



Through a PRISM, Darkly



Mark Rumold
Staff Attorney, EFF



ELECTRONIC FRONTIER FOUNDATION eff.org

NANOG 59 – October 7, 2013

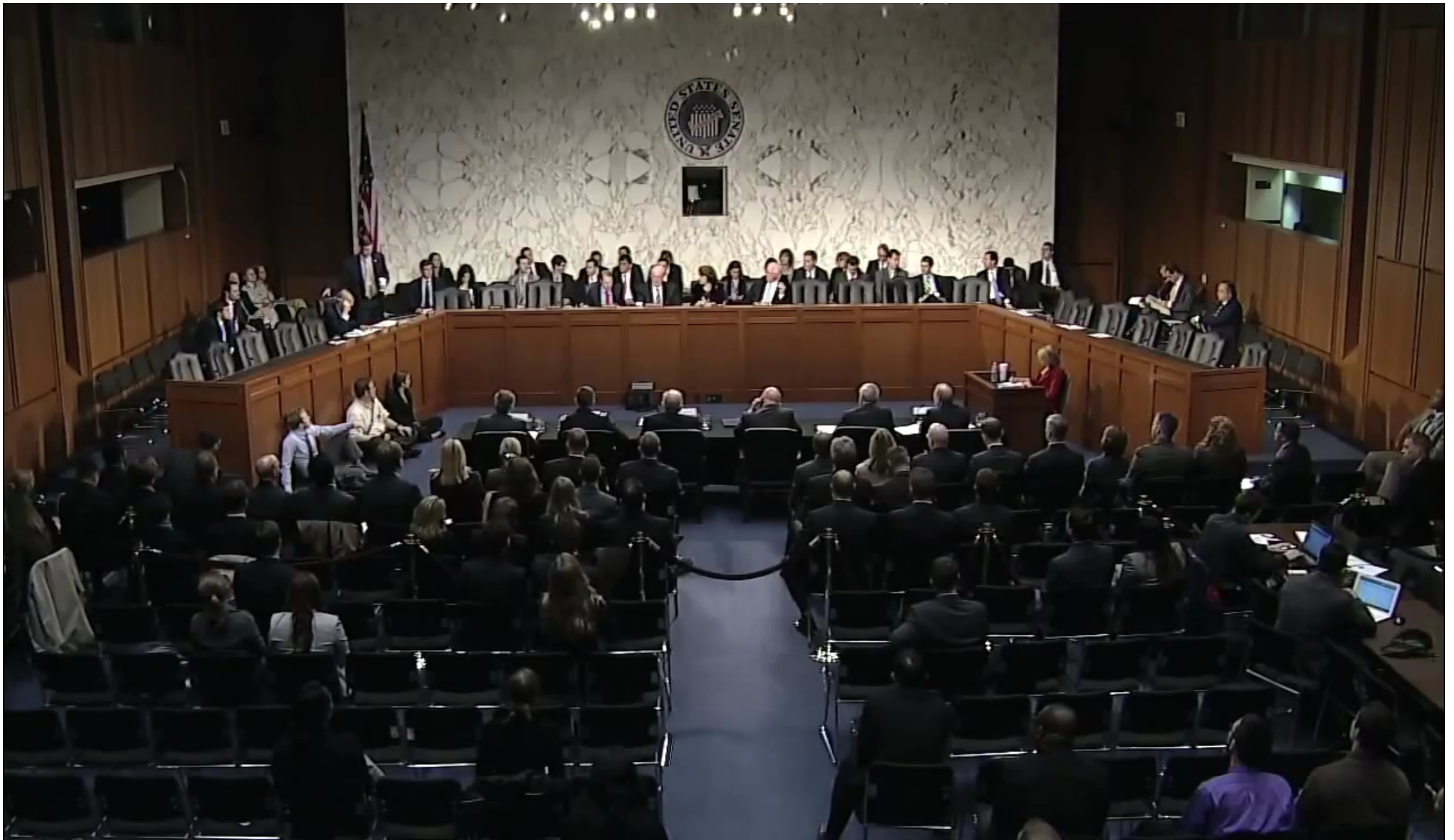
Electronic Frontier Foundation





ELECTRONIC FRONTIER FOUNDATION eff.org

NANOG 59 – October 7, 2013





N.S.A. Said to Search Content of Messages to and U.S.

By CHARLIE SAVAGE
Published: August 8, 2013

WASHINGTON
contents of vas
communication
mention inf
to intelliger

Related in C

Editorial: Brea
on Spying (Au

Connect W Us on Twit

Follow
@NYTNations
breaking news
headlines.

Twitter List: R

Readers

"Well, since
lied to us bel
scope of thei
programs, I
100 percent.
Bill, Charlot
Read Full Comm

headlines.

Twitter List: Reporters and Editors

Readers' Comments

Share your thoughts.

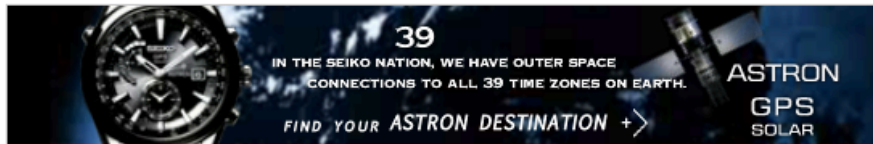
Post a Comment »
Read All Comments (42) »

theguardian

News | US | World | Sports | Comment | Culture | Business | Money

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VIDEO



SEIKO: the NSA's secret surveillance data

ol for cataloguing global
es on US collection

PORTS | OPINION



Pearl White

on Web

THREAT LEVEL

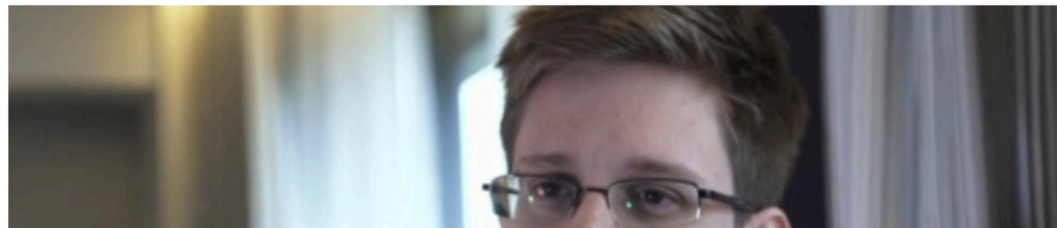
miscellaneous

Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show

BY KEVIN POULSEN 10.02.13 5:27 PM

Follow @kpoulsen

Share 11.4k
Tweet 3,439
+1 1.4k
in Share 84
Pin it



when selecting wiretap targets.

