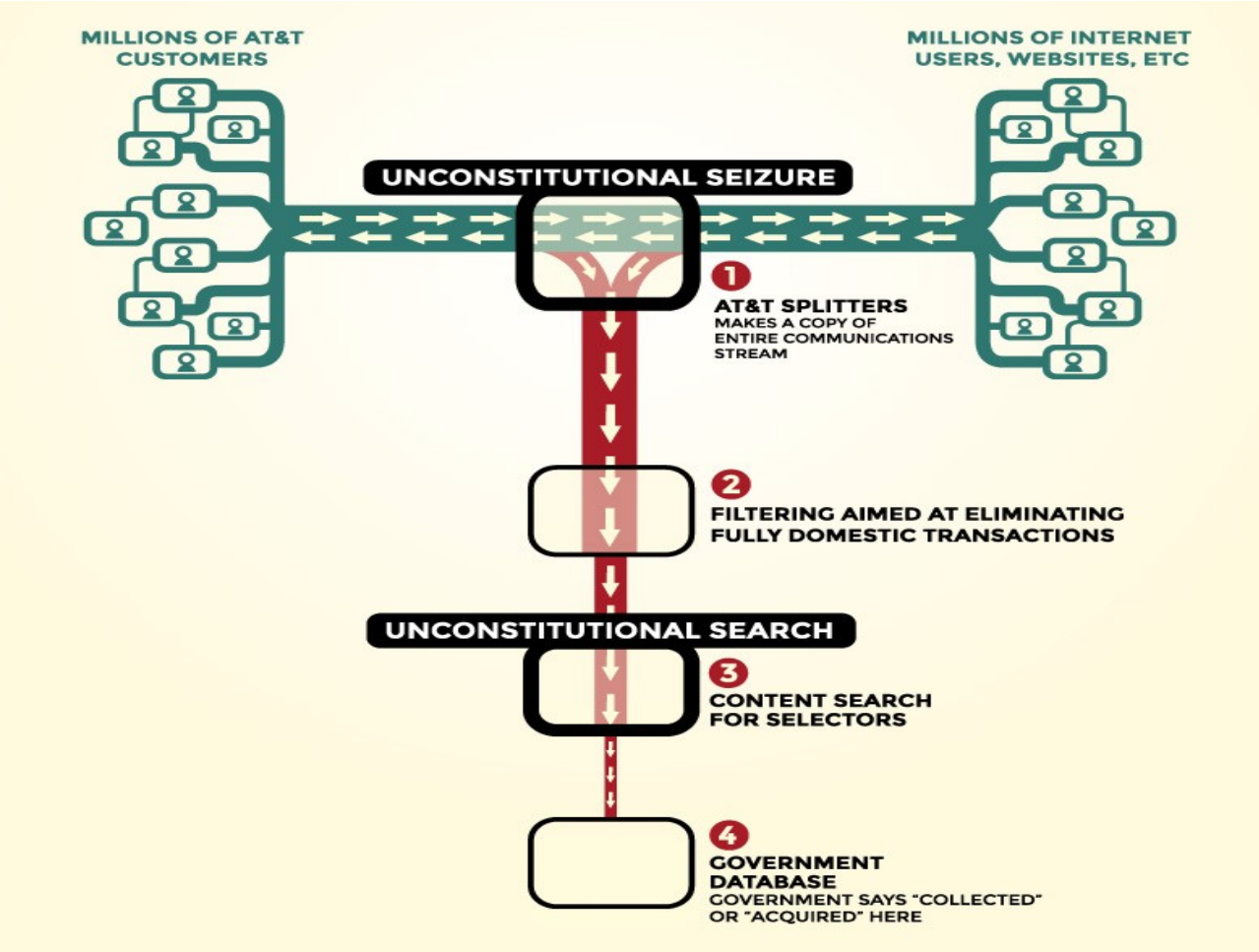
Boundless indeed

Know your spying laws

- Wiretap Act
- Foreign Intelligence Surveillance Act
- Electronic Communications Privacy Act
- USA Patriot Act (Section 215)
- Protect America Act (temporary)
- FISA Amendment Act (Section 702)
- Executive Order 12333

Fiber-Optic Splitters

- The “splitter cabinet” splits the light signals in two, making two identical copies of the data carried on the light signal
- One copy goes to the NSA
- Mark Klein revealed Room 641A of AT&T’s San Francisco facility

