Through a PRISM, Darkly

Kurt Opsahl
Senior Staff Attorney, 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

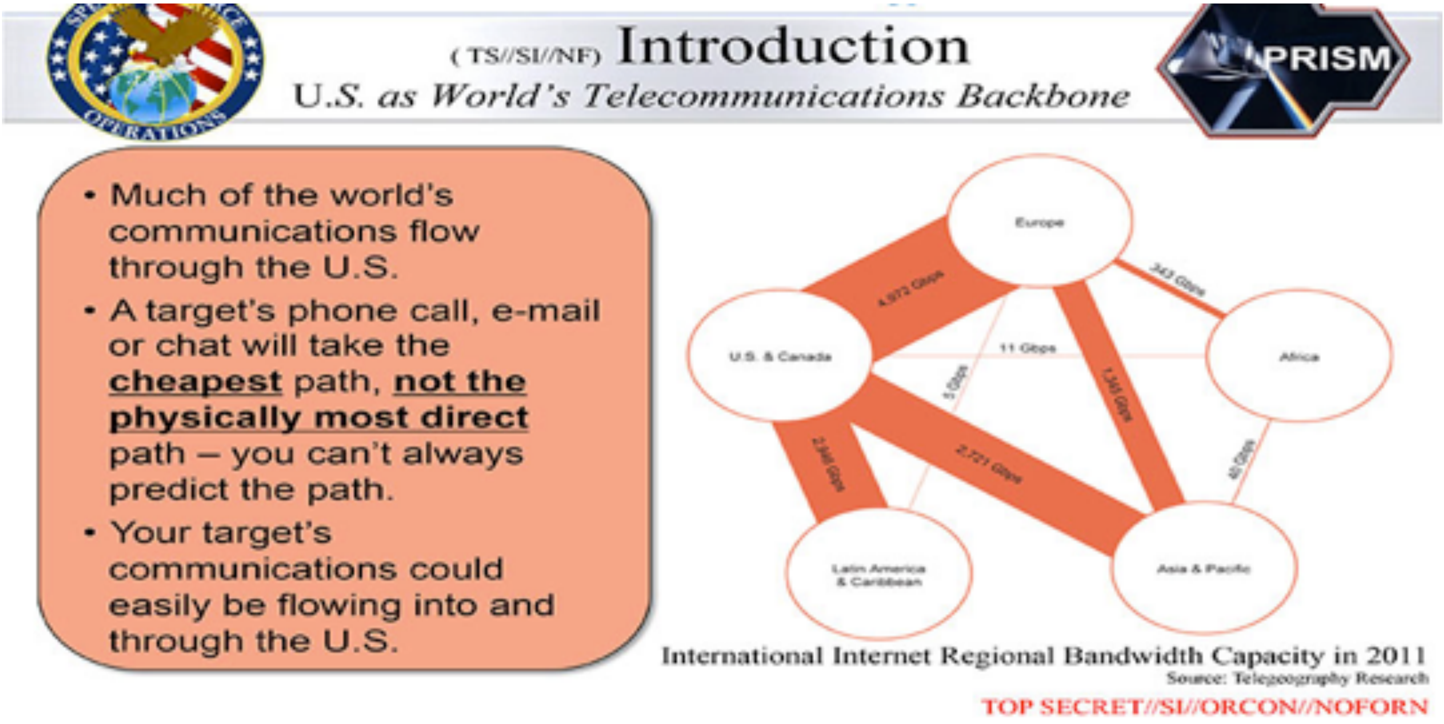
- After 9/11, President Bush unleashed the full power of the NSA
- A subset of the President’s Surveillance Program was later labeled the TSP
- PSP was without the court-approved warrants ordinarily required for domestic

Montag, 27. November 2017

The Eye of Sauron unleashed.

TSP was a tautology – defined as the part of the PSP that surveilled terrorists.

US Companies Sit on Wire



(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

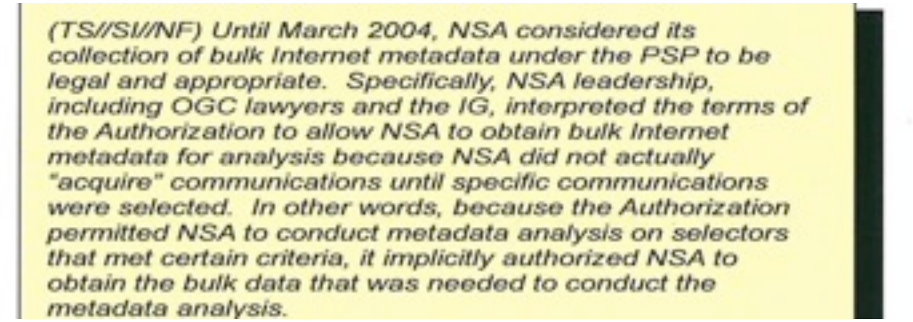
TOP SECRET//SI//ORCON//NOFORN

Montag, 27. November 2017

The PSP took advantage of being on the wire for most communications – even Asia to Africa would likely go through the United States.

Showdown at the Hospital

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



(TS//SI//NF) Until March 2004, NSA considered its collection of bulk Internet metadata under the PSP to be legal and appropriate. Specifically, NSA leadership, including OGC lawyers and the IG, interpreted the terms of the Authorization to allow NSA to obtain bulk Internet metadata for analysis because NSA did not actually "acquire" communications until specific communications were selected. In other words, because the Authorization permitted NSA to conduct metadata analysis on selectors that met certain criteria, it implicitly authorized NSA to obtain the bulk data that was needed to conduct the metadata analysis.

- Gonzales and Comey race to hospital

Montag, 27. November 2017

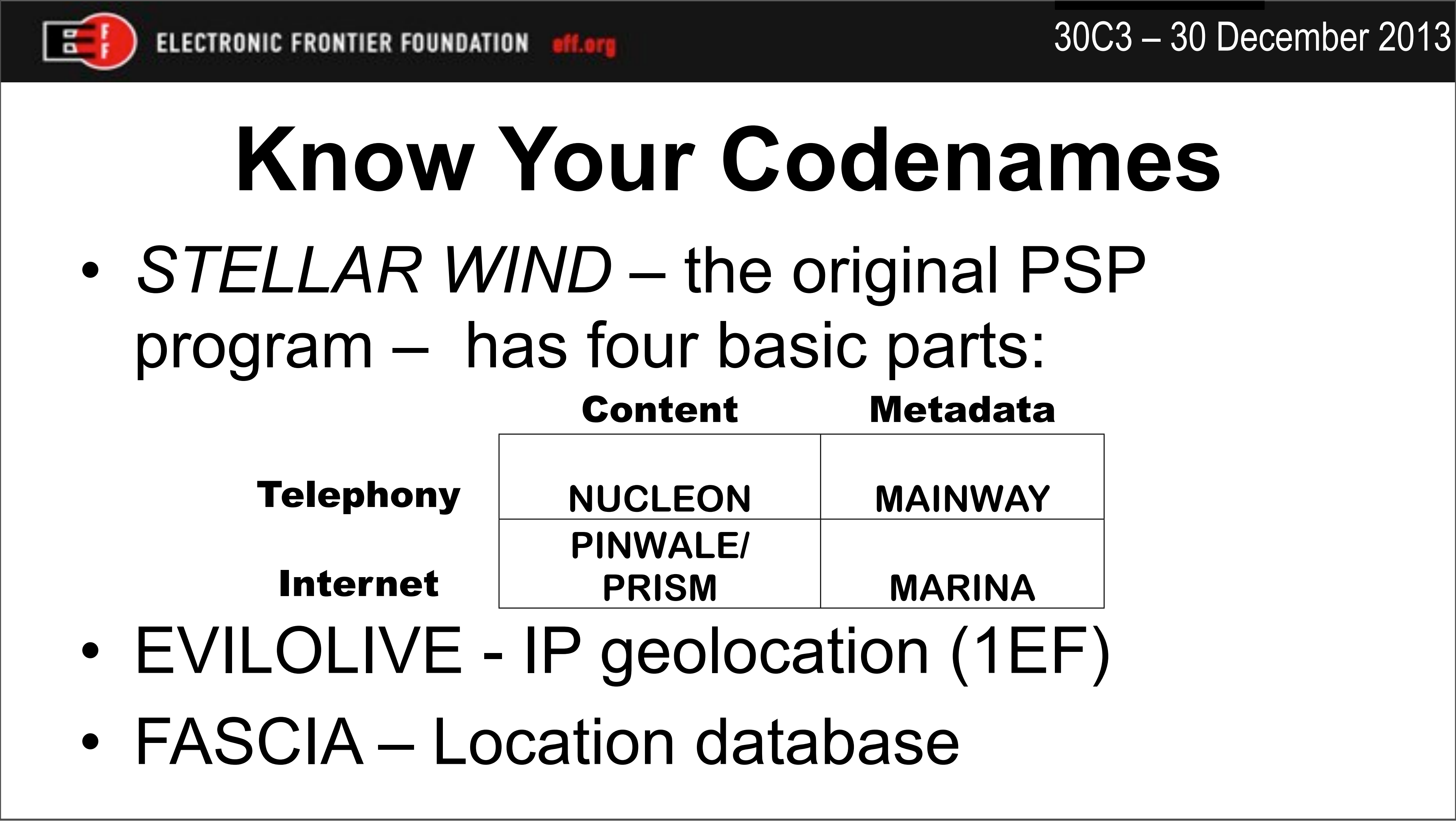
Acquisition word game.

Comey says no lawyer would buy this theory. Addington says I’m a lawyer. “No good lawyer.”

Comey is now the FBI Director.

Public Disclosure

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



Know Your Codenames

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

	Content	Metadata
Telephony	NUCLEON	MAINWAY
Internet	PINWALE/ PRISM	MARINA

- EVILOLIVE - IP geolocation (1EF)
- FASCIA – Location database

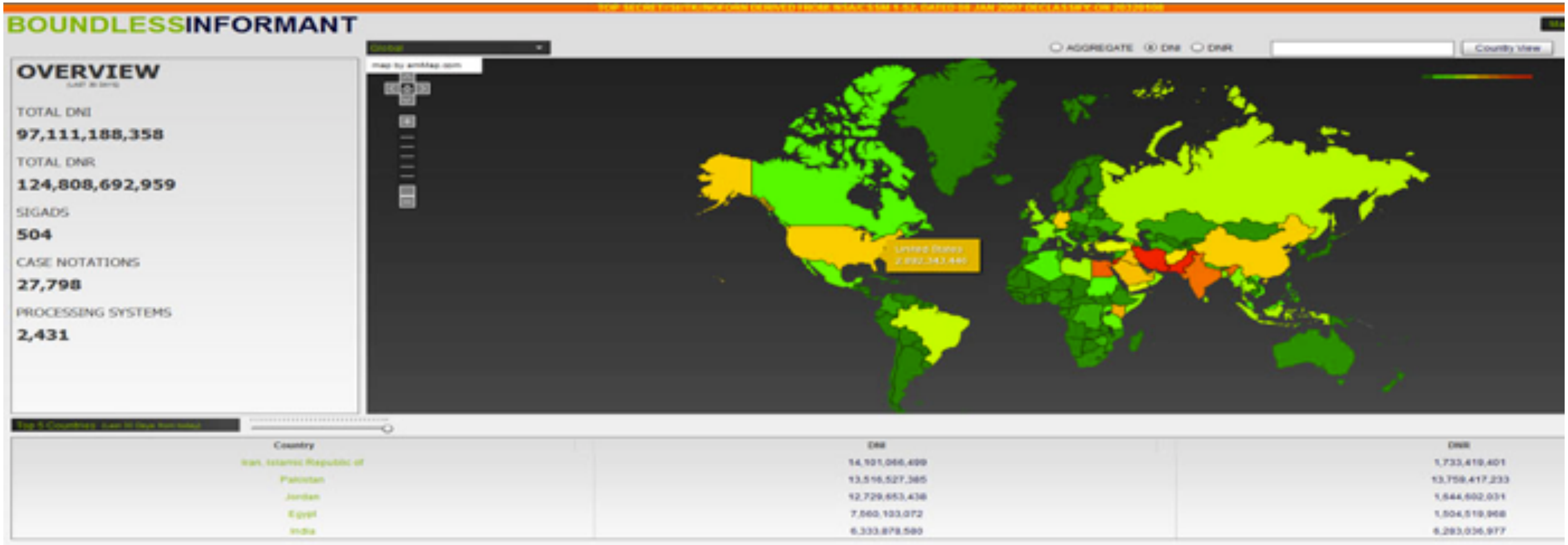
Montag, 27. November 2017

EvilOlive – palindrome, and anagram for I Love Evil. 1EF is one end foreign.

More information in these databases.