The largest number of episodes — 1,600 — “roamers,” in which a foreigner whose phone was wiretapped without a warrant came from China, where individual warrants are required. In the first quarter, the report found, because of Chinese citizens visiting for the Chinese Lunar New Year holiday

outlined in four slides
d questions document

ETA

00 EDT

FACEBOOK

TWITTER

GOOGLE+

SAVE

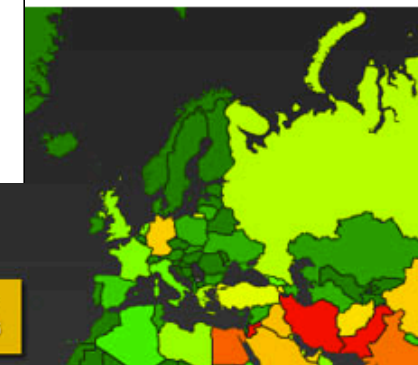
E-MAIL

SHARE

PRINT

REPRINTS

ogram



how the
Americans'
e in the
sday, a
ion, which
gram.

feat the
1 of liberal
lawmakers

had joined forces in response to revelations by Edward Snowden, a former NSA contractor, that the agency has collected the phone



What we'll cover today:

- Background; what we know; what the problems are; and what we're doing
- Codenames. From Stellar Wind to the President's Surveillance Program, PRISM to Boundless Informant
- Spying Law. A healthy dose of acronyms and numbers. ECPA, FISA and FAA; 215 and 702.



the background



changes



...yet much has stayed the same



The (Way) Background

- Established in 1952
- Twin mission:
 - “Information Assurance”
 - “Signals Intelligence”
- Secrecy:
 - “No Such Agency” & “Never Say Anything”





The (Mid) Background



- 1960s and 70s
- Cold War and Vietnam
- COINTELPRO and Watergate



The Church Committee

“[The NSA’s] capability at any time could be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything. Telephone conversations, telegrams, it doesn't matter. There would be no place to hide.”

Senator Frank Church, 1975



Reform

- Permanent Congressional oversight committees (SSCI and HPSCI)
- Foreign Intelligence Surveillance Act (FISA)
 - Established requirements for conducting *domestic* electronic surveillance of US persons
 - Still given free reign for *international* communications conducted *outside U.S.*



Changing Technology

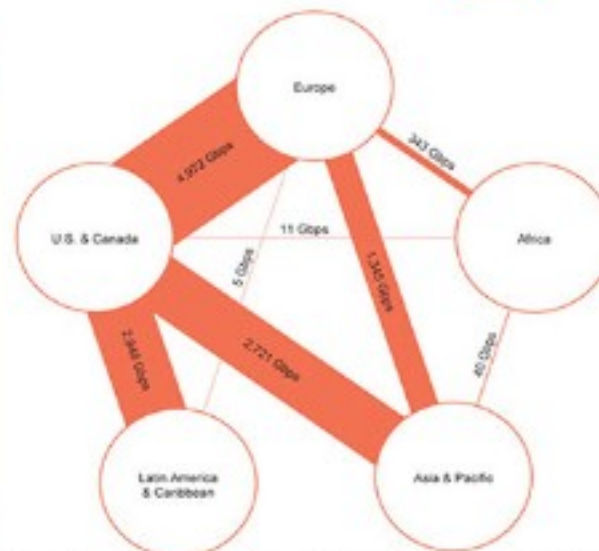
- 1980s - 2000s: build-out of domestic surveillance infrastructure
- NSA shifted surveillance focus from satellites to fiber optic cables
- BUT: FISA gives greater protection for communications on the wire + surveillance conducted *inside* the U.S.



“America’s Home Field Advantage”



- 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: Teleography Research

TOP SECRET//SI//ORCON//NOFORN



The (More Recent) Background

- After 9/11, President Bush authorized the NSA to spy inside the United States, including the collection of domestic content and metadata
- Called the Presidents Surveillance Program, the PSP was implemented without any court involvement (warrant or otherwise), which had been required for domestic surveillance since FISA
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001



***(TS//SI//NF) NSA Implements Controversial
11 March 2004 Authorization***

(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.

(TS//SI//NF) On 11 March 2004, General Hayden had to decide whether NSA would execute the Authorization without the Attorney General’s signature (IV-A/32-11). General Hayden described a conversation in which David Addington asked, “Will you do it (IV-A/32-11)?” At that time, General Hayden also said that he asked Daniel Levin, Counsel to the Attorney General, in March 2004 if he needed to stop anything he was doing. Mr. Levin said that he did not need to stop anything (IV-A/32-7 and IV-A/32a-7&8). After conferring with NSA operational and legal personnel, General Hayden stated that he decided to continue the PSP because 1) the members of Congress he briefed the previous day, 10 March, were supportive of continuing the Program, 2) he knew the value of the Program, and 3) NSA lawyers had determined the Program was legal.

Showdown at the Hospital

- March 2004; Acting Attorney General Comey refused to sign off on the PSP
- Gonzalez and Comey race to hospital
- Threats of resignation



(First) Public Disclosure

NYTimes.com[Go to a Section](#)

SEARCH [NYT Since 1981](#)


[Home](#) [News](#) [Travel](#) [Money](#) [Sports](#) [Life](#) [Tech](#) [Wee](#)

Bush Lets U.S. Spy on Callers

By JAMES RISEN and [ERIC LICHTBLAU](#)

Published: December 16, 2005

[Correction Appended](#)[Enlarge This Image](#)

Doug Mills/Associated Press

In 2002, President Bush toured the National Security Agency at Fort Meade, Md., with Lt. Gen. Michael V. Hayden, who was then the

WASHINGTON, Dec. 16 — After the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and other people in the United States to search for terrorists without the court-approved warrants required for domestic spying, according to a new report.

