Intelligence Accountability

Implications of the „Snowden Case“ for legislative oversight

ELECTRONIC INTERCEPTION

Easier then ever before

U.S. National Security Agency surveillance

Pre-2001

- ECHELON
- Main Core
- PROMIS

2001

- BLARNEY
- RAGTIME
- Turbulence
- PINWALE (NSA internet database)
- MAINWAY (NSA call database)
- Upstream (incl. Room 641A)

2007

- **PRISM**
- Boundless Informant
- **X-Keyscore**
- Dropmire
- Fairview
- Surveillance Detection Unit
- Bullrun

GCHQ collaboration

- IMP
- **Tempora**
- Mastering the Internet
- Global Telecoms Exploitation

Discontinued

- Trailblazer Project
- ThinThread
- President's Surveillance Program
- Terrorist Surveillance Program STELLARWIND

Hyperbolic map of the Internet

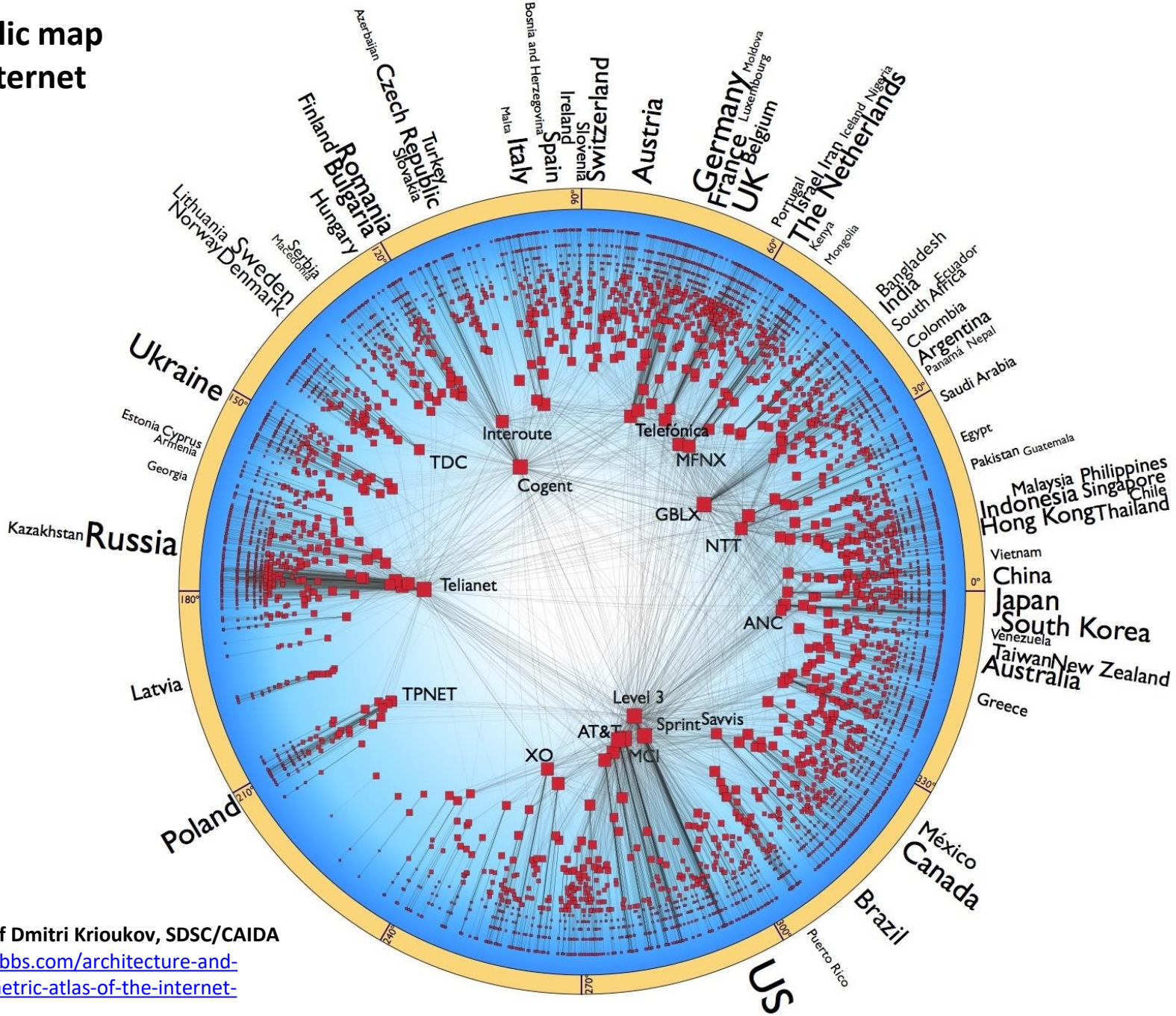
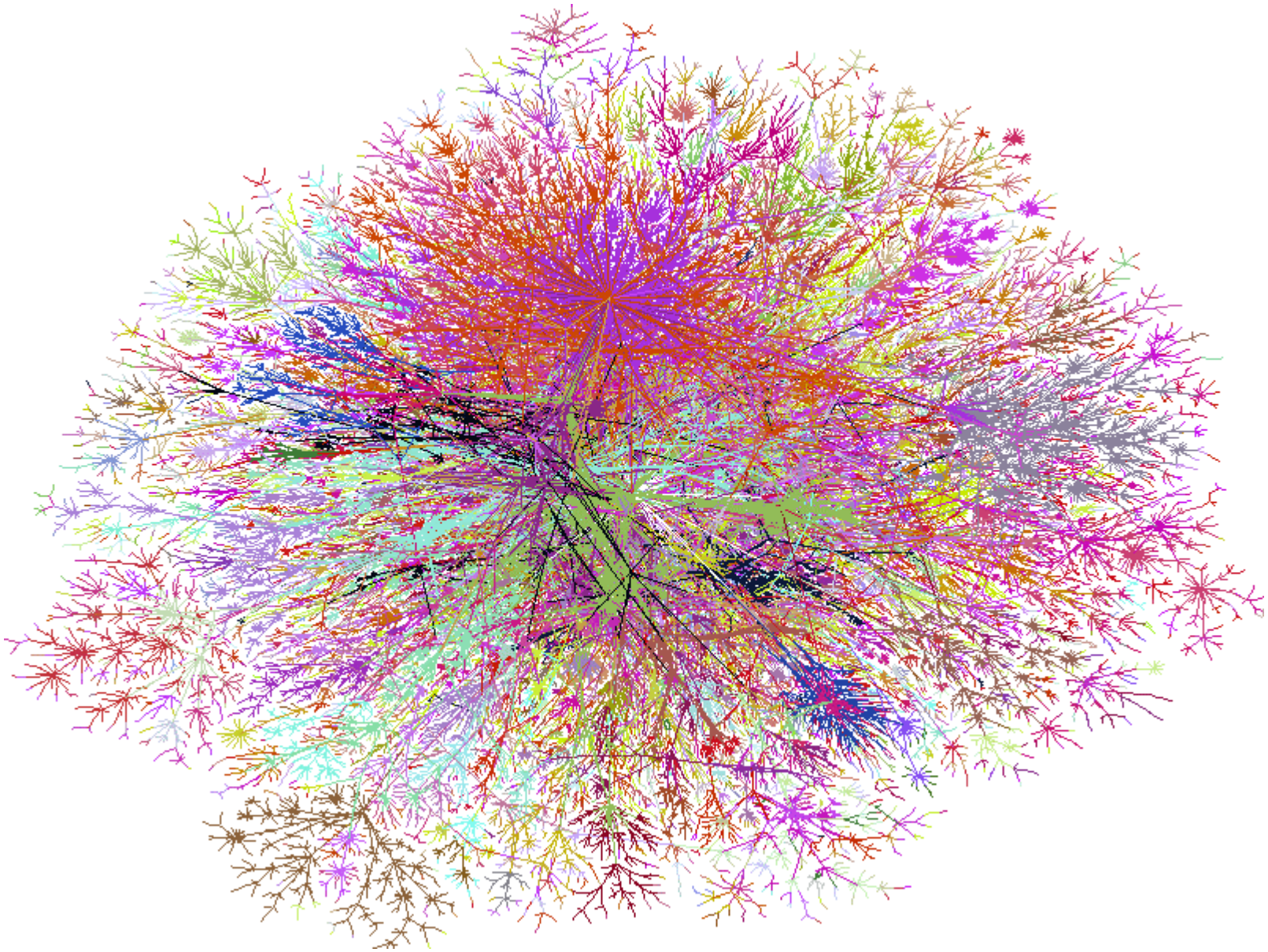