"The Marina metadata application tracks a user's browser experience, gathers contact information/content

Boundless indeed



TOP SECRET//SI//NOFORN DERIVED FROM NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON 20320108

BOUNDLESSINFORMANT

Global

○ AGGREGATE ⦿ DNI ○ DNR

Country View

OVERVIEW
(LAST 30 DAYS)

TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

SIGADS
504

CASE NOTATIONS
27,798

PROCESSING SYSTEMS
2,431

Top 5 Countries (Last 30 Days from today)

Country	DNI	DNR
Iran, Islamic Republic of	14,101,066,499	1,733,419,401
Pakistan	13,516,527,365	13,759,417,233
Jordan	12,729,653,436	1,644,602,031
Egypt	7,560,103,072	1,504,519,968
India	6,333,878,580	6,283,036,977

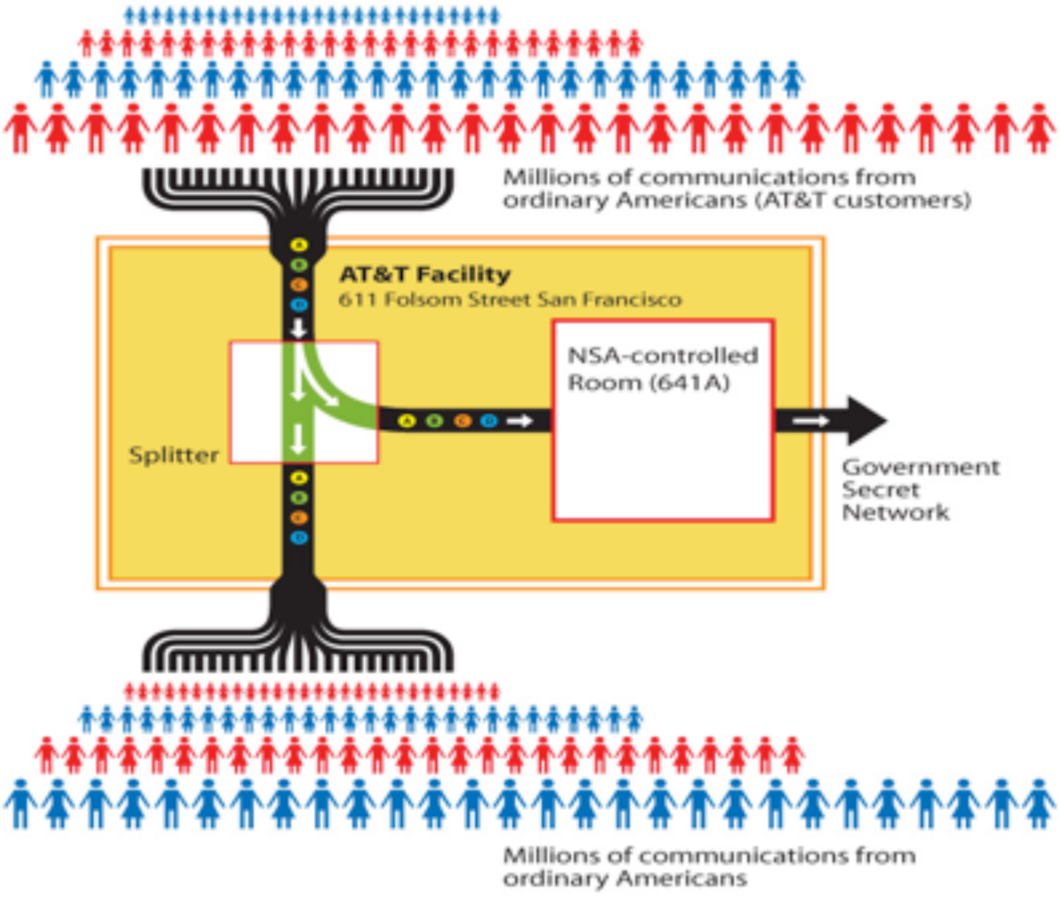
analysis and data visualization system with records from 504 separate DNR and DNI collection sources (SIGADs).

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)

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 communications from ordinary Americans (AT&T customers)

AT&T Facility

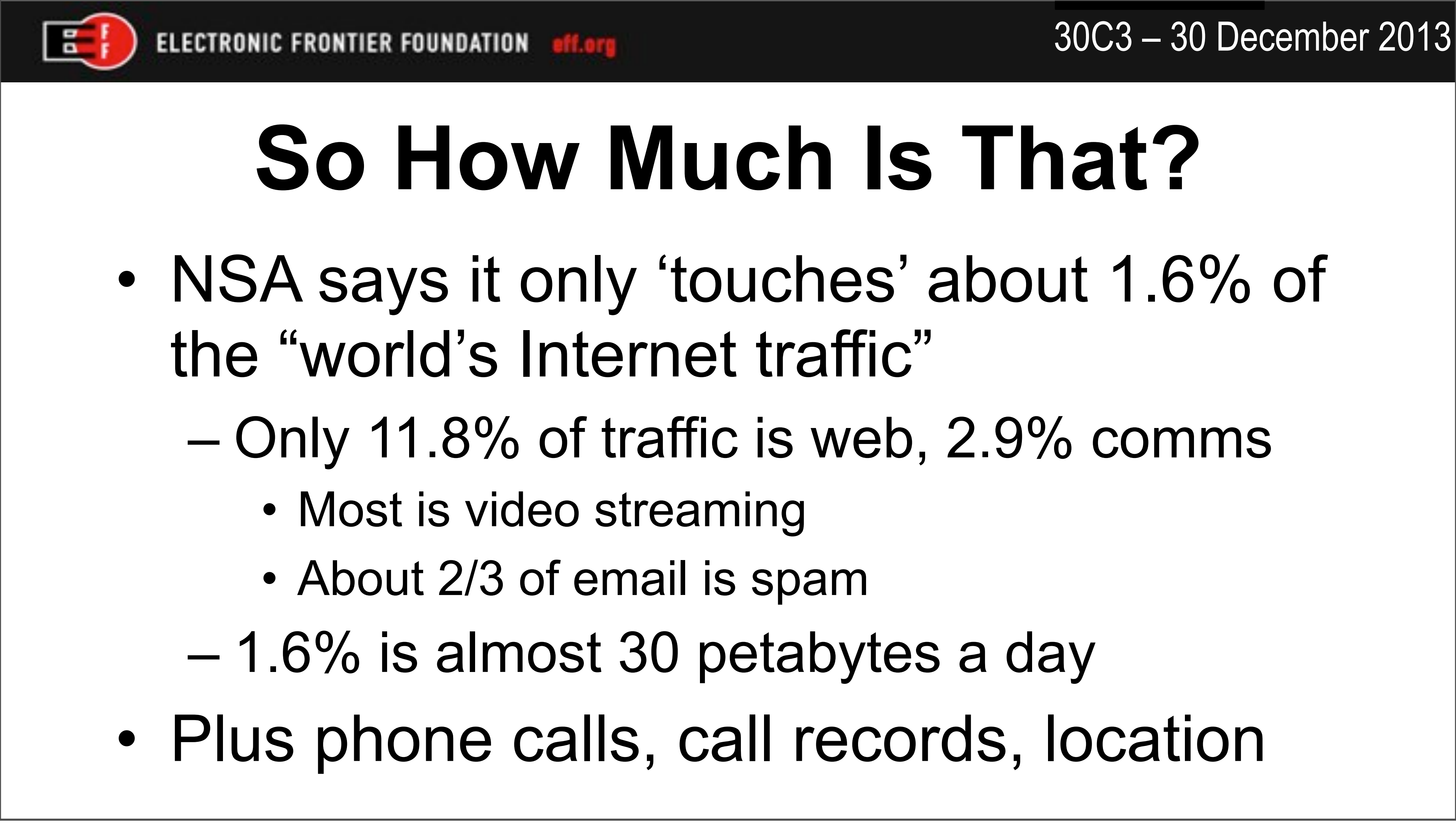
611 Folsom Street San Francisco

NSA-controlled Room (641A)

Splitter

Government Secret Network

Millions of communications from ordinary Americans



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

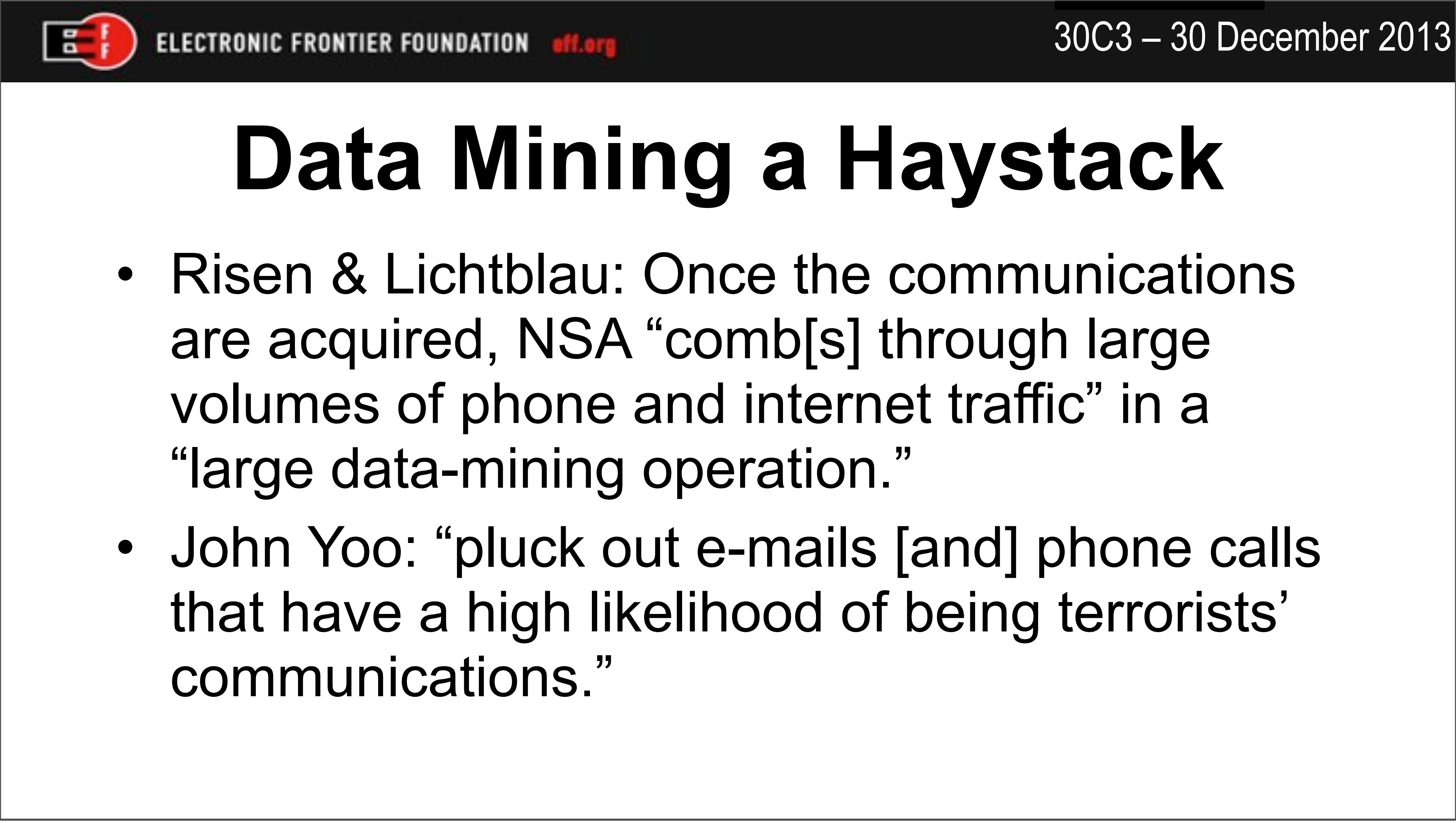
Montag, 27. November 2017

YouTube, Lovefilm, BBC’s iPlayer, NetFlix

Utah Data Facility

- 100k ft^2 (9.2k m^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 (464 m^2) to store and process year of *just U.S.* phone calls