Under a presidential authorization, the agency has monitored international e-mail and phone calls of thousands of people without warrants over the past several years, a top NSA official said. The agency, the report said, has also conducted entirely domestic cor

The previously undisclosed eavesdropping inside the NSA was a major shift in

[Washington/Politics](#)[Inside News](#)[Cars](#) [E](#)

NSA has massive database of Americans' phone calls

Updated 5/11/2006 10:38 AM ET

[Enlarge](#) By Roger Wollenberg, Getty Images

Gen. Michael Hayden, nominated by President Bush to become the director of the CIA, headed the NSA from March 1999 to April 2005. In that post, Hayden would have overseen the agency's domestic phone record collection program.

REACTION

[E-mail](#) [Print](#) [Reprints & Permissions](#) [RSS](#)

By Leslie Cauley, USA TODAY

The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth, people with direct knowledge of the arrangement told USA TODAY.

The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans — most of whom aren't suspected of any crime. This program does not involve the NSA listening to or recording conversations. But the spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity, sources said in separate interviews.

QUESTIONS AND ANSWERS: [The NSA record collection program](#)

"It's the largest database ever assembled in the world," said one person, who, like the others who agreed to talk about the NSA's activities, declined to be identified by name or affiliation. The agency's goal is "to create a database of every call ever made" within the nation's borders, this person added.



FISA Amendments Act (FAA)

- Gave the telcos immunity for participating in the NSA's program (and killed EFF's lawsuit, *Hepting v. AT&T*)
- Created a new “type” of surveillance under FISA for the “targeting” *within the United States* of those “reasonably believed to be located outside the U.S.”



FISA v. FISA Amendments Act

FISA

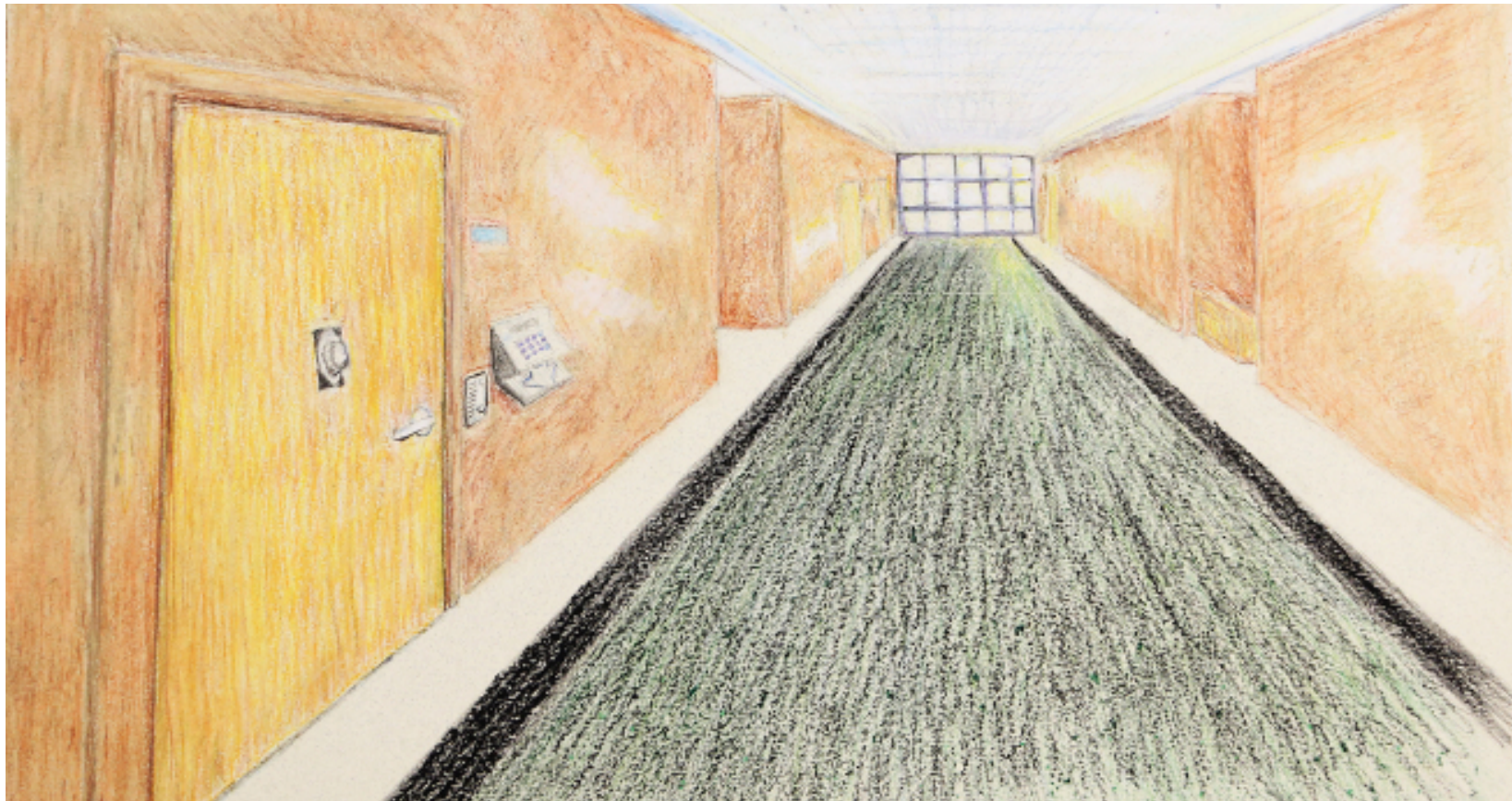
- Specific targets
- Specific court orders
- Surveillance inside U.S.
- BUT no court orders required for overseas (even if U.S. person)

FAA

- No specific targets
- Court sign off is on “programmatic” basis
- Surveillance conducted in U.S. “targeting” foreigners abroad
- Court order required to “target” U.S. person overseas



The Secret FISA Court





Foreign Intelligence Surveillance Court (FISC)

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



To Review:

- Foreign Intelligence Surveillance Act (FISA)
- USA Patriot Act (Section 215)
- FISA Amendments Act (Section 702)
- Executive Order 12,333



what we know



FAA Section 702





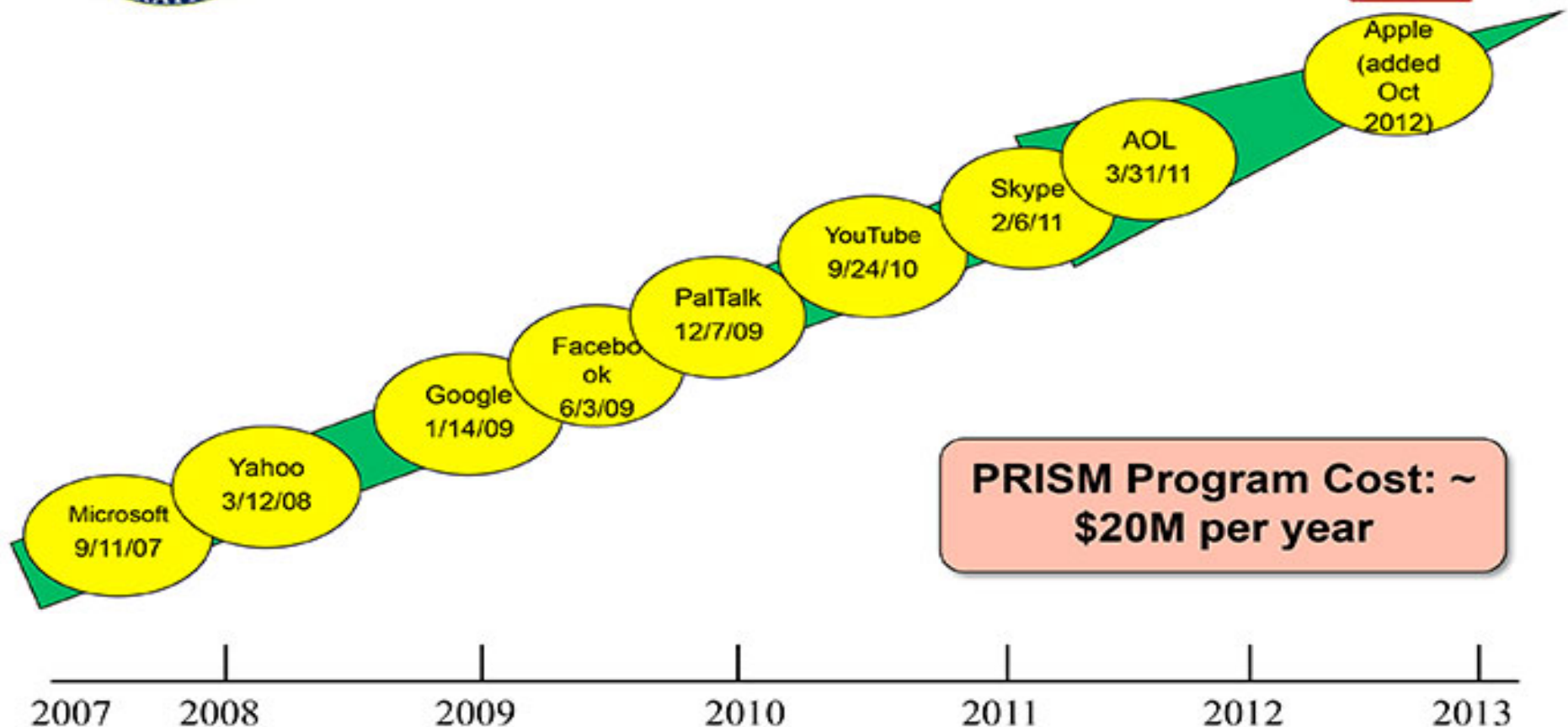
TOP SECRET//SI//ORCON//NOFORN



Hotmail®

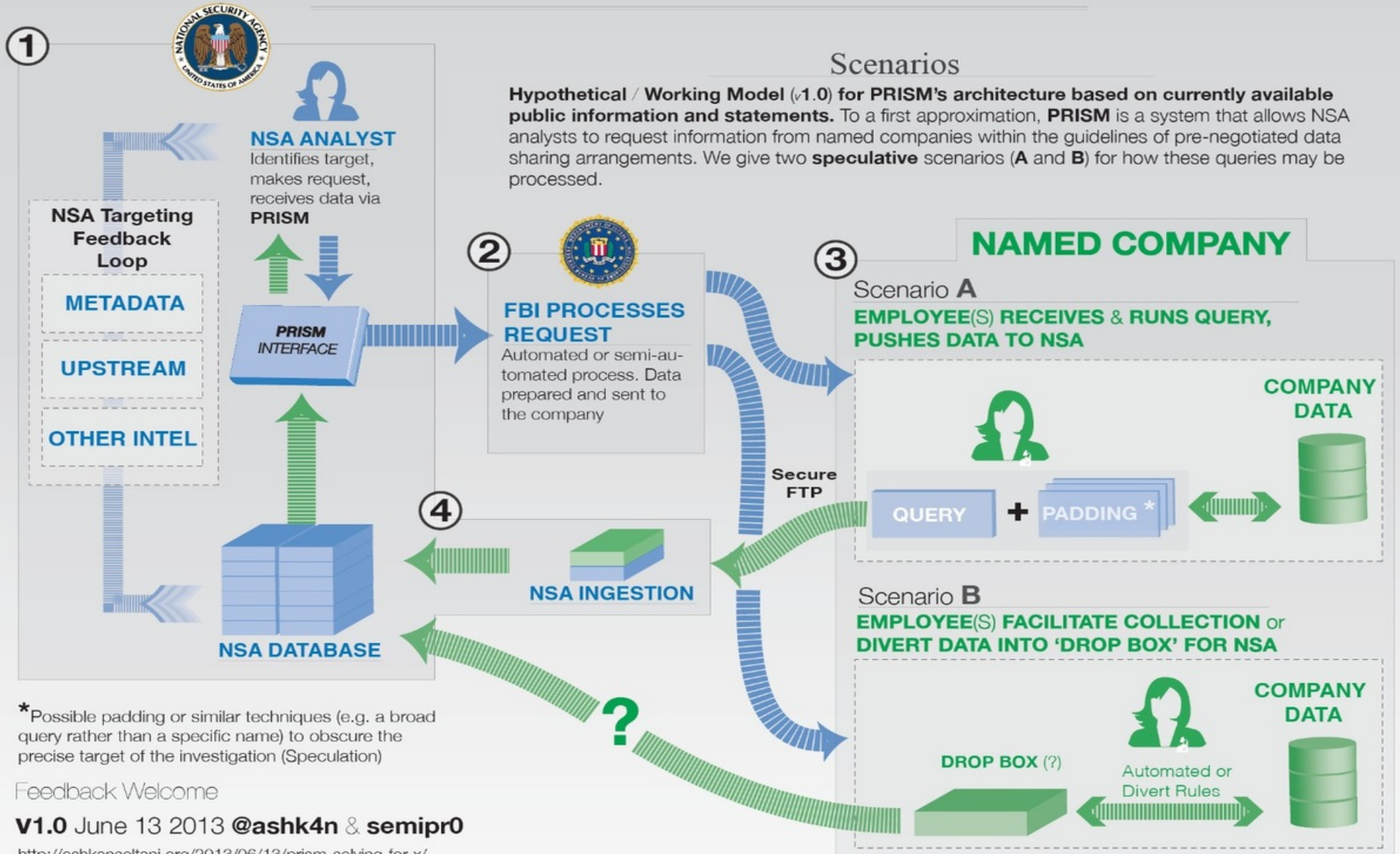


(TS//SI//NF) Dates When PRISM Collection
Began For Each Provider





HOW PRISM MAY WORK





FAA Section 702

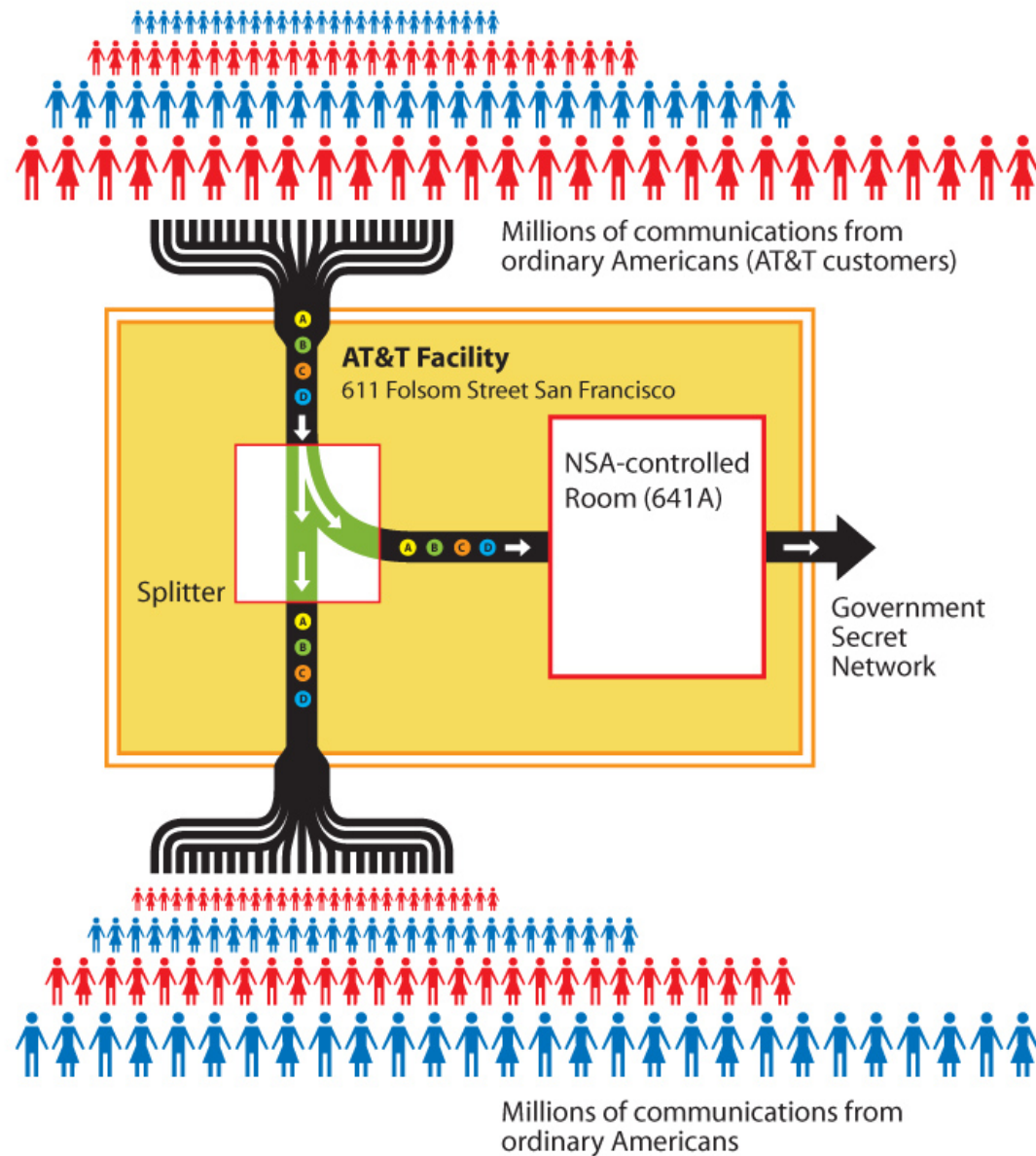




How “Upstream” Collection Works

- “Splitter cabinet” installed to capture and divert AT&T’s off-net, peering traffic
- Mark Klein installed one in Room 641A of AT&T’s Folsom Street facility
- Evidentiary foundation for *Jewel v. NSA* (2008)







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
- Only the FBI can apply for 215 Order



In Test Project, N.S.A. Tracked Cellphone Locations



- “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; same kind of order exists for three different companies

Related

As F.B.I. Pursued Snowden, an

reported on Wednesday morning by
The New York Times and later

[+](#) SHARE



The Internet Metadata Program

theguardian

[News](#) | [US](#) | [World](#) | [Sports](#) | [Comment](#) | [Culture](#) | [Business](#) | [Money](#)