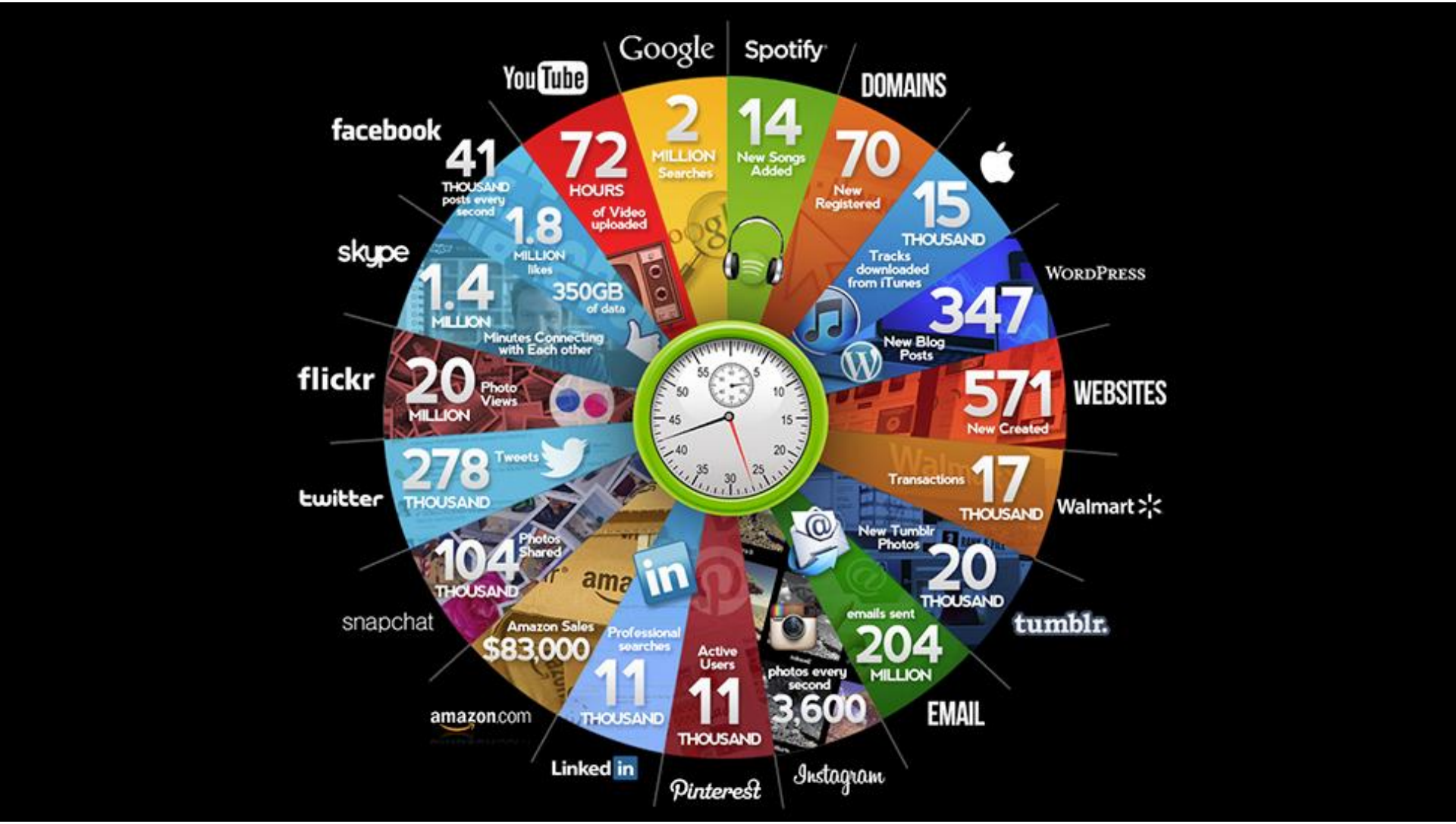
Image courtesy of Dmitri Krioukov, SDSC/CAIDA
http://www.drdobbs.com/architecture-and-design/first-geometric-atlas-of-the-internet-cr/227400098