Photo by Swilsonmc CC-BY-SA 3.0 Unported

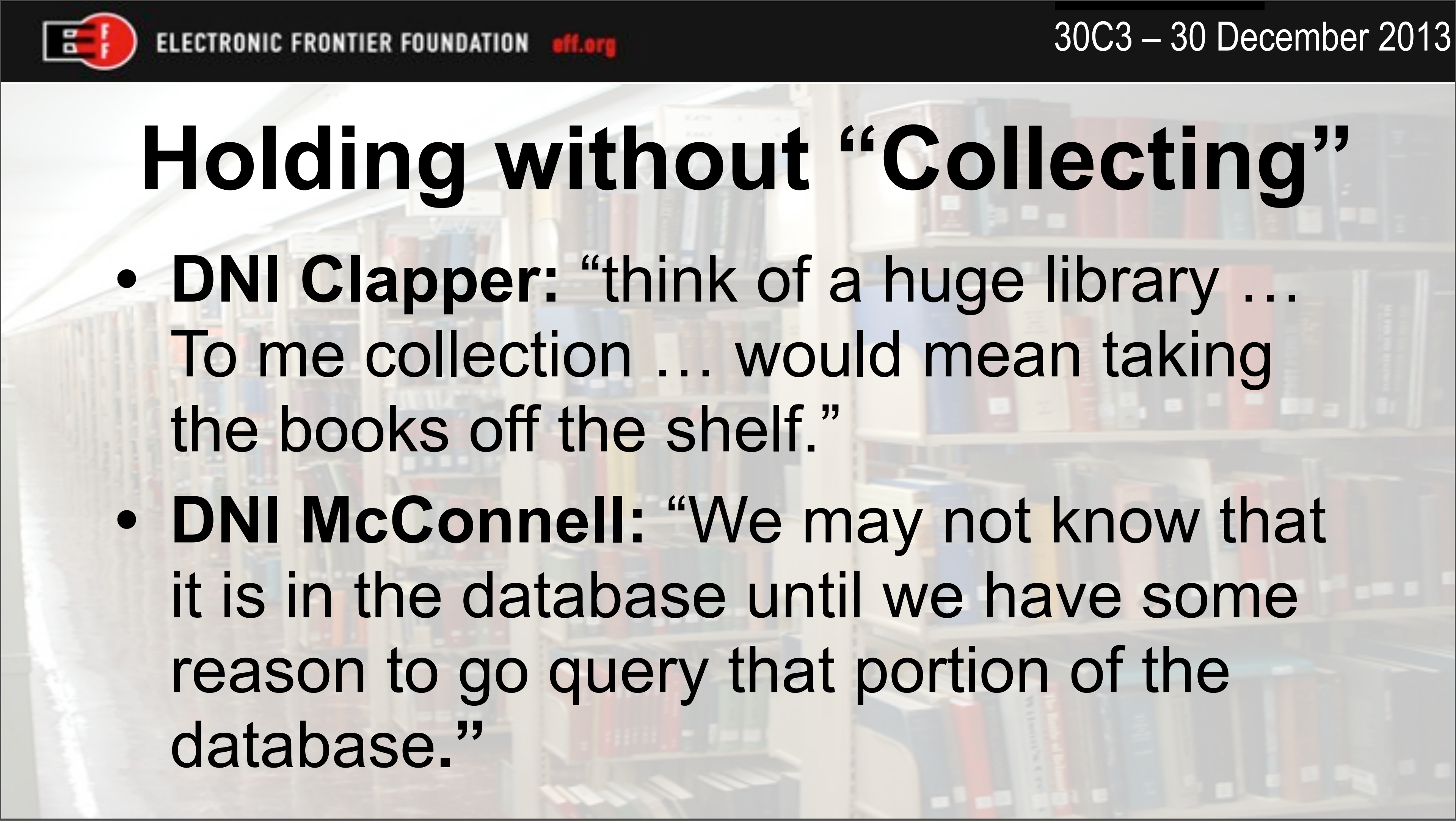


Data Mining a Haystack

- 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.”

Montag, 27. November 2017

Risen & Lichtblau – NYT reporters. John Yoo – chief legal architect of Program



Holding without “Collecting”

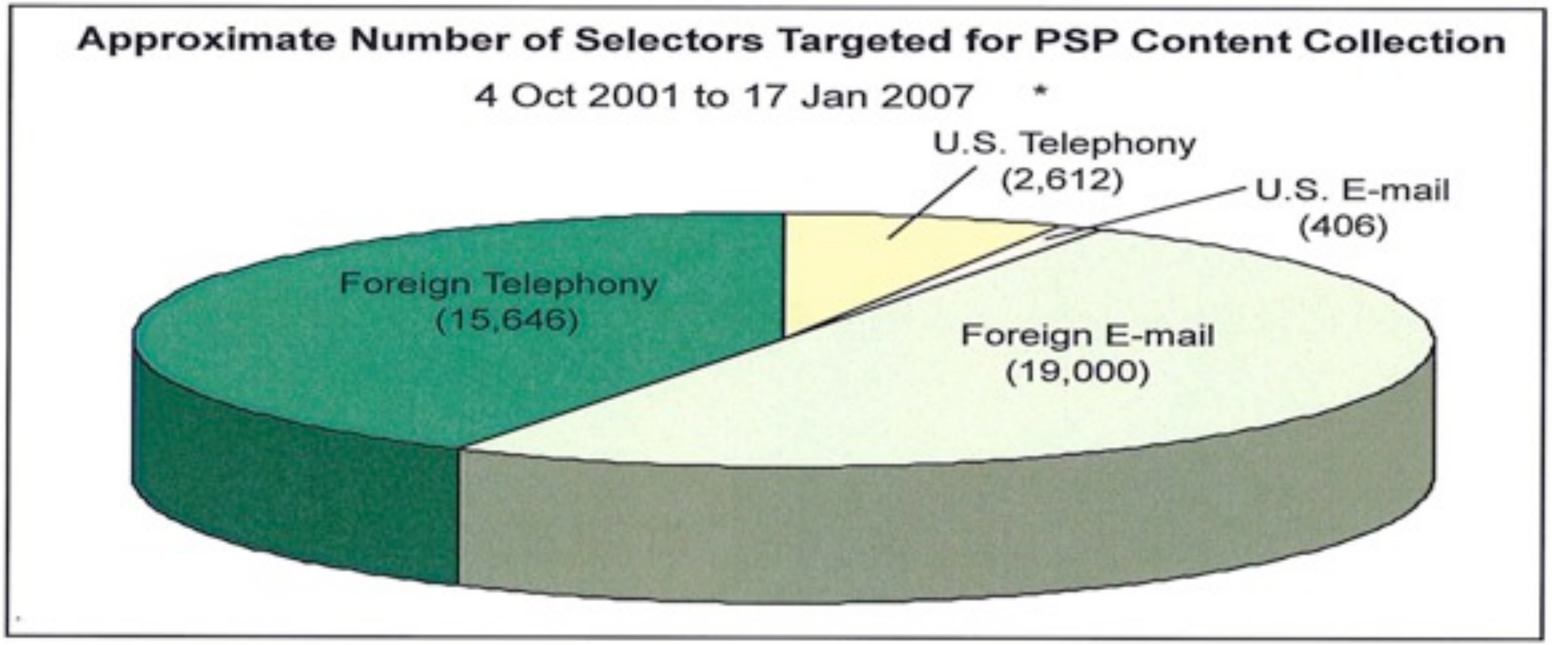
- **DNI Clapper:** “think of a huge library … To me collection … would mean taking the books off the shelf.”
- **DNI McConnell:** “We may not know that it is in the database until we have some reason to go query that portion of the database.”

Montag, 27. November 2017

Clapper interview with NBC

McConnell responding on context of question on how much U.S. person data is in the DB.

“Target” for “Collection”



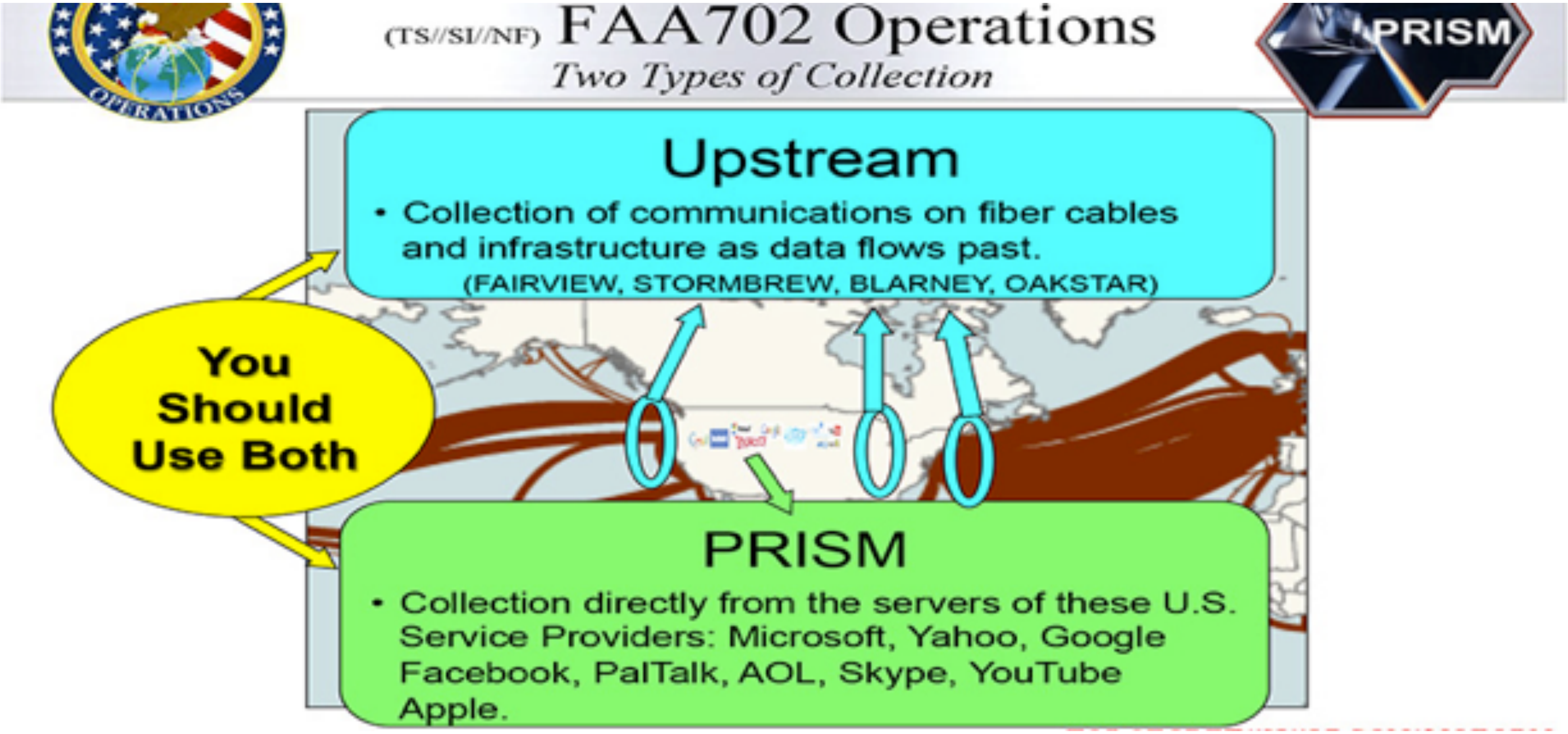
Approximate Number of Selectors Targeted for PSP Content Collection

4 Oct 2001 to 17 Jan 2007 *

Montag, 27. November 2017

Collection – word games. Seem like small numbers, but actually quite a lot

FISAAA 702



(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.