[News](#) > [World news](#) > [NSA](#)

Series: Glenn Greenwald on security and liberty

NSA collected US email records in bulk for more than two years under Obama

- Secret program launched by Bush continued 'until 2011'
- Fisa court renewed collection order every 90 days
- Current NSA programs still mine US internet metadata

[Follow Glenn Greenwald by email](#) BETA

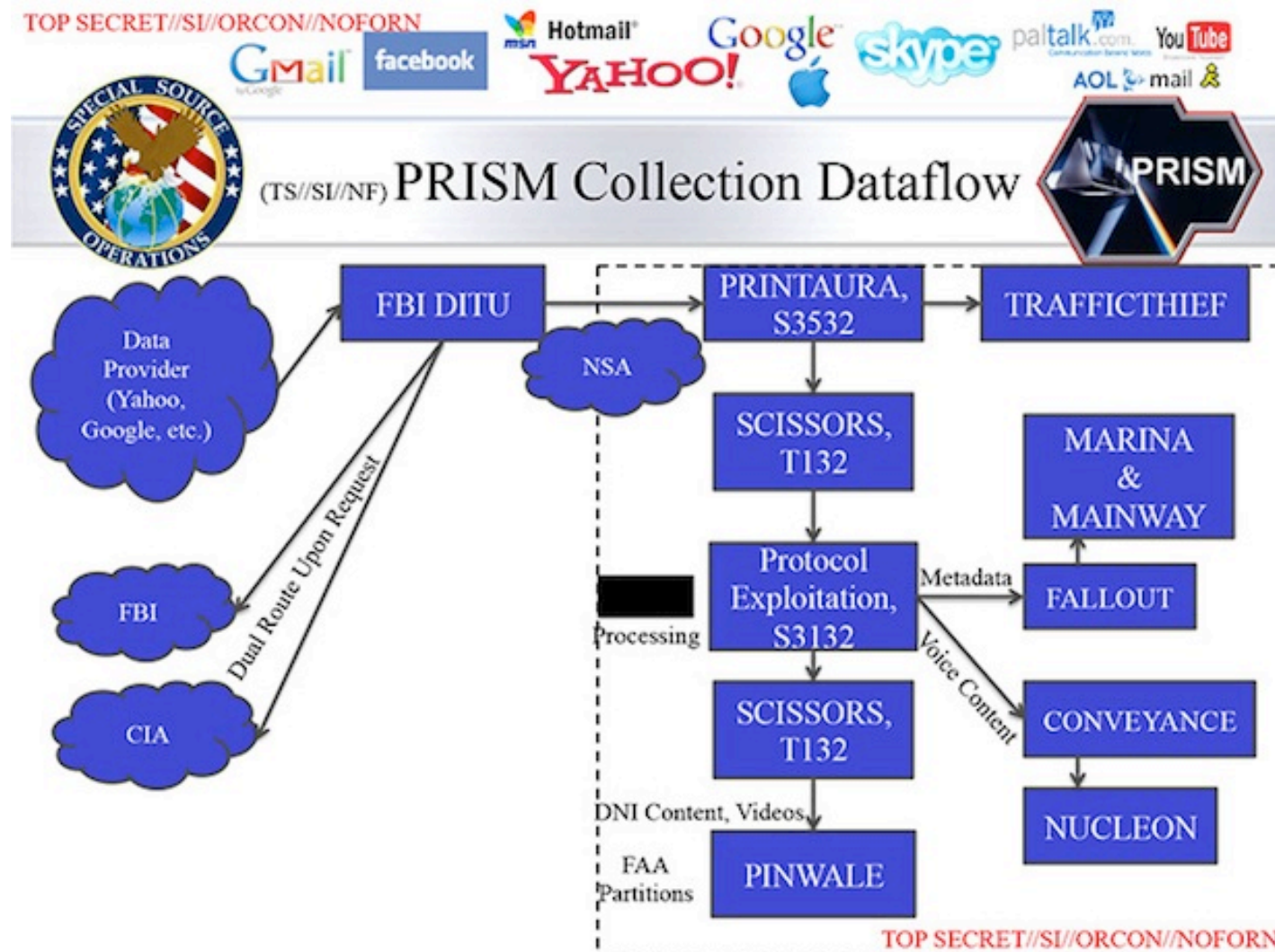
Glenn Greenwald and Spencer Ackerman
The Guardian, Thursday 27 June 2013 11.20 EDT
[Jump to comments \(1278\)](#)



- Still relatively little known about this part of the Program
- Shifted under FISA PR/TT authority in 2004/5
- Ended for “operational and resource” reasons in 2011