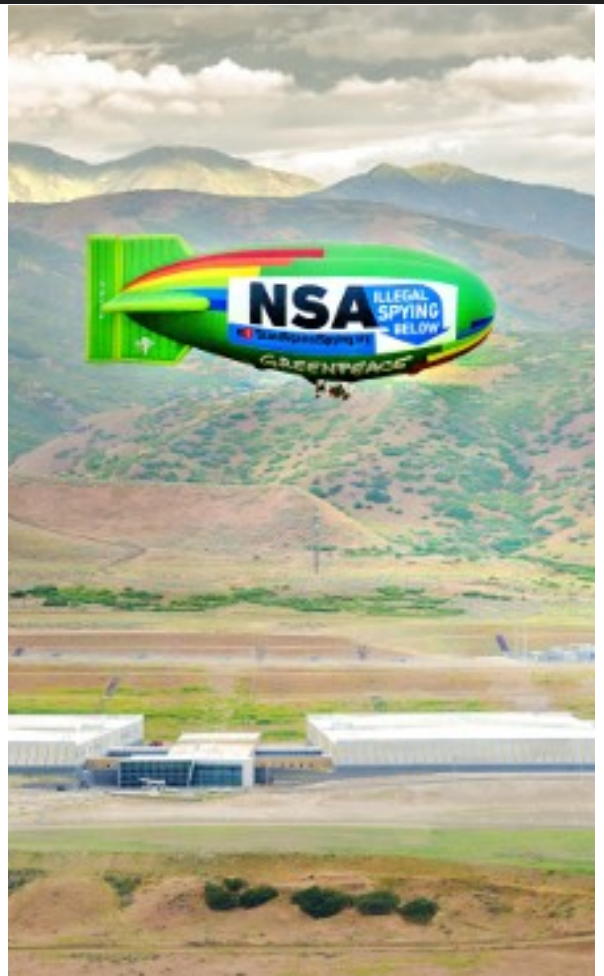

MILLIONS OF AT&T CUSTOMERS
MILLIONS OF INTERNET USERS, WEBSITES, ETC
UNCONSTITUTIONAL SEIZURE
1
AT&T SPLITTERS
MAKES A COPY OF ENTIRE COMMUNICATIONS STREAM
2
FILTERING AIMED AT ELIMINATING FULLY DOMESTIC TRANSACTIONS
UNCONSTITUTIONAL SEARCH
3
CONTENT SEARCH FOR SELECTORS
4
GOVERNMENT DATABASE
GOVERNMENT SAYS "COLLECTED" OR "ACQUIRED" HERE

So How Much Is That?

- NSA says it only ‘touches’ about 1.6% of the “world’s Internet traffic”
  - Only 11.8% of traffic is web, 2.9% comms
    - Most is video streaming
    - About 2/3 of email is spam
  - 1.6% is almost 30 petabytes a day
- Plus phone calls, call records, location

Utah Data Facility

- 100k ft^2 server space
- Estimates between 3 and 12 exabytes
- 65 to 75 megawatts
- Brewster Kahle of the Internet Archive estimates less than 5k ft^2 to store and process year of *just U.S.* phone calls