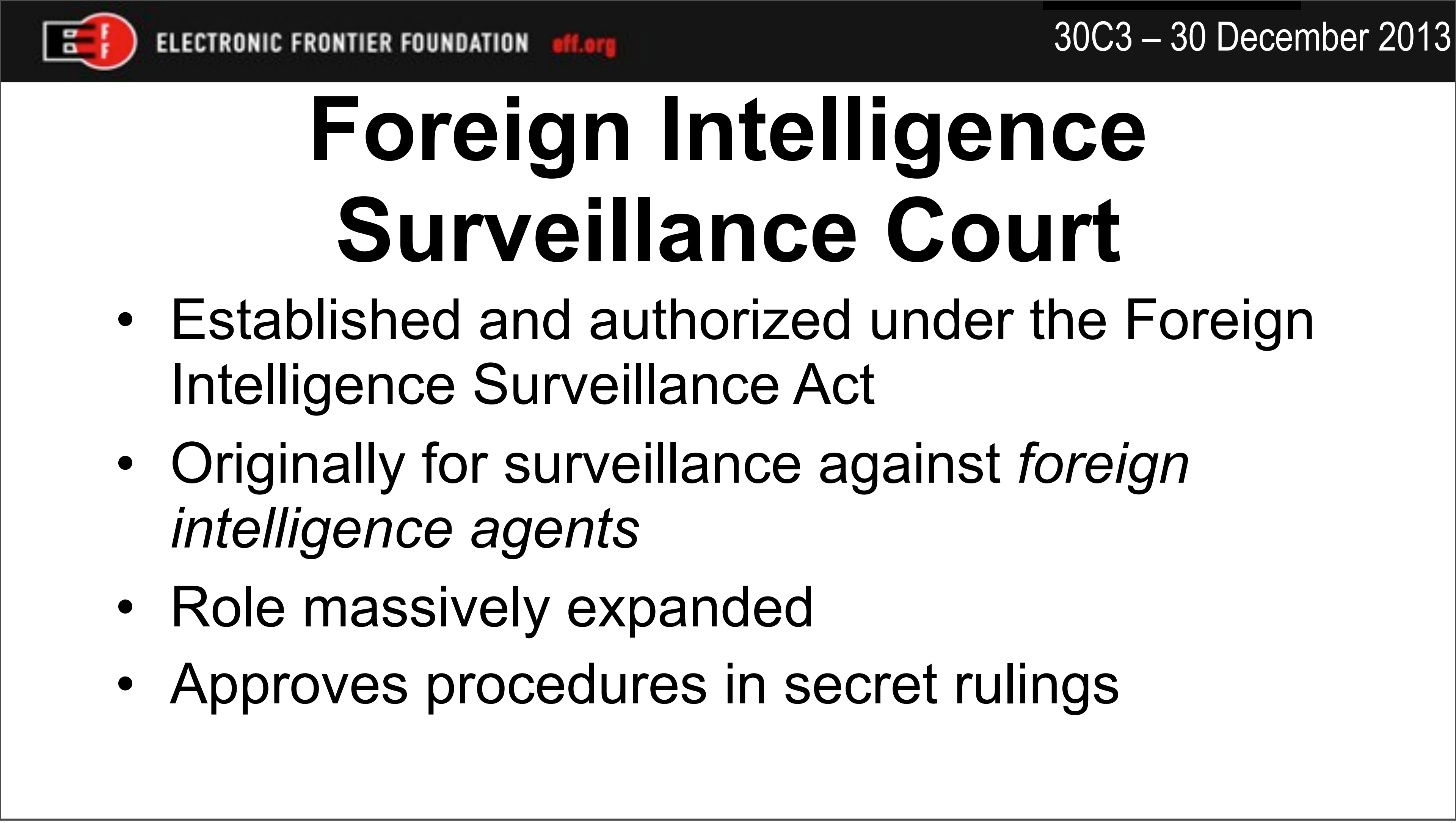
FISA Amendments Act

- 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

The Secret Court

Montag, 27. November 2017

Meets in SCIF. First at DOJ, then at DC district court.



Foreign Intelligence Surveillance Court

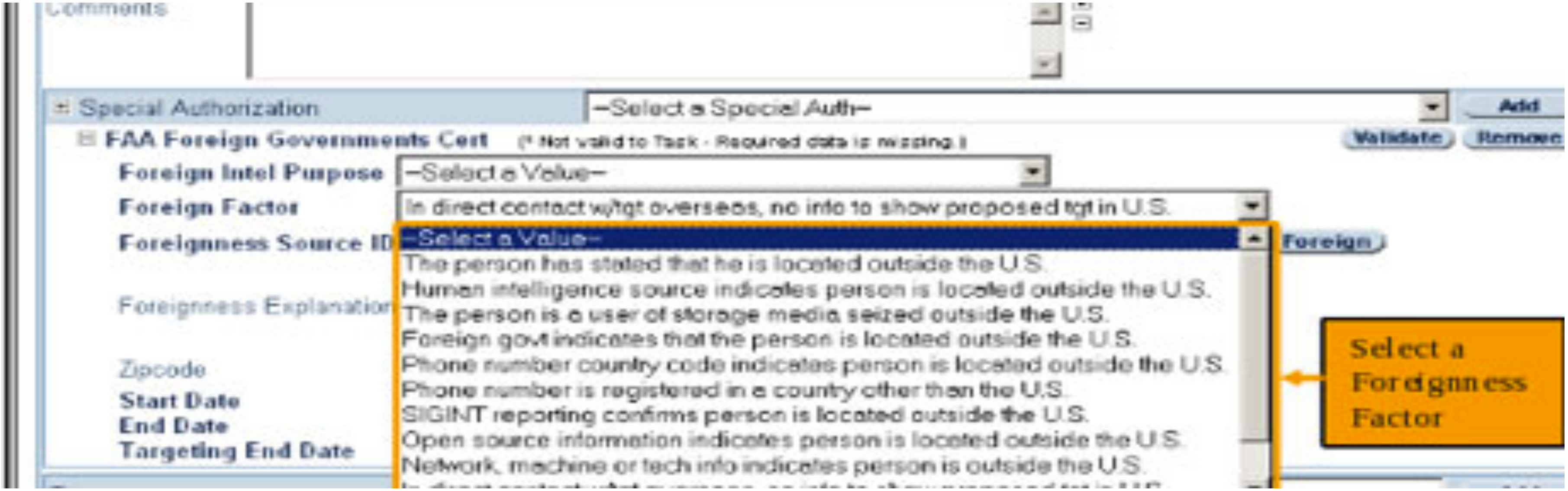
- Established and authorized under the Foreign Intelligence Surveillance Act
- Originally for surveillance against *foreign intelligence agents*
- Role massively expanded
- Approves procedures in secret rulings

Chief Judge Walton: “The FISC does not have the capacity to investigate issues of noncompliance, and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders.”

Key Definitions

- “United States person”
  - US 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:



Special Authorization: —Select a Special Auth—

FAA Foreign Governments Cert (* Not valid to Task - Required data is missing.)

Foreign Intel Purpose: —Select a Value—

Foreign Factor: In direct contact w/tgt overseas, no info to show proposed tgt in U.S.

Foreignness Source ID:

- —Select a Value—
- The person has stated that he is located outside the U.S.
- Human intelligence source indicates person is located outside the U.S.
- The person is a user of storage media seized outside the U.S.
- Foreign govt indicates that the person is located outside the U.S.
- Phone number country code indicates person is located outside the U.S.
- Phone number is registered in a country other than the U.S.
- SIGINT reporting confirms person is located outside the U.S.
- Open source information indicates person is located outside the U.S.
- Network, machine or tech info indicates person is outside the U.S.

Foreignness Explanation

Zipcode

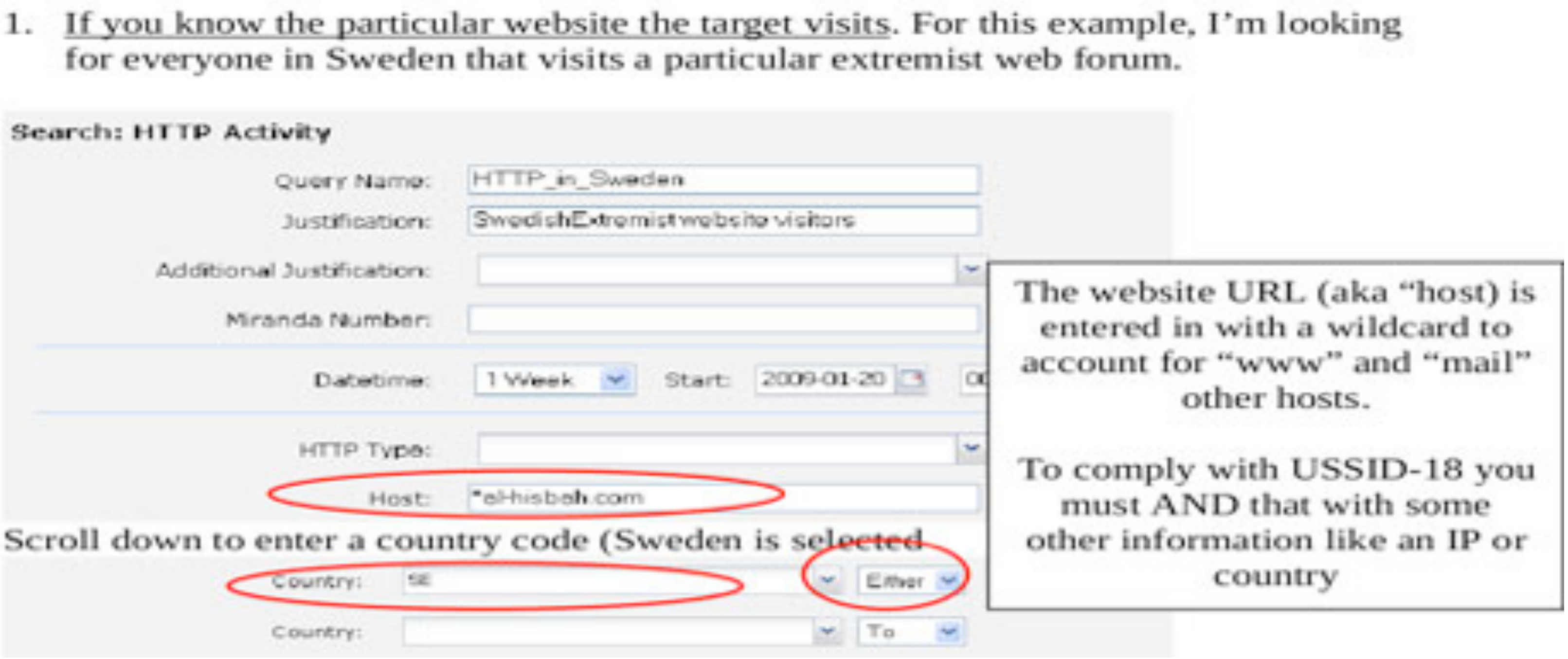
Start Date

End Date

Targeting End Date

Select a Foreignness Factor

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.

Search: HTTP Activity

Query Name: HTTP_in_Sweden
Justification: SwedishExtremistwebsite visitors
Additional Justification:
Miranda Number:
Datetime: 1 Week Start: 2009-01-20 0

HTTP Type:
Host: *elHisbah.com

Scroll down to enter a country code (Sweden is selected

Country: SE Either
Country: To

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

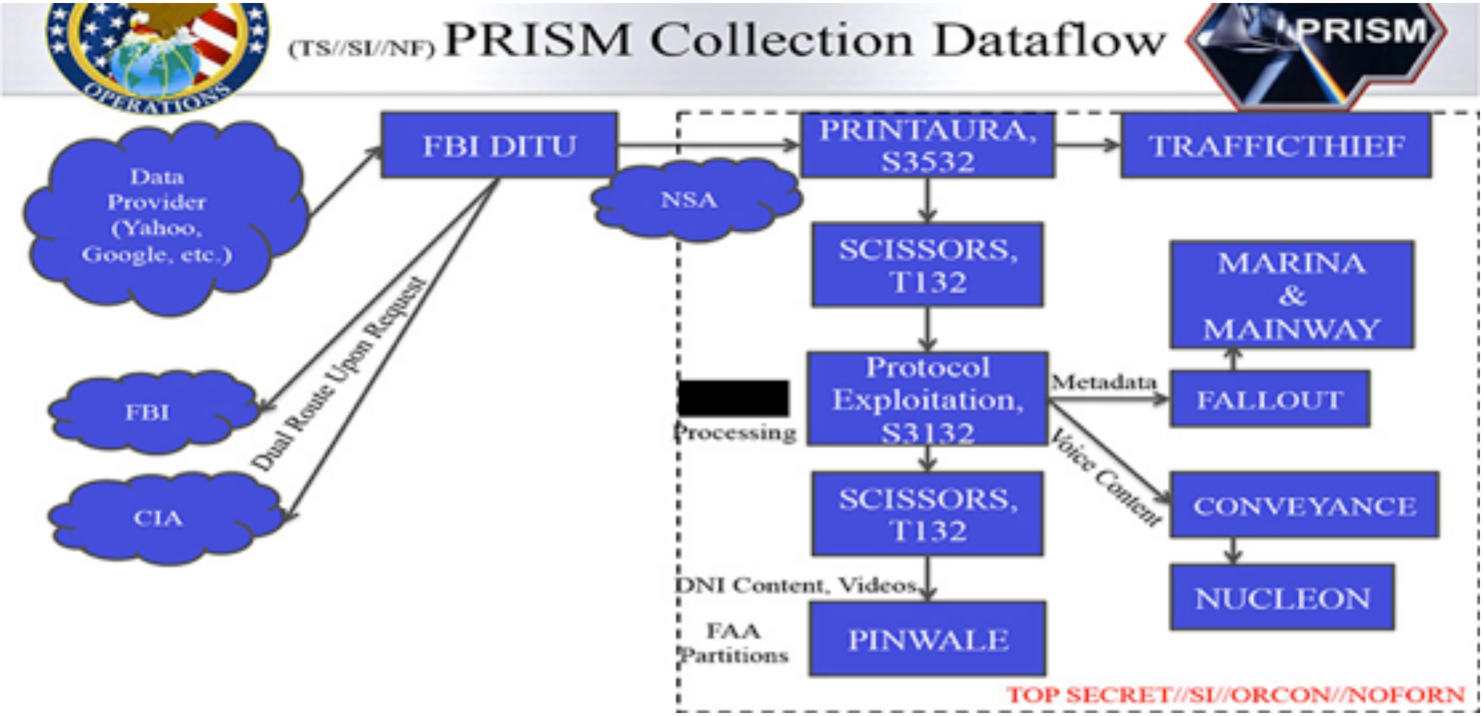
To comply with USSID-18 you must AND that with some other information like an IP or country