Meet the Databases





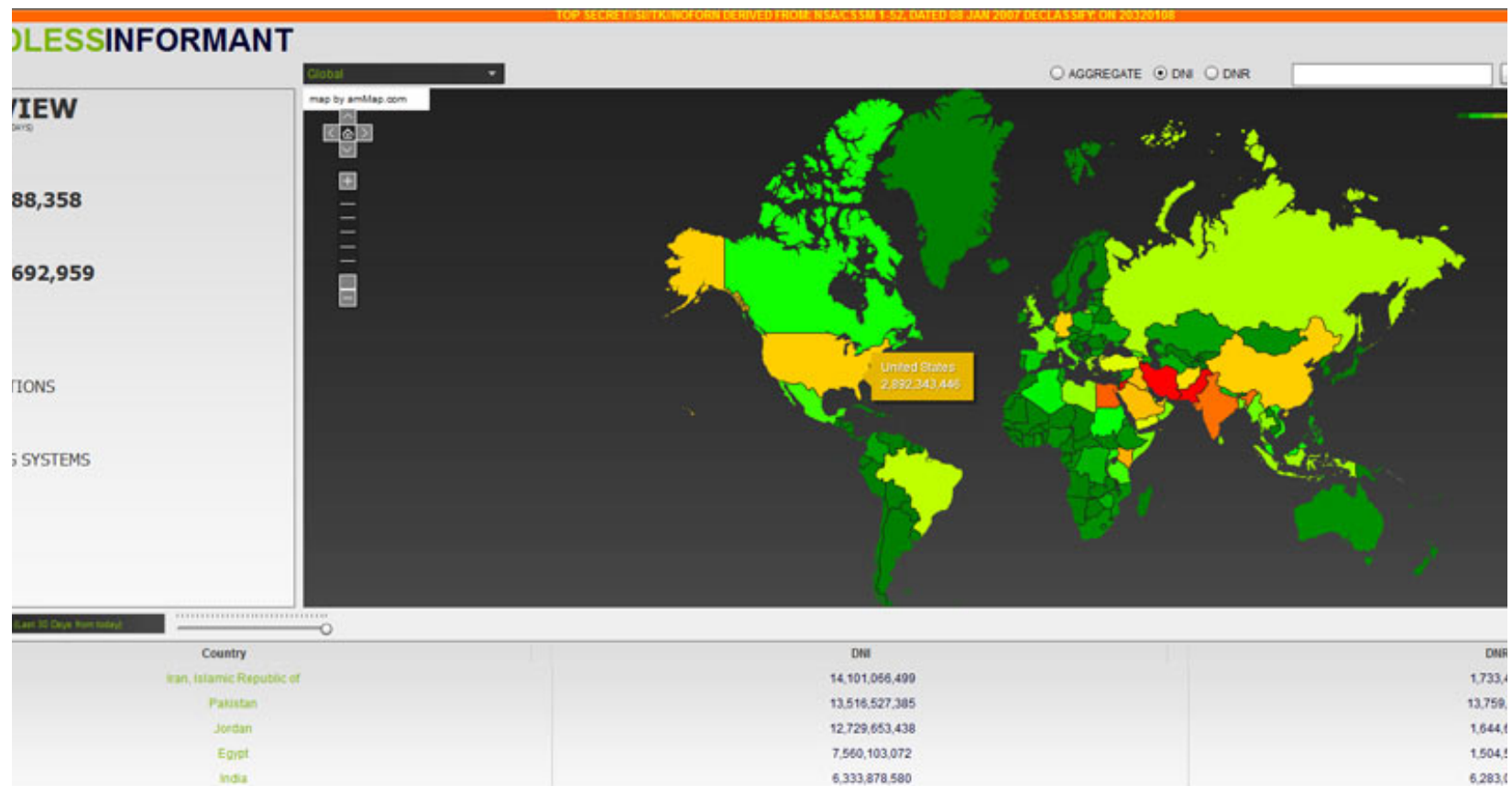
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?





Boundless indeed





Silent Crypto Wars

PRO PUBLICA Journalism in the Public Interest

Home | Our Investigations | Tools & Data | MuckReads | Get Involved | About Us

Support ProPublica's award-winning investigative journalism with a tax-

Surveillance

Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security



The National Security Agency headquarters at Fort Meade, Md., in January 2010. (Saul Loeb/AFP/Getty Images)

by Jeff Larson, ProPublica, Nicole Perloth, The New York Times, and Scott Shane, The New York Times, Sep. 5, 2013, 3:08 p.m.

Note: This story is not subject to our Creative Commons license.

Closer Look: [Why We Published the Decryption Story](#)

Sept. 6: This story has been updated with a response from the Office of the Director of National Intelligence.

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and

This story has been reported in partnership between The New York Times, the Guardian and ProPublica based on documents obtained by The Guardian.

3,224 | 151 | 497 | 5.4k

Tweet | Share | +1 | Like

The New York Times

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCI

POLITICS | EDUCATION | TEXAS

SAMSUNG
The Next Big Thing Is
Introducing Galaxy Note 3 + Galaxy Gear

N.S.A. Able to Foil Basic Safeguards

By NICOLE PERLOTH, JEFF LARSON and SCOTT SHANE
Published: September 5, 2013 | 1406 Comments

The [National Security Agency](#) is winning its long-running, on encryption, using supercomputers, technical trickery, and behind-the-scenes persuasion to undermine the major protecting the privacy of everyday communications in the age, according to newly disclosed documents.

[Enlarge This Image](#)



Associated Press

This undated photo released by the United States government shows the National Security Agency campus in Fort Meade, Md.

This article has been reported in partnership among The New York Times, The Guardian and ProPublica based on documents obtained by The Guardian. For The Guardian: James Ball, Julian Borger, Glenn Greenwald. For The New York Times: Nicole Perloth, Scott Shane. For ProPublica: Jeff

The agency has circumvented or cracked much of the encryption, that guards commerce and banking systems, protects sensitive data like secrets and medical records automatically secures the Web searches, Internet of phone calls of Americans around the world, the doc

Many users assume — or companies — that their data including those of the government keep it that way. The agency deciphering protected information closely guarded secrets, in highly classified program

theguardian [Google Custom](#)

News | US | World | Sports | Comment | Culture | Business | Money | Environment | Science

News | World news | The NSA files

Series: Glenn Greenwald on security and liberty [Previous](#) | [Next](#) | [Index](#)

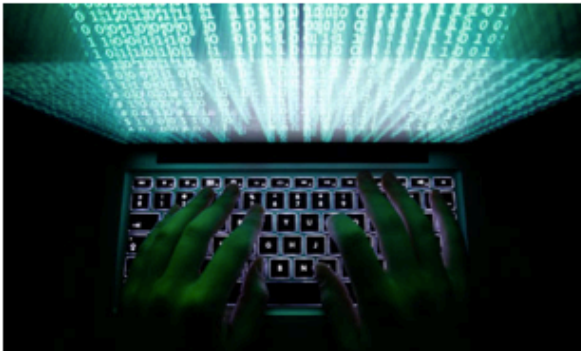
Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- \$250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

• Q&A: submit your questions for our privacy experts

[Follow Julian Borger by email](#) **BETA**

James Ball, Julian Borger and Glenn Greenwald
Guardian Weekly, Thursday 5 September 2013
[Jump to comments \(4142\)](#)



Through covert partnerships with tech companies, the spy agencies have inserted secret vulnerabilities into encryption software. Photograph: Kasper Pempel/Reuters

[Share](#) 31192
[Tweet](#) 11.4K
[+1](#) 3.6k
[Pin it](#) 57
[in Share](#) 888
[Email](#)

[Article history](#)

World news
The NSA files · NSA · Surveillance · United States · US national security · Privacy