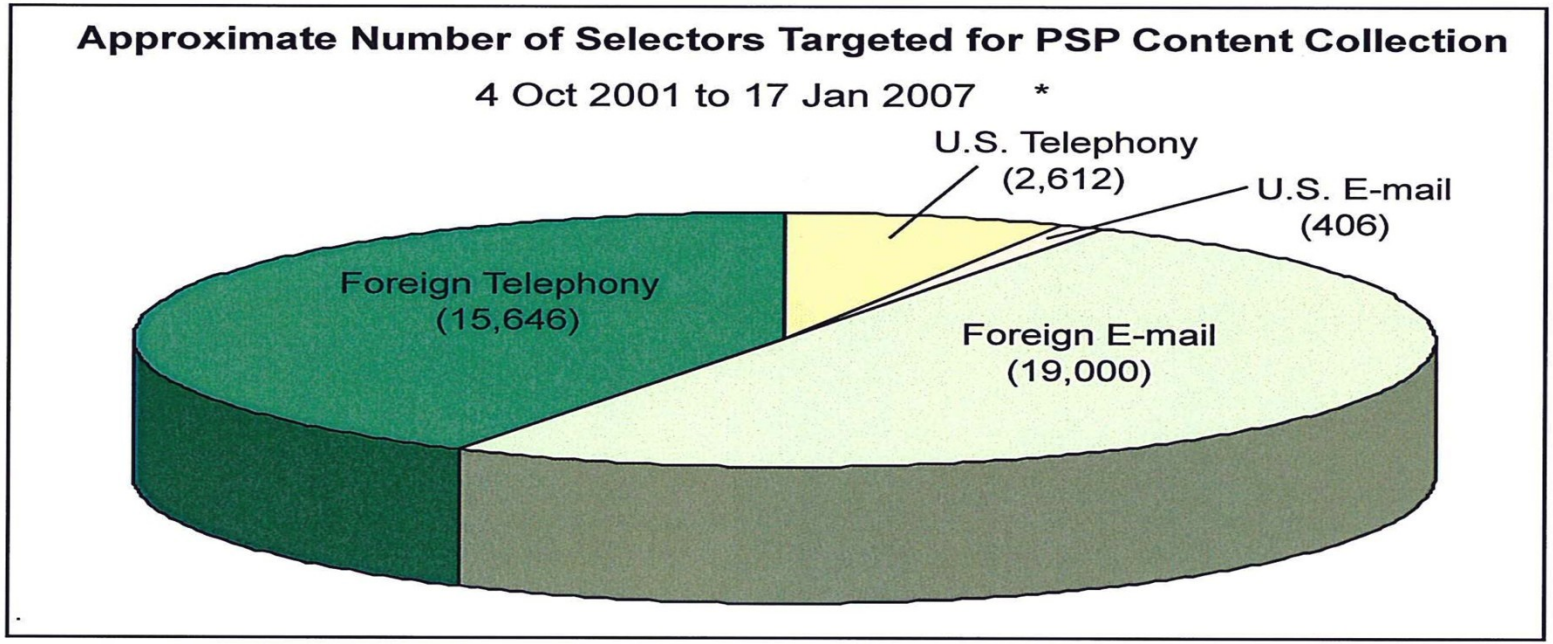
Data Mining a Haystack

- Risen & Lichtblau: Once the communications are acquired, NSA “comb[s] through large volumes of phone and internet traffic” in a “large data-mining operation.”
- John Yoo: “pluck out e-mails [and] phone calls that have a high likelihood of being terrorists’ communications.”

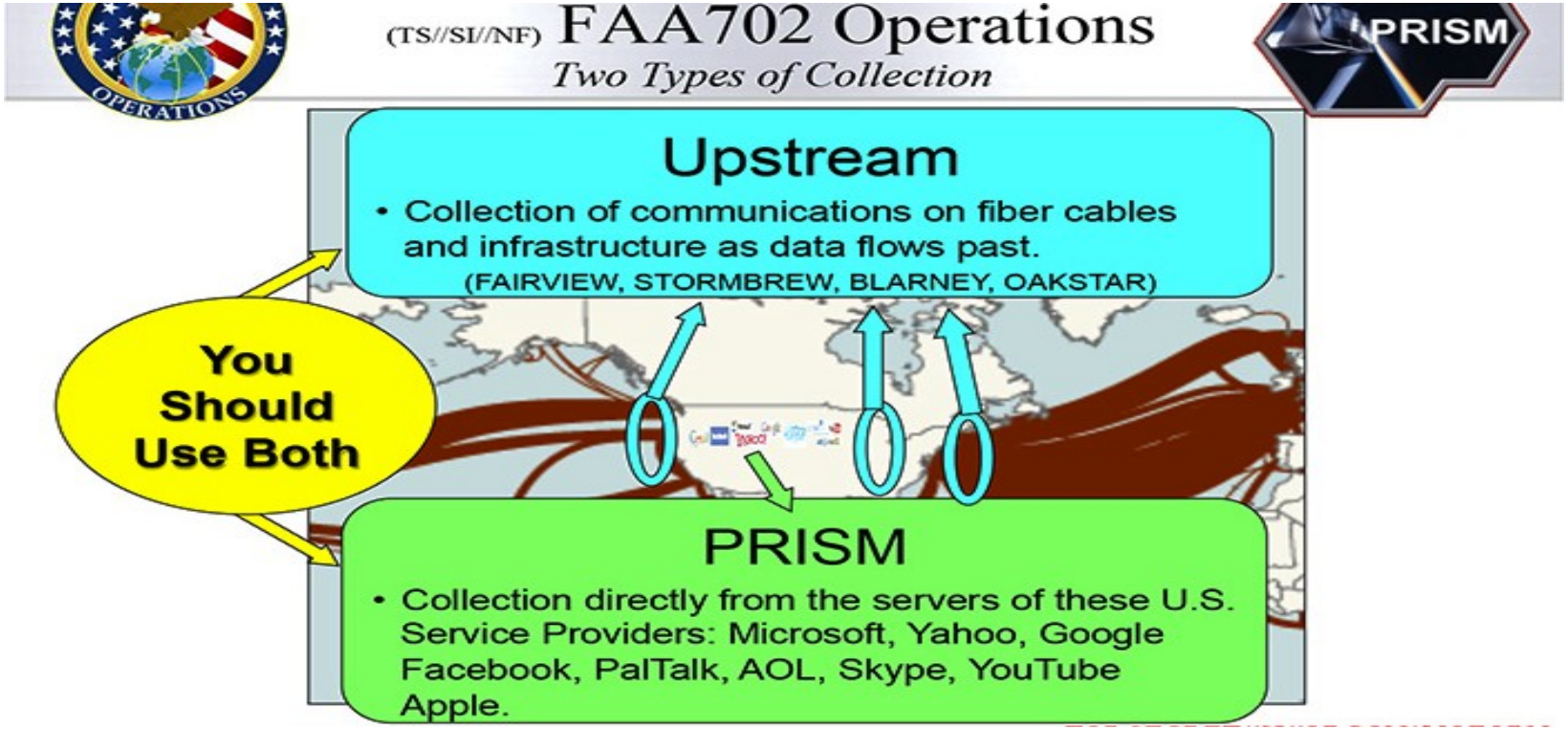
Holding without “Collecting”

- **DNI Clapper:** “think of a huge library … To me collection … would mean taking the books off the shelf.”
- **DNI McConnell:** “We may not know that it is in the database until we have some reason to go query that portion of the database**.”**

“Target” for “Collection”



FISAAA 702


(TS//SI//NF) FAA702 Operations
Two Types of Collection
PRISM
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.