Montag, 27. November 2017

One selection searches lots of info

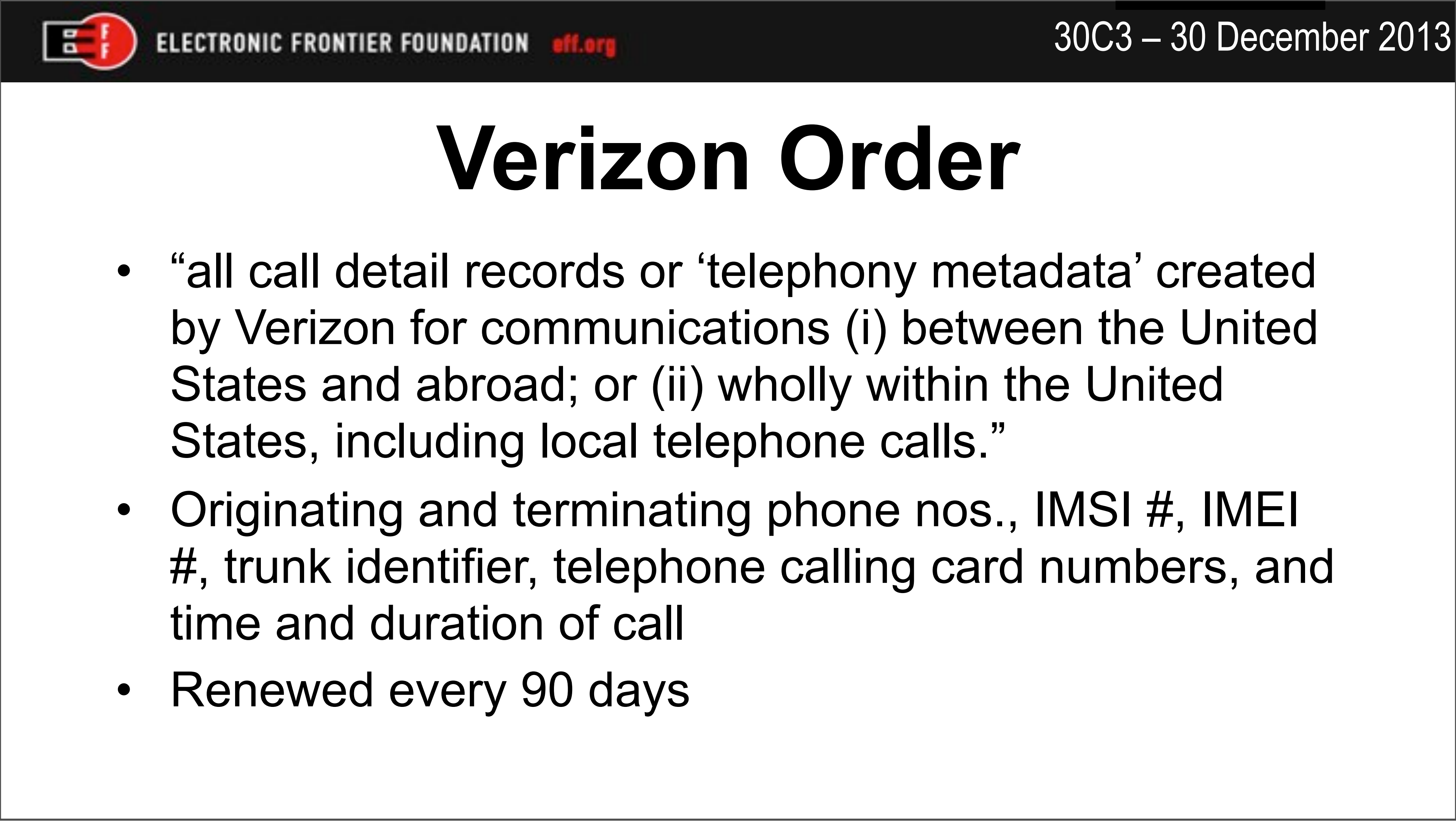
NSA looked at any communications that mentioned both the Swedish manufacturer Ericsson and "radio" or "radar".

Processing


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

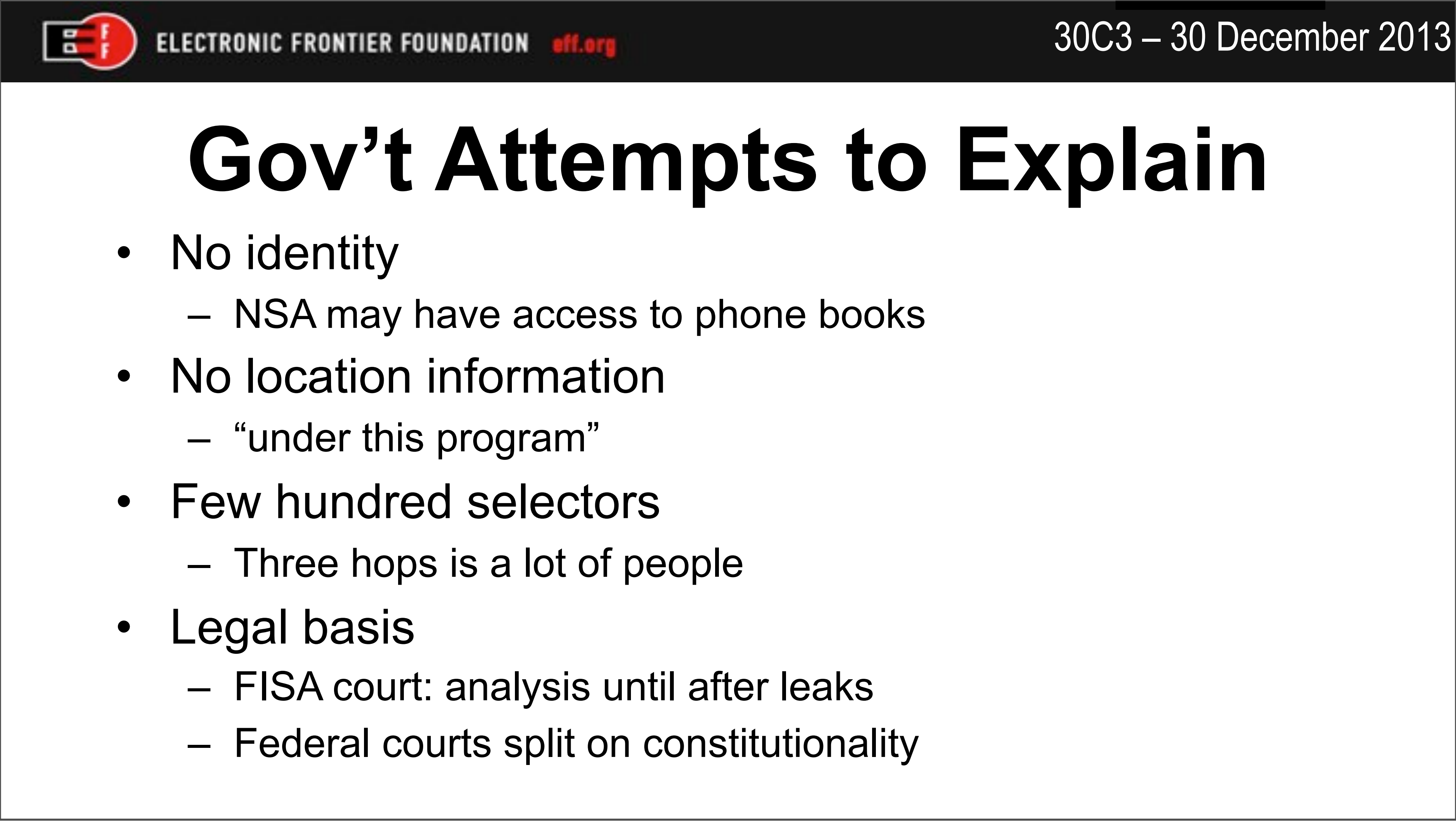
- “all call detail records or ‘telephony metadata’ created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.”
- Originating and terminating phone nos., IMSI #, IMEI #, trunk identifier, telephone calling card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

Montag, 27. November 2017

International Mobile Subscriber Identity, International Mobile Station Equipment Identity

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.”



ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

Gov’t Attempts to Explain

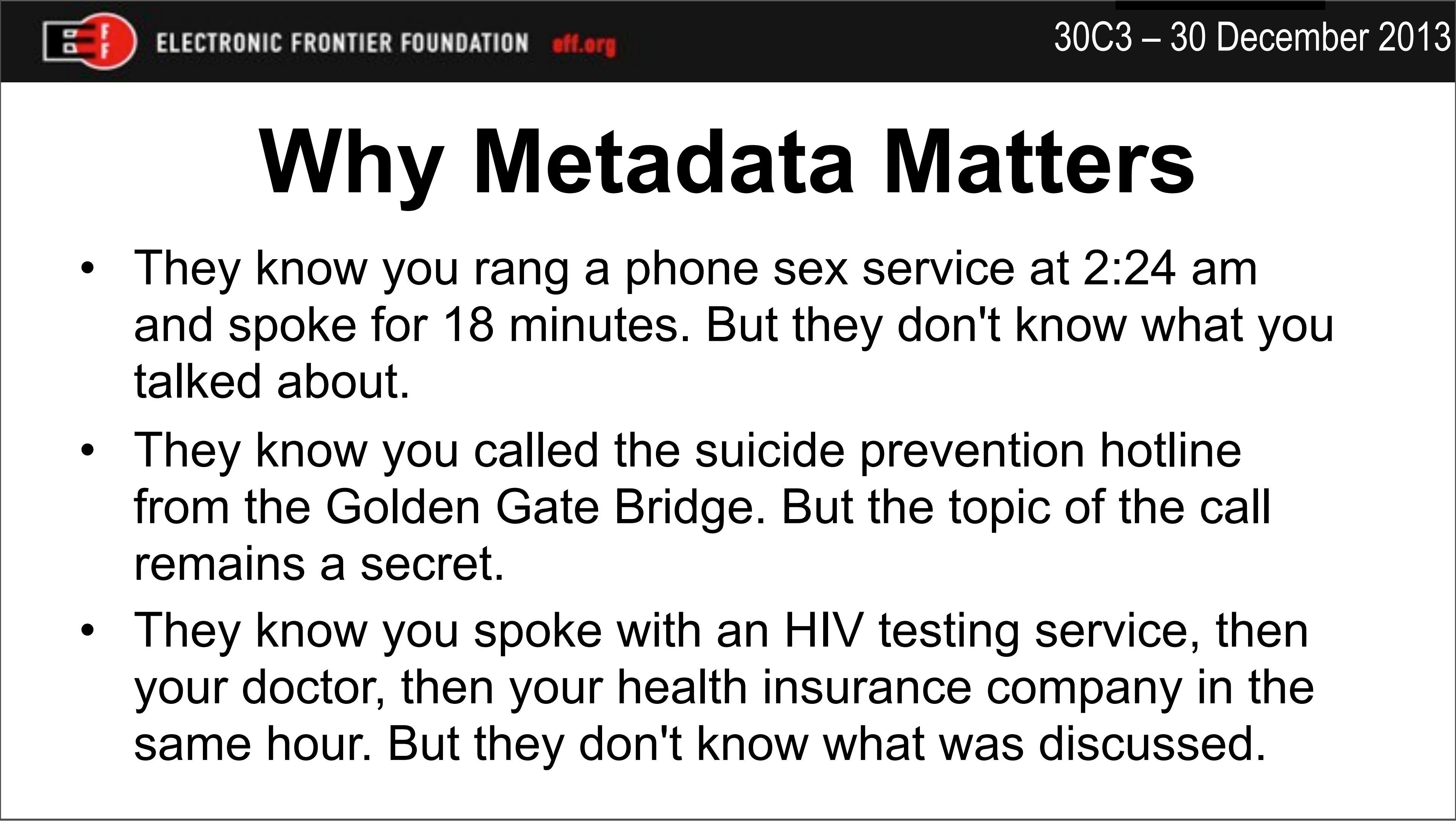
- No identity
  - NSA may have access to phone books
- No location information
  - “under this program”
- Few hundred selectors
  - Three hops is a lot of people
- Legal basis
  - FISA court: analysis until after leaks
  - Federal courts split on constitutionality

Montag, 27. November 2017

Of course, we later discovery that the NSA is tracking location information, under a different program.