UK news
GCHQ

Technology
Internet · Data protection · Data and computer security

Series
Glenn Greenwald on security and liberty

More from Glenn Greenwald on security and liberty on



Efforts to Undermine Anonymity on the Web

theguardian

[News](#) | [US](#) | [World](#) | [Sports](#) | [Comment](#) | [Culture](#) | [Business](#) | [Money](#)

[News](#) > [World news](#) > [NSA](#)

Attacking Tor: how the NSA targets users' online anonymity

Secret servers and a privileged position on the internet's backbone used to identify users and attack target computers



Bruce Schneier

theguardian.com, Friday 4 October 2013 10.50 EDT

[Jump to comments \(131\)](#)



Tor is a well-designed and robust anonymity tool, and successfully attacking it is difficult. Photograph: Magdalena Rehova/Alamy

The online anonymity network Tor is a high-priority target for the National Security Agency. The work of attacking Tor is done by the NSA's application vulnerabilities branch, which is part of the systems intelligence directorate, or SID. The majority of NSA employees work in SID, which is tasked with collecting data from communications systems around the world.

According to a top-secret NSA presentation provided by the whistleblower Edward Snowden, one successful technique the NSA has developed involves exploiting the Tor browser bundle, a collection of programs designed to make it easy for people to install and use the software. The

- Largely failed to undermine Tor application
- Able to exploit vulnerabilities in the Tor-Firefox browser bundle
- Use “Quantum” servers (located at key locations on backbone) to execute MITM
- Easily the most detailed technical description of specific NSA exploits



Secret NSA Audit

- "2,776 incidents (/year) of unauthorized collection, storage, access to or distribution of legally protected communications" in DC/Ft. Meade alone
- *E.g.* NSA misread area code 202 as country code 20 & grabbed all the calls from Washington, D.C. instead of Egypt.



Repeated Problems with FISC Oversight

- NSA and DOJ failed to disclose information about how the programs worked to FISC
- **Section 215:** no intelligence official knew how program fully worked; never told the court
- **Section 702:** Collected tens of thousands of purely domestic emails, but never told court



LOVEINT and other intentional violations

arstechnica

MAIN MENU • MY STORIES: 0 • FORUMS SUBSCRIBE JOBS

LAW & DISORDER / CIVILIZATION & DISCONTENT

LOVEINT: On his first day of work, NSA employee spied on ex-girlfriend
New letter from NSA oversight to senator details 12 instances of obvious abuse.

by Cyrus Farivar • Sept 27 2013, 9:35am PDT

GOVERNMENT NATIONAL SECURITY 148

notbeforecoffee

In 2005, a National Security Agency employee was given his first day of access to the United States' SIGINT (signals intelligence) capability. So what did he do with his vast powers?

According to a newly published letter (PDF) by the NSA

NSA LEAKS

Key Senator wants to ban bulk surveillance, leading to Democratic showdown



the problem(s)



two questions:

Is it legal?

Is it legitimate?



Parts of the Program are Illegal and Unconstitutional

- From 2001 to 2004/5:
 - the program was operating in violation of statutes, the Constitution, and without any type of judicial oversight
- Today:
 - Section 215: 1st and 4th Amendment; violates statute
 - Section 702: 4th Amendment problems



The Program is Absolutely Illegitimate

- “Do you think a program of this magnitude, gathering information involving a large number of people involved with the telephone companies and so on, could be indefinitely kept secret from the American people?”
- Neither the public, nor Congress, nor the Judiciary were meaningfully in debating propriety of the Program, nor the laws that “support” it

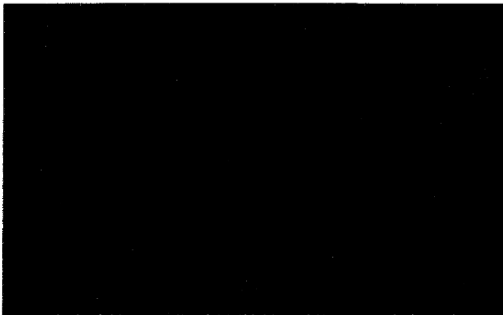
- Rep. Bob Goodlatte (R-Va) to Bob Litt,
General Counsel ODNI (July 2013)



October 3, 2011 FISC Opinion

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



MEMORANDUM OPINION

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court")

“[T]he government’s revelations . . . mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major [intelligence] collection program.”

“The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications.”



what we're doing

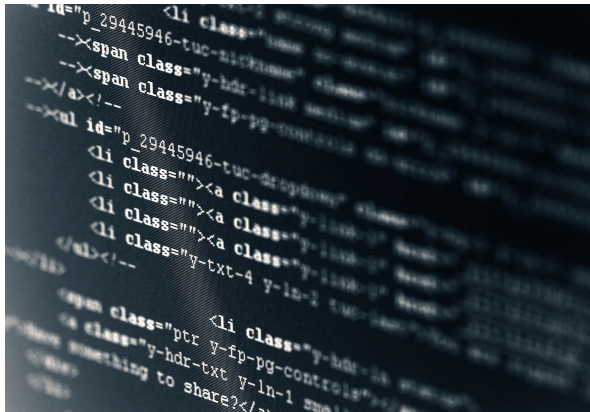


What EFF is doing:

- Litigation
 - *Jewel v. NSA* (filed in 2008)
 - *First Unitarian v. NSA* (filed in July)
 - *EFF v. DOJ* (FOIA cases, 215 and FISC)
- Legislation
 - Push for new Church Committee
 - Amend Section 215 and FAA
- Technology (HTTPS Everywhere)



what are you doing?



&



West Coast Code

East Coast Code



United States v. Kincade

A decision, like the majority's in this case, “that draws **no hard lines and revels in the boon that new technology will provide to law enforcement**, is an engraved **invitation to future expansion**. And when **that inevitable expansion comes**, we will look to the regime we approved today as the **new baseline** and say, **this too must be OK** because **it's just one small step** beyond the last thing we approved. My colleagues in the plurality assure us that, when that day comes, they will stand vigilant and guard the line, but **by then the line — never very clear to begin with — will have shifted**. The fishbowl will look like home.”



questions?

Mark Rumold
Staff Attorney, EFF
mark@eff.org

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