FISA Amendments Act

- Section 702 was passed in 2008, and the U.S. relies on this for the collection of content
- Targeting and Minimization docs
  - Targeting 51% chance of foreign
  - Assumes foreign unless proved otherwise
  - Encrypted information kept forever
  - Can turn over U.S. person info in some circumstances

The Secret Court

Foreign Intelligence Surveillance Court

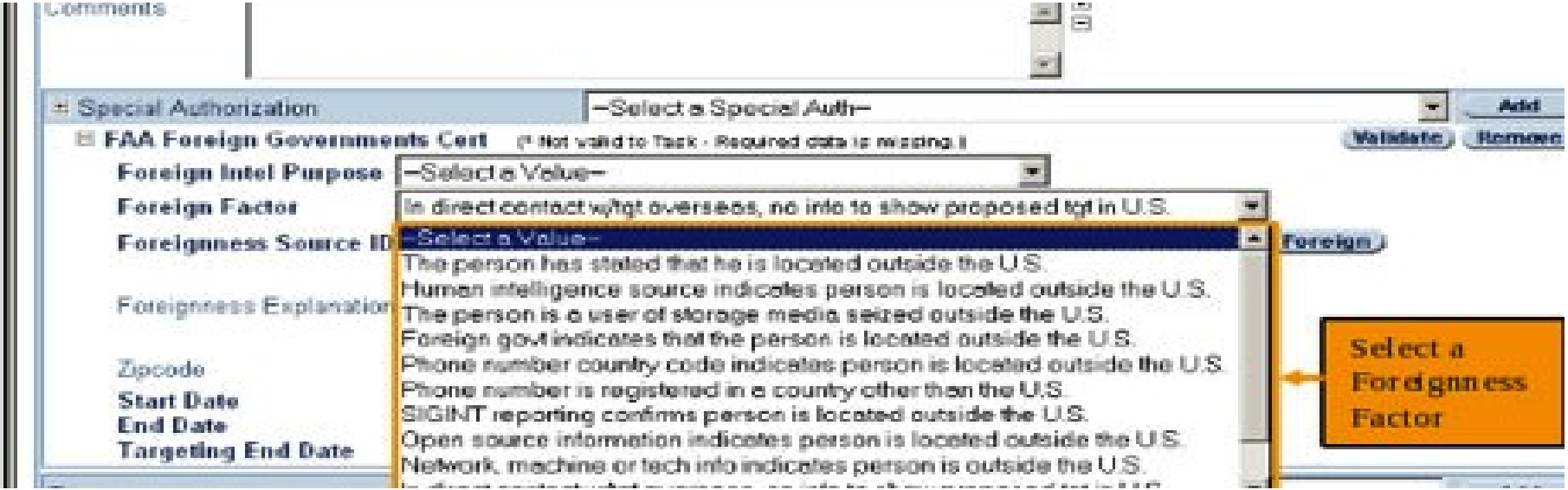
- Established and authorized under the Foreign Intelligence Surveillance Act
- Originally for surveillance against *foreign intelligence agents*
- Role massively expanded
- Approves procedures in secret rulings

Key Definitions

- “United States person”
  - U.S. Citizen or permanent resident
  - Group with “substantial number of U.S. persons”
  - U.S. corporation
- “Foreign intelligence information”
  - Attacks, terrorists, intelligence activity
  - OR relates to the “conduct of the foreign affairs of the United States”

XKeyScore Dashboard:

51% Foreign



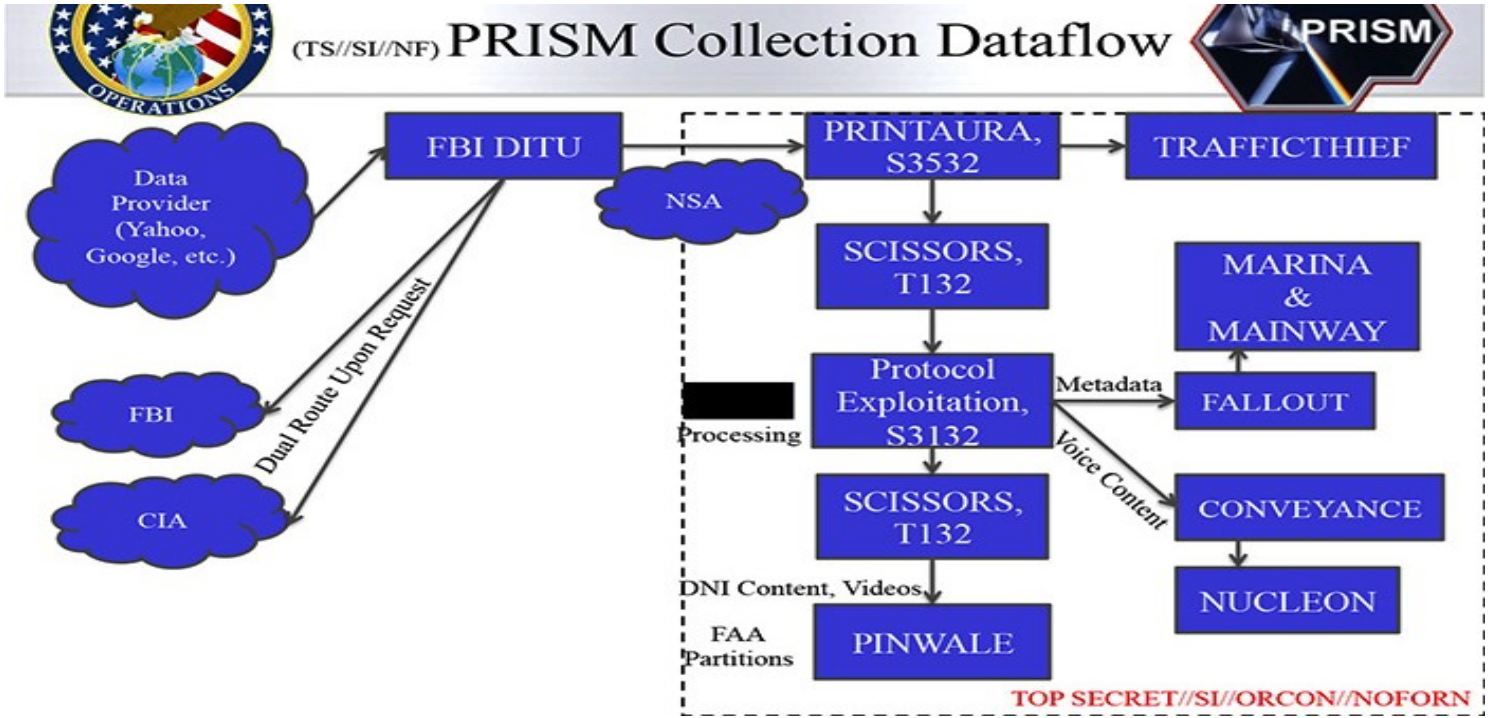
Targeting

1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

The website URL (aka "host) is entered in with a wildcard to account for "www" and "mail" other hosts.

To comply with USSID-18 you must AND that with some other information like an IP or country

Processing


(TS//SI//NF) PRISM Collection Dataflow
PRISM
Data Provider (Yahoo, Google, etc.)
FBI DITU
NSA
PRINTAURA, S3532
TRAFFICTHIEF
SCISSORS, T132
MARINA & MAINWAY
Protocol Exploitation, S3132
Metadata
FALLOUT
Processing
Voice Content
CONVEYANCE
SCISSORS, T132
NUCLEON
DNI Content, Videos
FAA Partitions
PINWALE
FBI
CIA
Dual Route Upon Request
TOP SECRET//SI//ORCON//NOFORN

Section 215 of Patriot Act

- Section 215 amended FISA to allow orders to produce “tangible things”
- Must be “relevant to an authorized investigation (other than a threat assessment)”
- No broader than a Grand Jury Subpoena

Verizon Order

- “all call detail records or ‘telephony metadata’ created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.”
- Originating and terminating phone nos., IMSI #, IMEI #, trunk identifier, telephone calling card numbers, and time and duration of call
- Renewed every 90 days

Just Metadata

- **President Obama:** “When it comes to telephone calls, nobody is listening to your telephone calls." Instead, the government was just "sifting through this so-called metadata.”
- **DNI Clapper:** “The program does not allow the Government to listen in on anyone’s phone calls. The information acquired does not include the content of any communications or the identity of any subscriber.”

Gov’t Attempts to Explain

- No identity
  - NSA may have access to phone books
- No location information
  - “under this program”
- Few hundred selectors
  - Three hops is a lot of people
- Legal basis
  - FISA court: analysis until after leaks
  - Federal courts split on constitutionality