First they said 300, then 200.

First issued gov’t memo, then FISA court opinions.



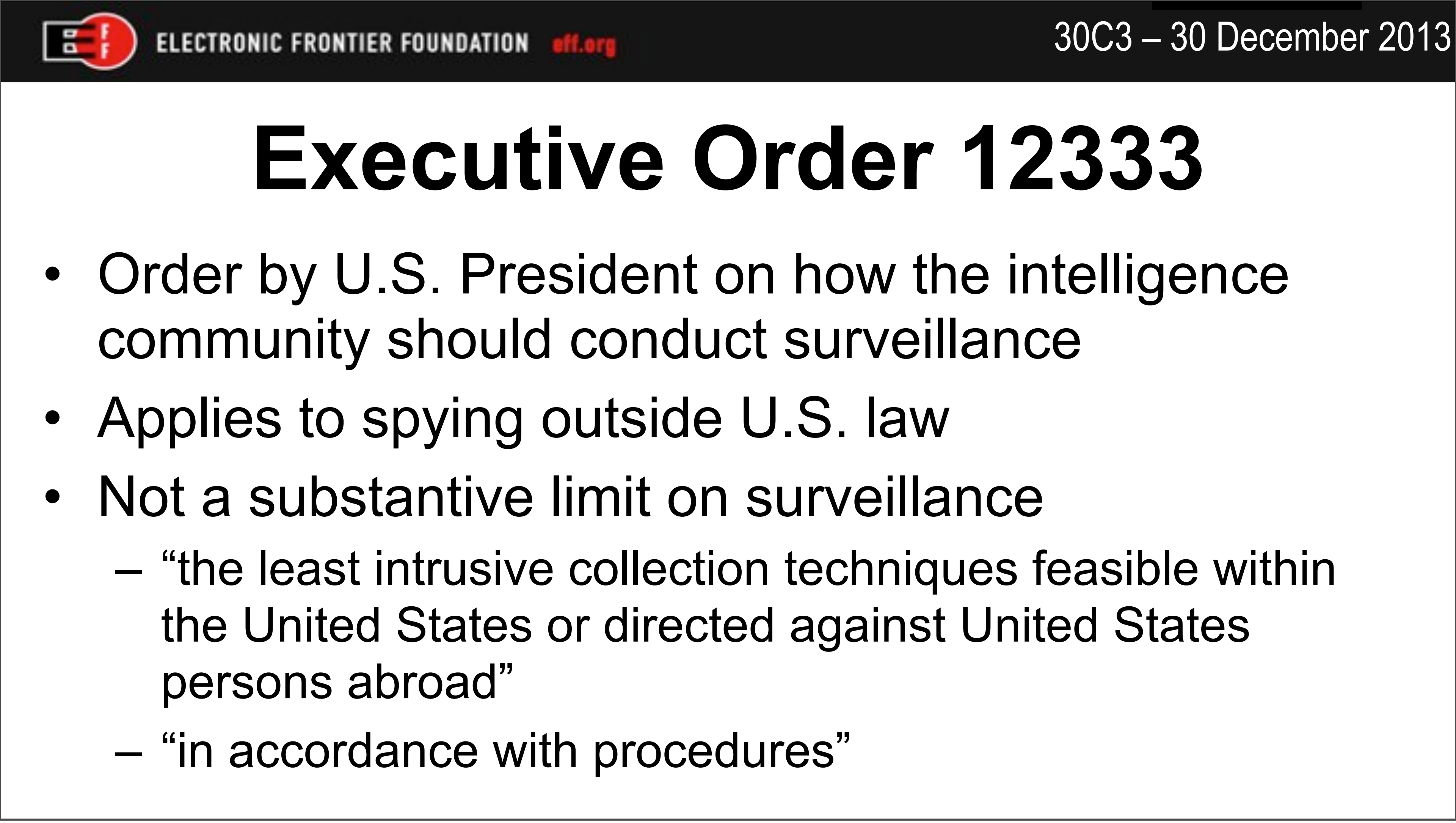
ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

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.

Montag, 27. November 2017

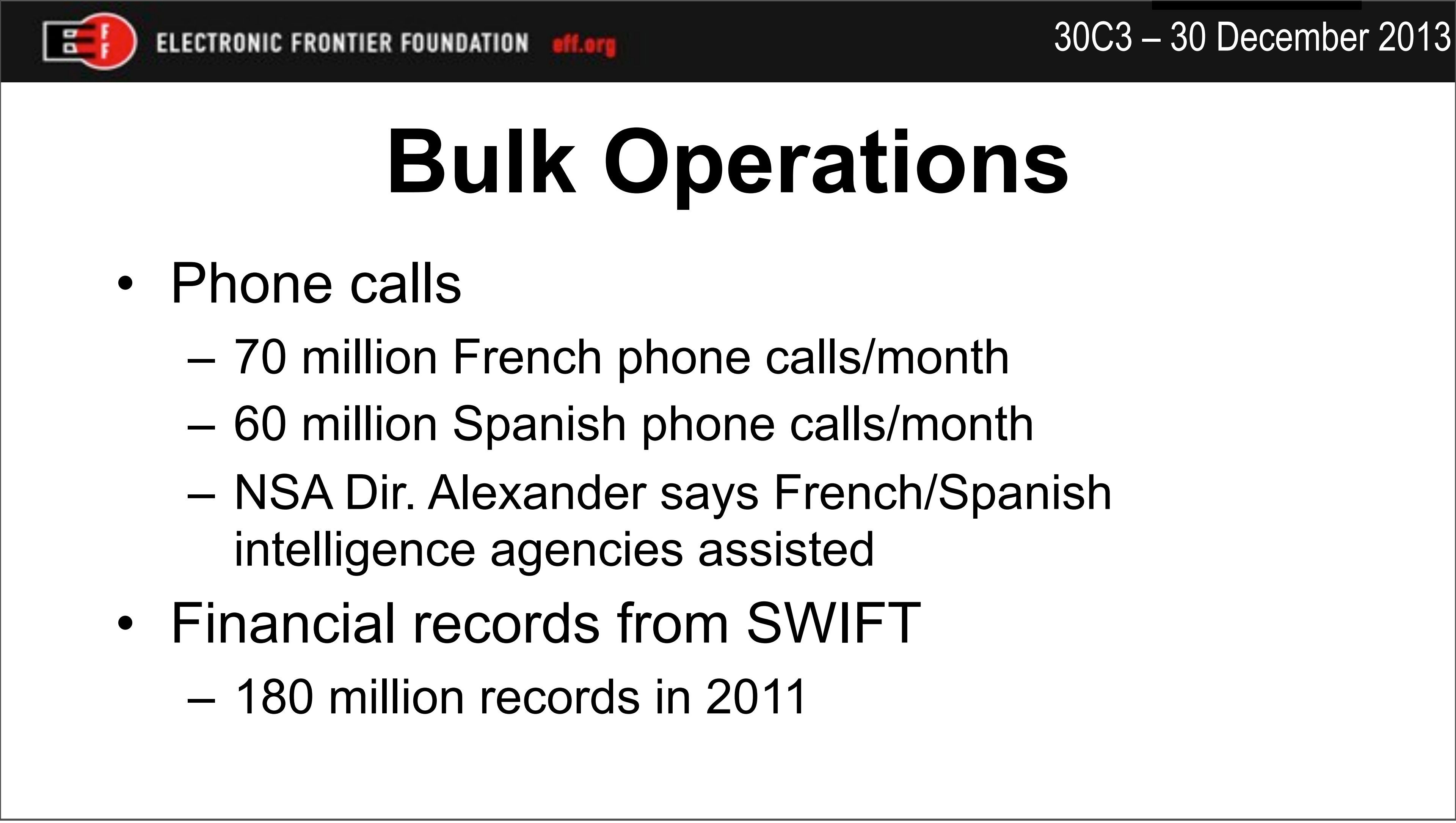


Executive Order 12333

- 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”

Montag, 27. November 2017

Later amended by Executive Order 13355: Strengthened Management of the Intelligence Community, on August 27, 2004. On July 30, 2008, President Bush issued Executive Order 13470 amending Executive Order 12333 to strengthen the role of the DNI.



Bulk Operations

- Phone calls
  - 70 million French phone calls/month
  - 60 million Spanish phone calls/month
  - NSA Dir. Alexander says French/Spanish intelligence agencies assisted
- Financial records from SWIFT
  - 180 million records in 2011

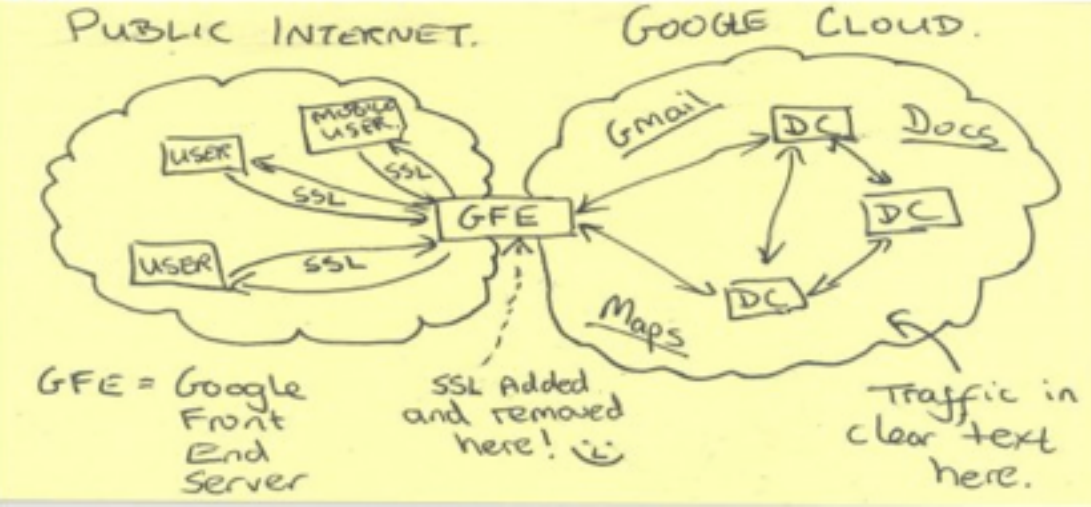
Montag, 27. November 2017

Society for Worldwide Interbank Financial Telecommunication, or SWIFT, is a cooperative owned by around 8,000 financial institutions, runs a messaging service that enables worldwide financial transactions between banks.

Der Spiegel reported that SWIFT was a target of spying by the NSA’s “tailored access operations” division, which collected printer traffic data from numerous banks

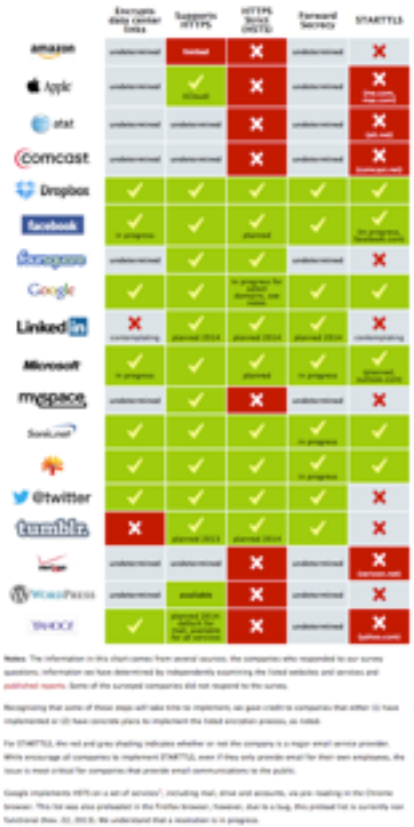
MUSCULAR

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


PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER.
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! :-)
Traffic in clear text here.