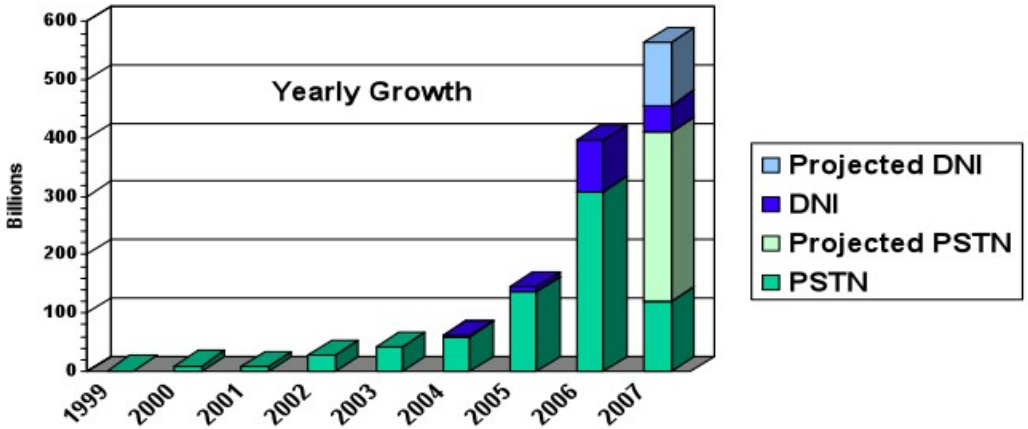
Why Metadata Matters

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

SECRET//COMINT//REL TO USA, FVEY//20320108

Large Scale Expansion of NSA Metadata Sharing

(S//SI//REL) Increases NSA communications metadata sharing from 50 billion records to 850+ billion records (grows by 1-2 billion records per day)



**(C//REL) Includes Call Events from 2nd Party SIGINT Partners (est. 126 Billion records)*

Executive Order 12333

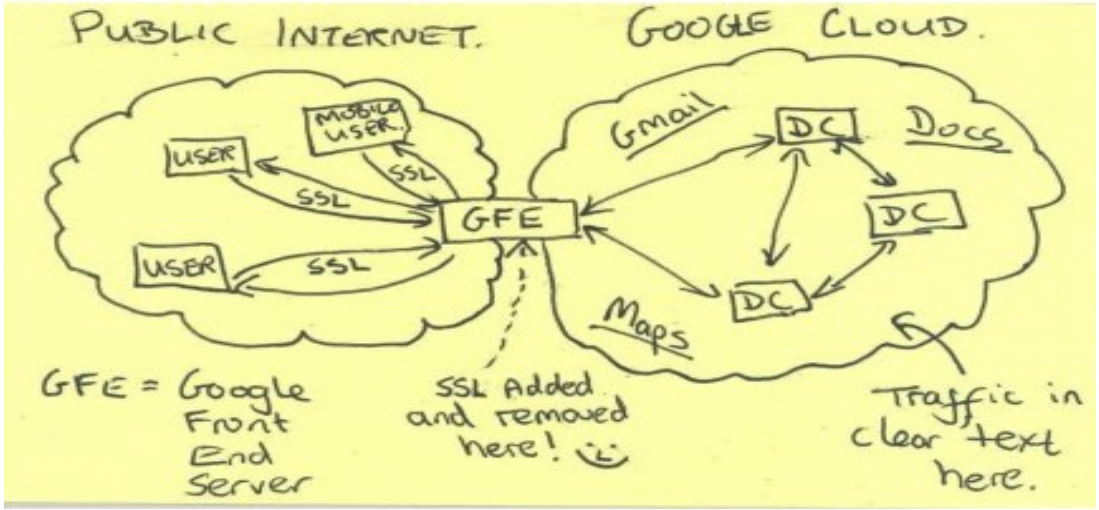
- Order by U.S. President on how the intelligence community should conduct surveillance
- Applies to spying outside U.S. law
- Not a substantive limit on surveillance
  - “the least intrusive collection techniques feasible within the United States or directed against United States persons abroad”
  - “in accordance with procedures”

Bulk Operations

- Phone calls
  - Millions of Spanish/French phone calls/month
    - NSA Dir. Alexander says French/Spanish intelligence agencies assisted
  - MYSTIC: Full take audio for Bahamas and Afganistan
- Financial records from SWIFT
  - 180 million records in 2011

MUSCULAR

- Since 2009, NSA infiltrated links between tech company data centers
  - Google
  - Yahoo
  - and more
- Works with UK GCHQ; routed to Ft. Meade



Encrypt All the Bits

- Responses to the smiley face
  - Dropbox, Facebook, Google, Microsoft, Twitter, Yahoo and others massively increased encryption
  - Email encryption of billions of messages
  - Full page ads opposing bulk collection

Crypto Survey Results

	Encrypts data center links	Supports HTTPS	HTTPS Strict (HSTS)	Forward Secrecy	STARTTLS
amazon	undetermined	limited	✗	undetermined	✓
	undetermined	✓ (iCloud)	✗	undetermined	✗ (me.com, mac.com)
at&t	undetermined	undetermined	✗	undetermined	✗ (att.net)
COMCAST	undetermined	undetermined	✗	undetermined	✗ (comcast.net)
Dropbox	✓	✓	✓	✓	✓
facebook	✓ in progress	✓	✓ planned	✓	✓ (in progress, facebook.com)
foursquare	undetermined	✓	✓	undetermined	✗
Google	✓	✓	in progress for select domains, see notes	✓	✓
LinkedIn	✗ contemplating	✓ planned 2014	✓ planned 2014	✓ planned 2014	✗ contemplating
Microsoft	✓ in progress	✓	✓ planned	✓ in progress	✓ (planned, outlook.com)
myspace	undetermined	✓	✗	undetermined	✗
Sonic.net	✓	✓	✓	✓ in progress	✓
	✓	✓	✓	✓ in progress	✓
	✓	✓	✓	✓	✓
tumblr.	✗	✓ planned Q2 2014	✓ planned 2014	✓	✗
verizon	undetermined	undetermined	✗	undetermined	✗ (verizon.net)
WordPress	undetermined	available	✗	undetermined	✗
YAHOO!	✓	✓ default for Mail; planned 2014 for all	✓ planned 2014	✓ yahoo.com: planned 2014 for all	✓ (yahoo.com)

Notes: The information in this chart comes from several sources: the companies who responded to our survey questions; information we have determined by independently examining the listed websites and services, and published reports. Some of the surveyed companies did not respond to the survey.

Recognizing that some of these steps will take time to implement, we gave credit to companies that either (1) have implemented or (2) have concrete plans to implement the listed encrytion process, as noted.

For STARTTLS, the red and grey shading indicates whether or not the company is a major email service provider. While encourage all companies to implement STARTTLS, even if they only provide email for their own employees, the issue is most critical for companies that provide email communications to the public.

Google implements HSTS on accounts.google.com for all browsers that support HSTS, which at the time of this writing are Chrome, Chromium, Firefox, Opera, and Safari. HSTS on other Google domains is only functional in Chrome, Chromium, and Safari.

CO-TRAVELLER

- The NSA obtains location information from cell tower triangulation, wifi, GPS
- Automating guilt by association
  - Correlate patterns of movement
  - Speed and trajectory
- Looking for disposable cellphones
  - Switching on, calling, and then switching off
  - New phone connects after another phone stops

Targeted Operations

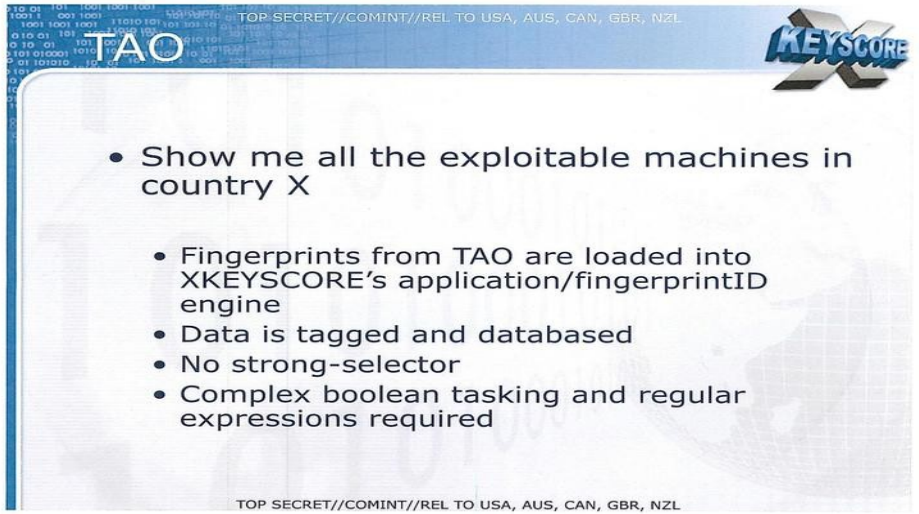
- “Special Collection Service”
  - Angela Merkel’s cell phone since 2002
  - American diplomatic buildings
- Spied on at least 35 world leaders
  - Mexico, Brazil, senior EU officials
- Economic spying
  - Petrobras
  - 2010 Group of 20 summit in Toronto.