Encrypt All the Bits

- Responses to the smiley face
  - Dropbox, Facebook, Google, Microsoft, Twitter, Yahoo and others deploying encryption on data center links
  - Increased adoption of HTTPS/HSTS
  - More forward secrecy
  - Full page ads opposing bulk collection



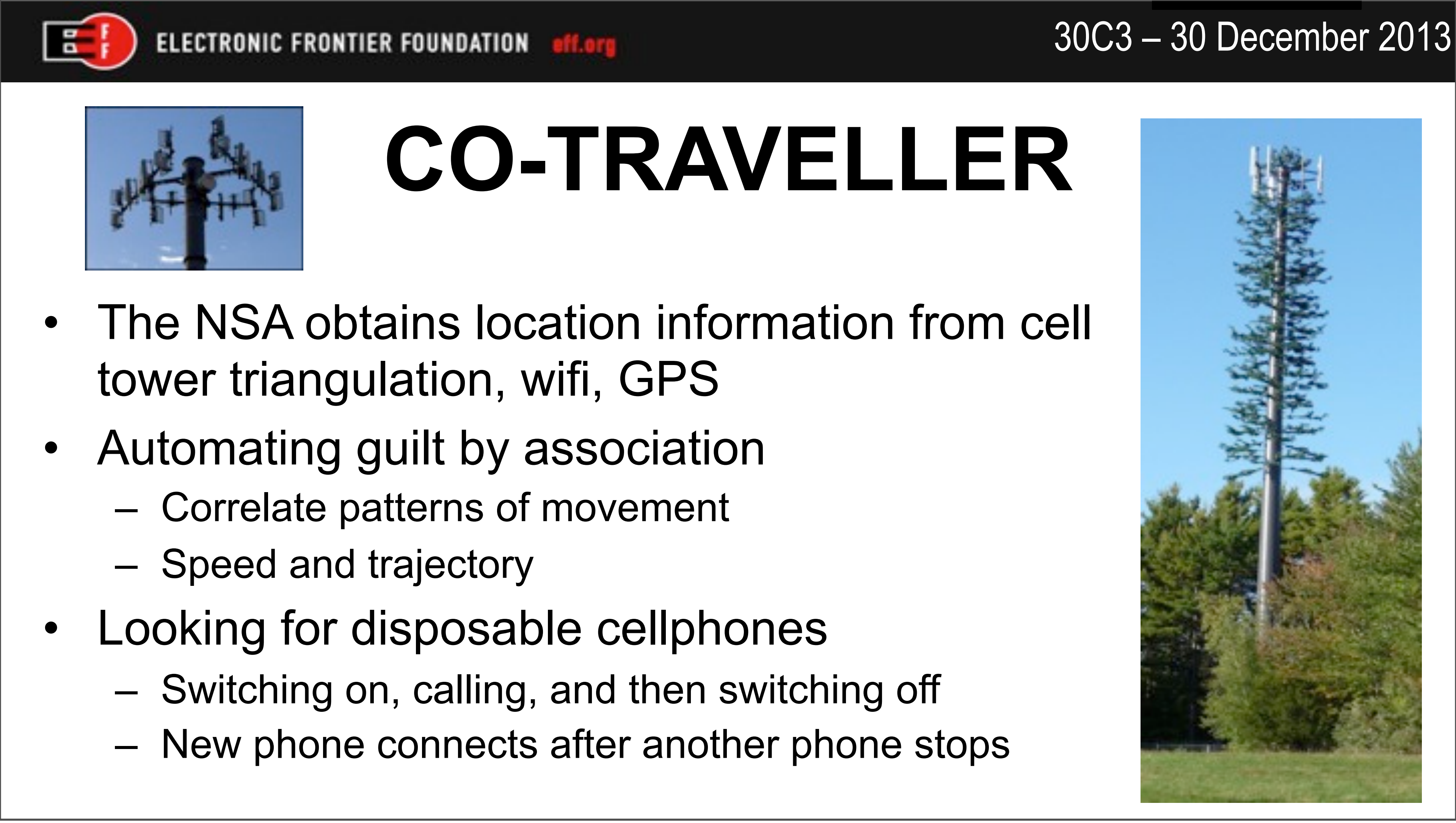
	Encrypts data center links	Supports HTTPS	HTTPS Strict (HSTS)	Forward Secrecy	STARTTLS
amazon	undetermined	limited	✗	undetermined	✗
Apple	undetermined	✓ iCloud	✗	undetermined	✗ (me.com, mac.com)
at&t	undetermined	undetermined	✗	undetermined	✗ (att.net)
comcast	undetermined	undetermined	✗	undetermined	✗ (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	✗
SonicNet	✓	✓	✓	✓ in progress	✓
	✓	✓	✓	✓ in progress	✓
@twitter	✓	✓	✓	✓	✗
tumblr.	✗	✓ planned 2013	✓ planned 2014	✓	✗
verizon	undetermined	undetermined	✗	undetermined	✗ (verizon.net)
WordPress	undetermined	available	✗	undetermined	✗
YAHOO!	✓	planned 2014 default for mail, available for all services	✗	undetermined	✗ (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 encryption process, as noted.

For STARTTLS, the red and grey shading indicates whether or not the company is a major email service provider. While we 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 a set of services*, including mail, drive and accounts, via pre-loading in the Chrome browser. This list was also preloaded in the Firefox browser; however, due to a bug, this preload list is currently not functional (Nov. 22, 2013). We understand that a resolution is in progress.



ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

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

Montag, 27. November 2017

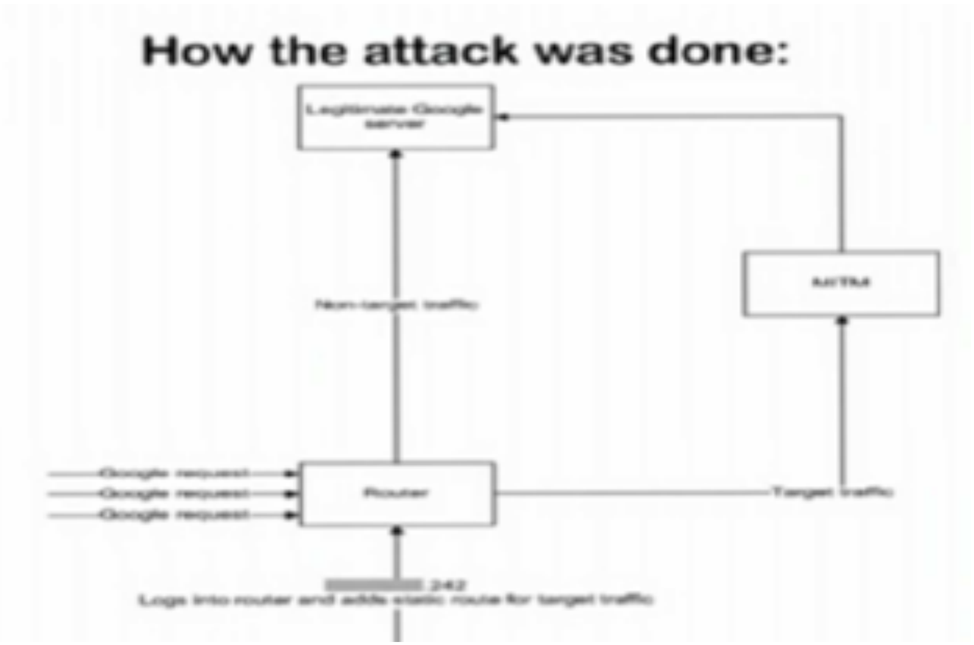
HAPPYFOOT intercepts mobile app traffic that sends a smartphone’s location to ad networks

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

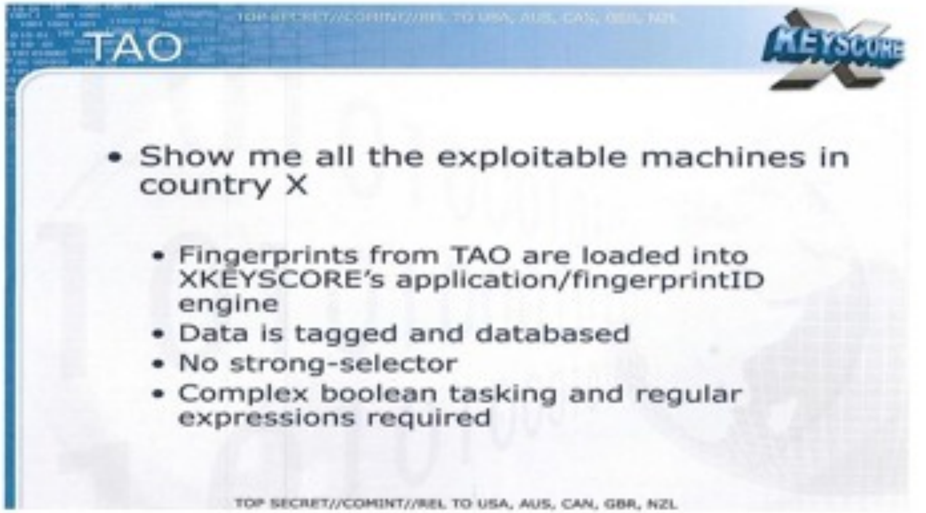


Montag, 27. November 2017

Side note: with codenames like Prism and Flying Pig, suggests that someone in the code naming department is a fan of Pink Floyd album covers.

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



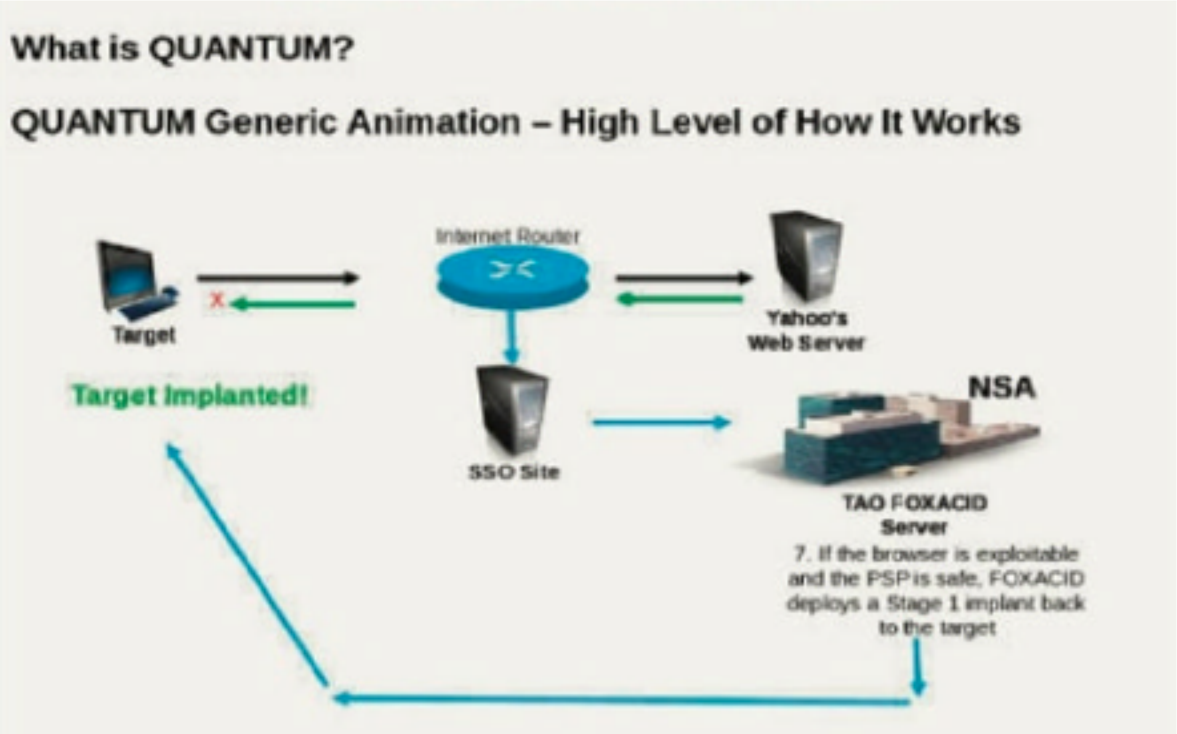
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

TAO

- Show me all the exploitable machines in country X
  - Fingerprints from TAO are loaded into XKEYSCORE’s application/fingerprintID engine
  - Data is tagged and databased
  - No strong-selector
  - Complex boolean tasking and regular expressions required

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

QUANTUM INSERT



What is QUANTUM?