The Flying Pig in the Middle

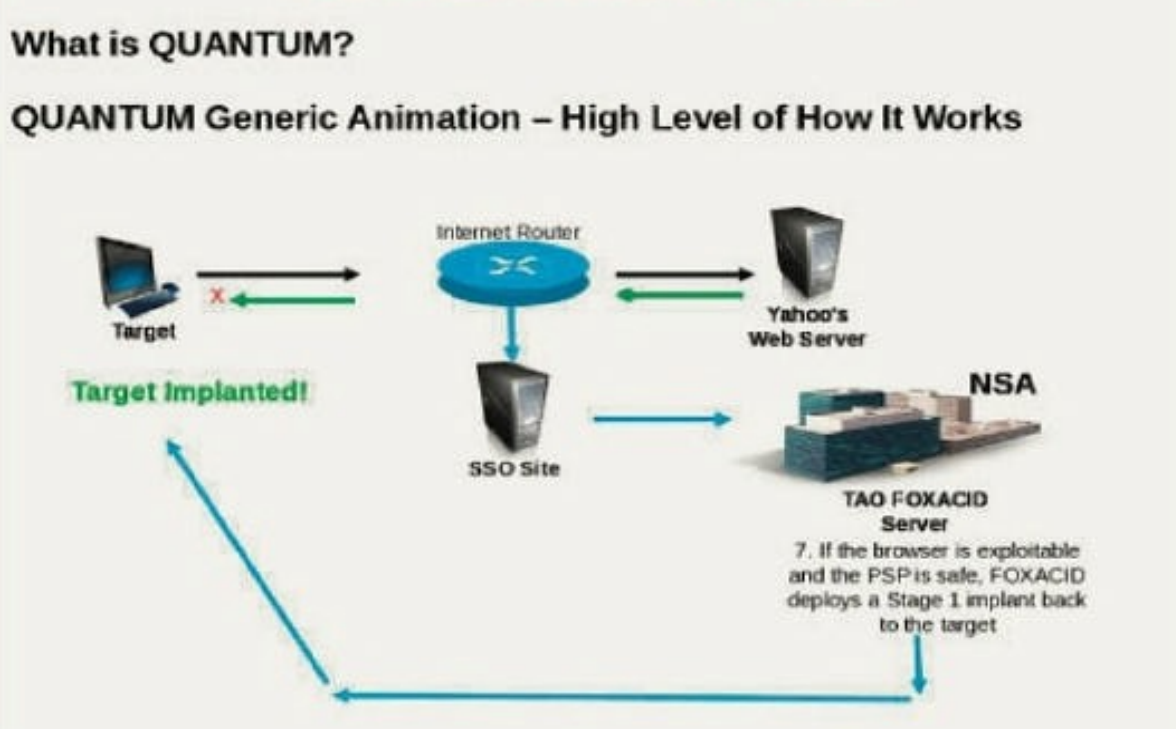
- Instead of cracking SSL: pwn router, impersonate certificates
- GCHQ operates FLYINGPIG to organize SSL certificates

The TAO of the NSA

- Office of Tailored Access Operations
- 231 ops in 2011
  - Mexican President's email, OPEC
  - Many way to target – Google PREF cookies



QUANTUM INSERT



BULLRUN – It's Sabotage!

- $250 million/year program to decrypt
  - "Insert vulnerabilities"
  - "covertly influence and/or overtly leverage"
  - "influence policies, standards and specifications for commercial public key technologies"
    - NSA paid $10 million to RSA to make default
- 2010: breakthrough for "vast amounts" of data

- Efforts to fingerprint and exploit users via Firefox
  - EGOTISTICALGIRAFFE exploits Firefox bugs
  - FBI used same technique on Freedom Host (.onion)
- Core security appears intact
  - Use fingerprints on Tor related traffic (TAILs and Linux Journal)

Abuses of Power

- Audit found: “2,776 incidents (/year) of unauthorized collection, storage, access to or distribution of legally protected communications” in D.C./Ft. Meade alone
  - Misread country code 20 as area code 202 and grabbed all the calls from Washington D.C., instead of from Egypt.
  - The “202” area code collection was deemed irrelevant: “The issue pertained to Metadata ONLY so there were no defects to report”
- LOVEINT – tracking ex-lovers, spouses
- Monitored email of prominent Muslim-Americans

Discrediting Radicalizers

- The NSA is gathering evidence of “radicalizer’s” visits to porn sites
  - Also “online promiscuity” and “deceitful use of funds”
- “Radicalizers” are people who speak on their “extremist” views online
  - Seeking to discredit the message

Reform: What Can Be Done

- PCLOB:
  - Recommend US end bulk collection: "lacks a viable legal foundation," ineffective.
- President's Review Group
  - 40 recommendations for promoting transparency, left open the door for future mass surveillance

Litigation

- Phone records cases
  - Klayman v. Obama (DC Circuit)
  - ACLU v. Clapper (2nd Circuit)
  - Smith v. Obama (9th Circuit)
  - First Unitarian Church of Los Angeles v. NSA
- Full cases
  - Jewel v. NSA (since 2008!)
- FOIA

STOP WATCHING US

Legislation and Activism

- Built broad coalition
  - Over half-million petition signatures to U.S. Congress
  - Interpret for public
- USA Freedom
  - Support, but its small

International

- 13 Principles (necessaryandproportionate.net)
  - Over 300 organizations worldwide
  - Basis for UN Resolution
    - You can sign!
- Legal processes
  - ECHR complaint; OAS hearing

Technology

- Still to be done: **Ease of use**
  - End-to-end in phones, IM, text messages
  - Securify the interwebs, social networking, disk drives, flash memory, “data at rest”
- Shore up crypto tools against sabotage

You

- Pay attention, Share, Vote
  - Activism is an open source project
- Use the tools – “I am Spartacus”
- Build the tools for a future you would want to live in

Questions?

Kurt Opsahl

Deputy General Counsel, EFF

@kurtopsahl

kurt@eff.org

More info at https://eff.org/nsa-spying