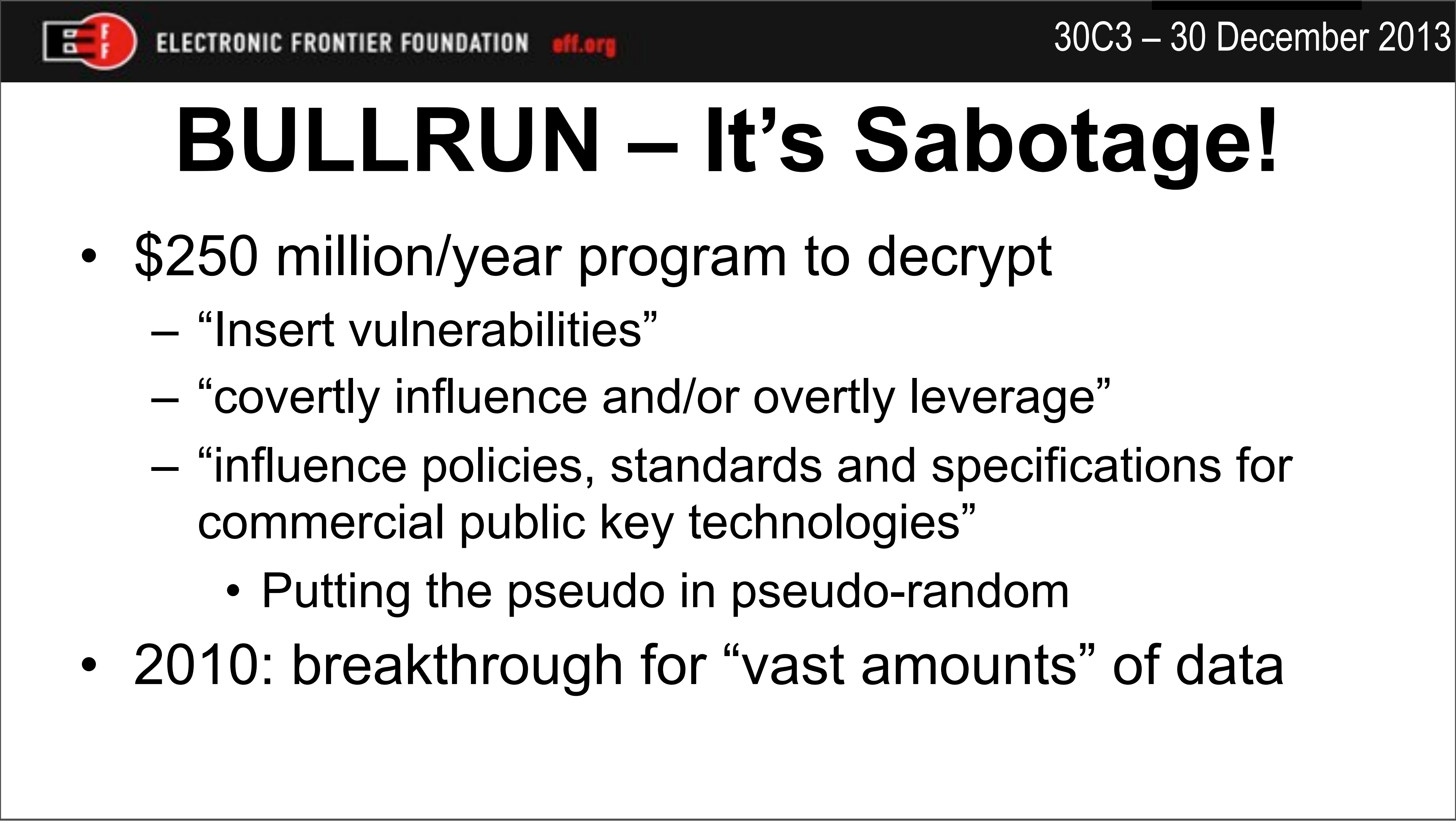
QUANTUM Generic Animation – High Level of How It Works

7. If the browser is exploitable and the PSP is safe, FOXACID deploys a Stage 1 implant back to the target

Montag, 27. November 2017

Quantum sits on backbone, responds faster than legitimate server (race condition), redirects to FoxAcid server, which serves up malware via Ferret Cannon.

TAO maintains a library of exploits, each based on a different vulnerability in a system. Different exploits are authorized against different targets, depending on the value of the target, the target's technical sophistication, the value of the exploit, and other considerations.



ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

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”
    - Putting the pseudo in pseudo-random
- 2010: breakthrough for “vast amounts” of data

Montag, 27. November 2017

The name "BULLRUN" was taken from the First Battle of Bull Run, the first major battle of the American Civil War. GCHQ has a similar program codenamed Edgehill, the first battle of the English Civil War.

Dual_EC_DRBG

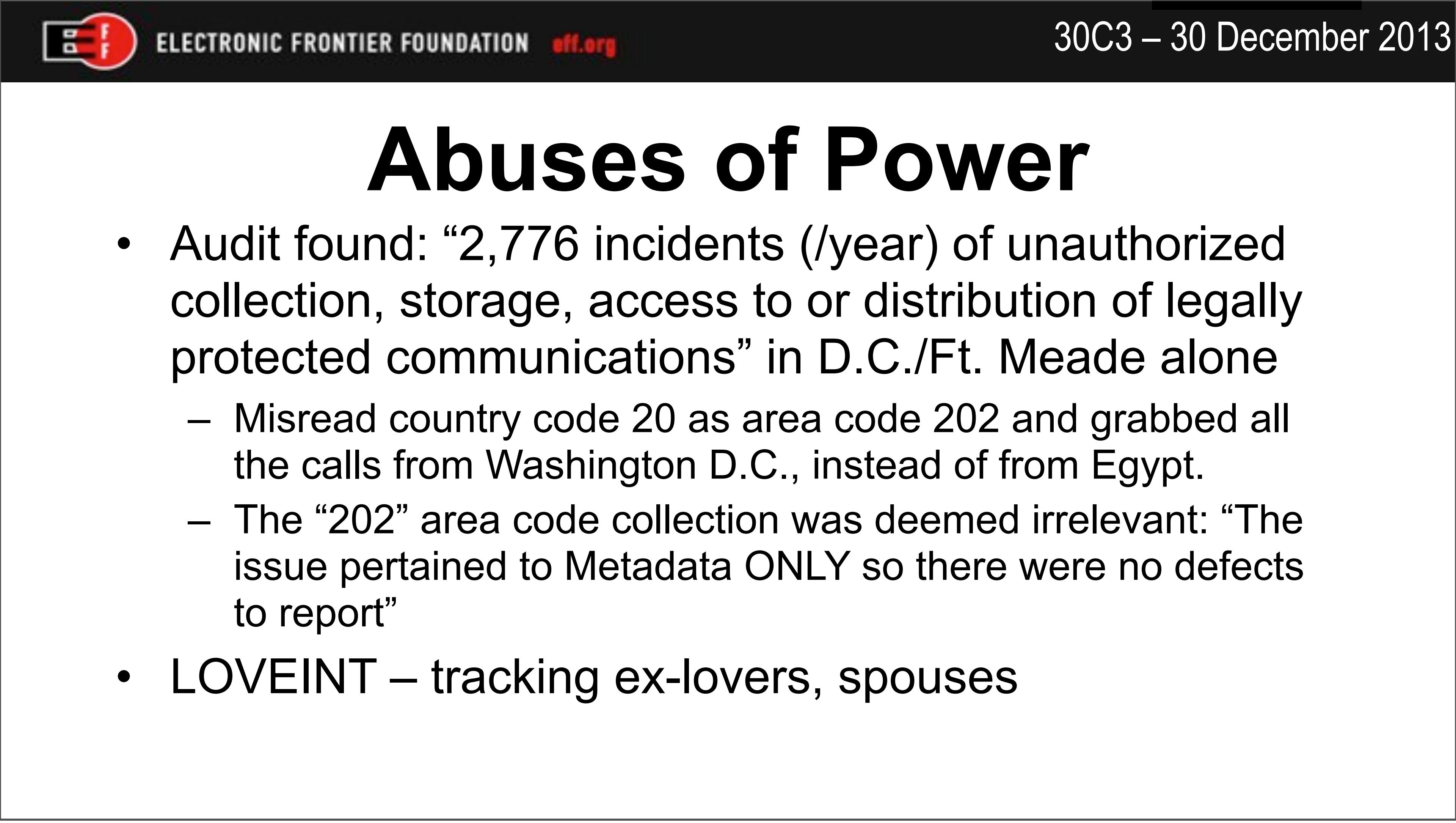
Tor Stinks

- Efforts to fingerprint and exploit users via Firefox
  - EGOTISTICALGIRAFFE exploits Firefox bugs
  - FBI used same technique on Freedom Host (.onion)
- Core security appears intact
  - No de-anonymizing on demand

Montag, 27. November 2017

EgotisticalGiraffe exploits a type confusion vulnerability in E4X, which is an XML extension for Javascript. This vulnerability exists in Firefox 11.0—16.0.2, as well as Firefox 10.0 ESR—the Firefox version used until recently in the Tor browser bundle.

Inadvertently fixed when Mozilla removed the E4X library with the vulnerability



ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

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

Montag, 27. November 2017

NSA Dir. Alexander told Blackhat that there was no one who went outside the bounds. Domestically.

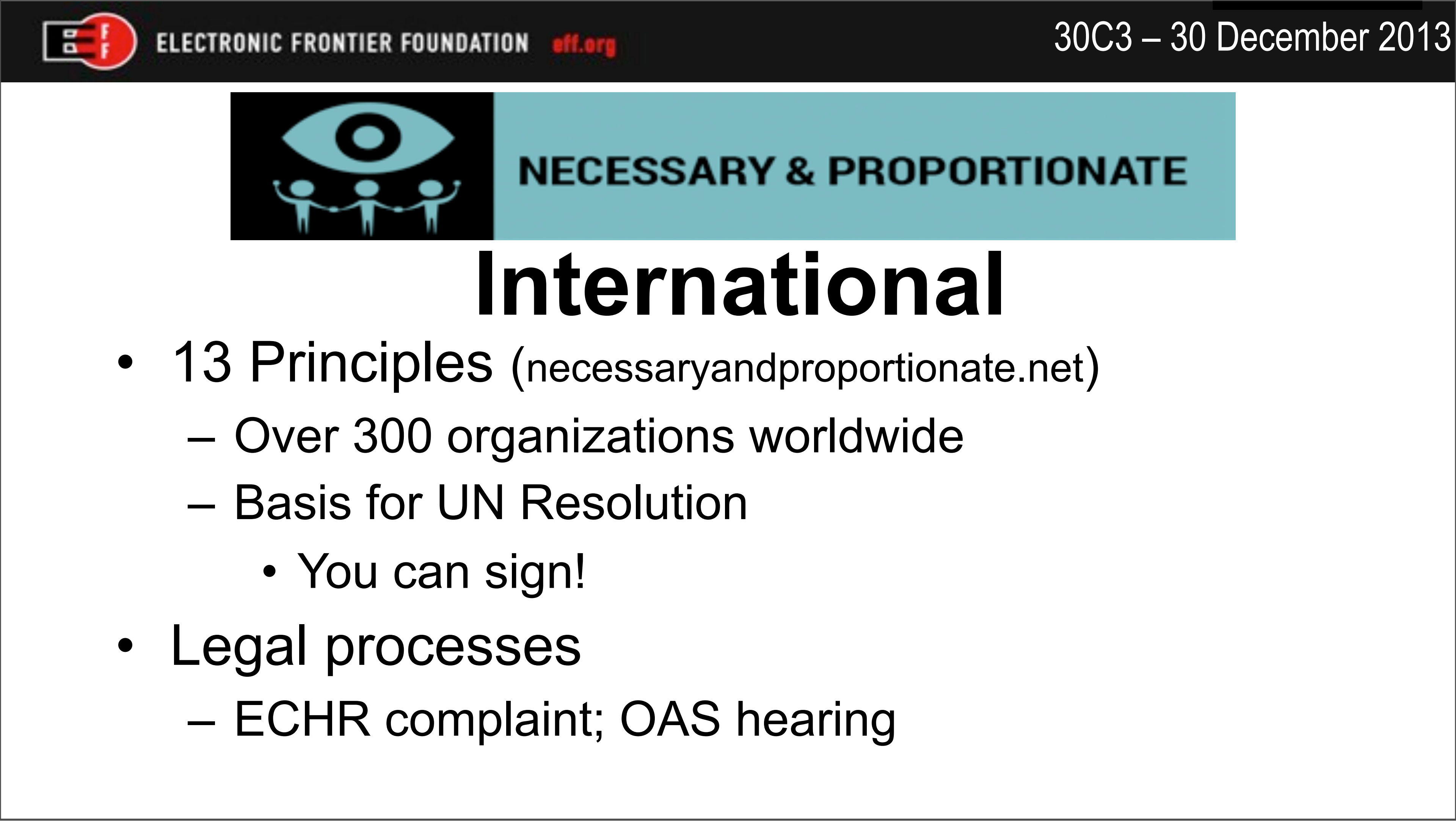
10 incidents of LOVEINT – self reported. Overseas.

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

STOP WATCHING US

- Built broad coalition
  - Over half-million petition signatures to U.S. Congress
  - Interpret for public
- Commenting on U.S. bills
  - Feinstein/Rogers
  - Leahy/Sensenbrenner



ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

NECESSARY & PROPORTIONATE

International

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

Montag, 27. November 2017

Privacy International has submitted a claim to the UK Investigatory Powers Tribunal (IPT) European Convention on Human rRghts

The Inter-American Commission on Human Rights, Organization of American States (OAS), held a hearing on October 28, 2013 on the NSA's mass surveillance and its impact on human rights in the Americas. The hearing was held at the request of the American Civil Liberties Union, and included the U.N. Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue.

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
Senior Staff Attorney, EFF
@kurtopsahl
kurt@eff.org