Internet topology (connections of all the sub-networks in the world)



Credit: Bill Cheswick, Lumeta Corp
http://plyojump.com/classes/internet_era.php

On-line in 60 seconds…



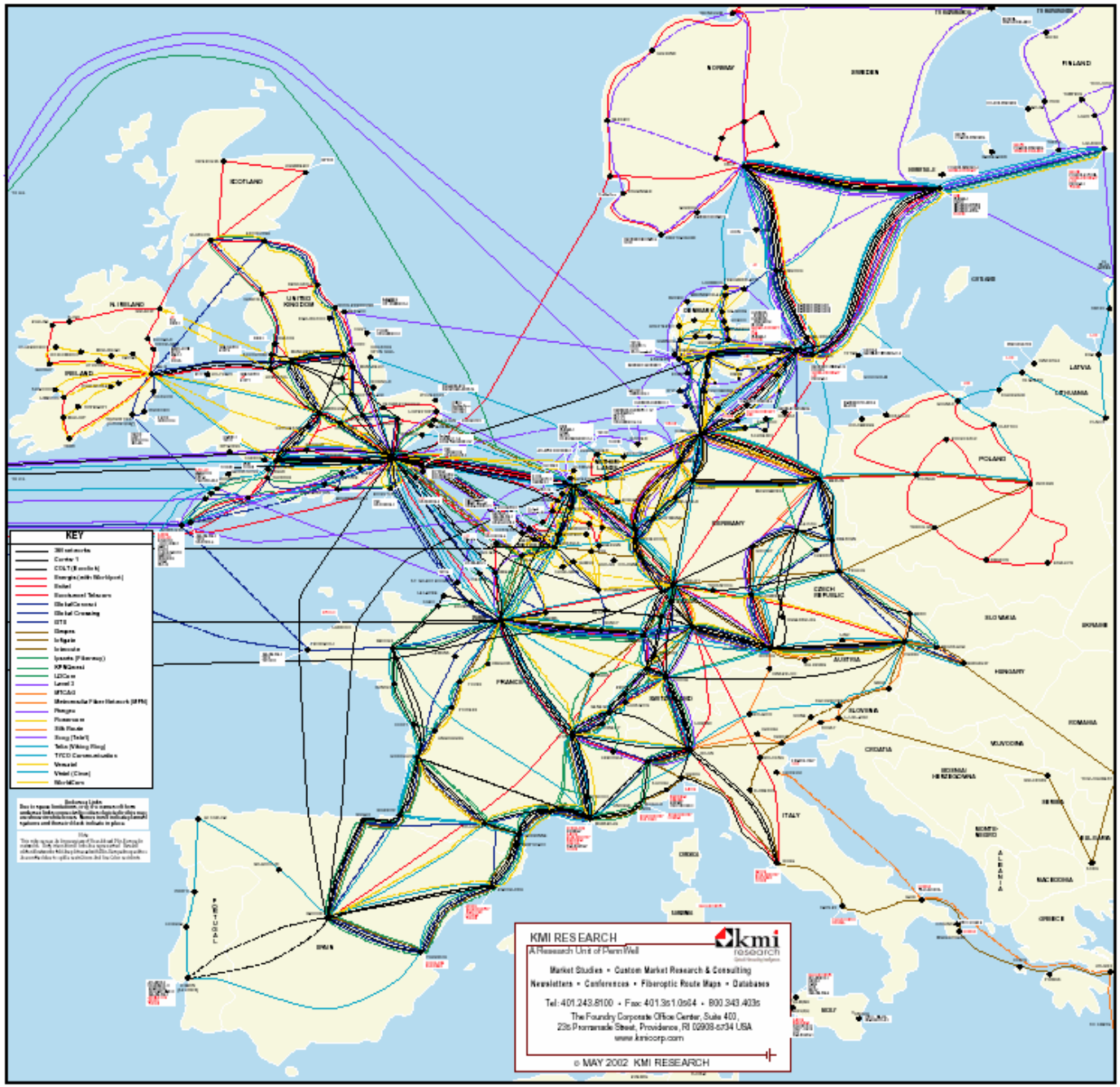
http://blog.qmee.com/qmee-online-in-60-seconds/

Typical modern telecommunication provider…

http://theconnectivist.wordpress.com/2013/08/14/what-may-move-america-movil-into-europe/

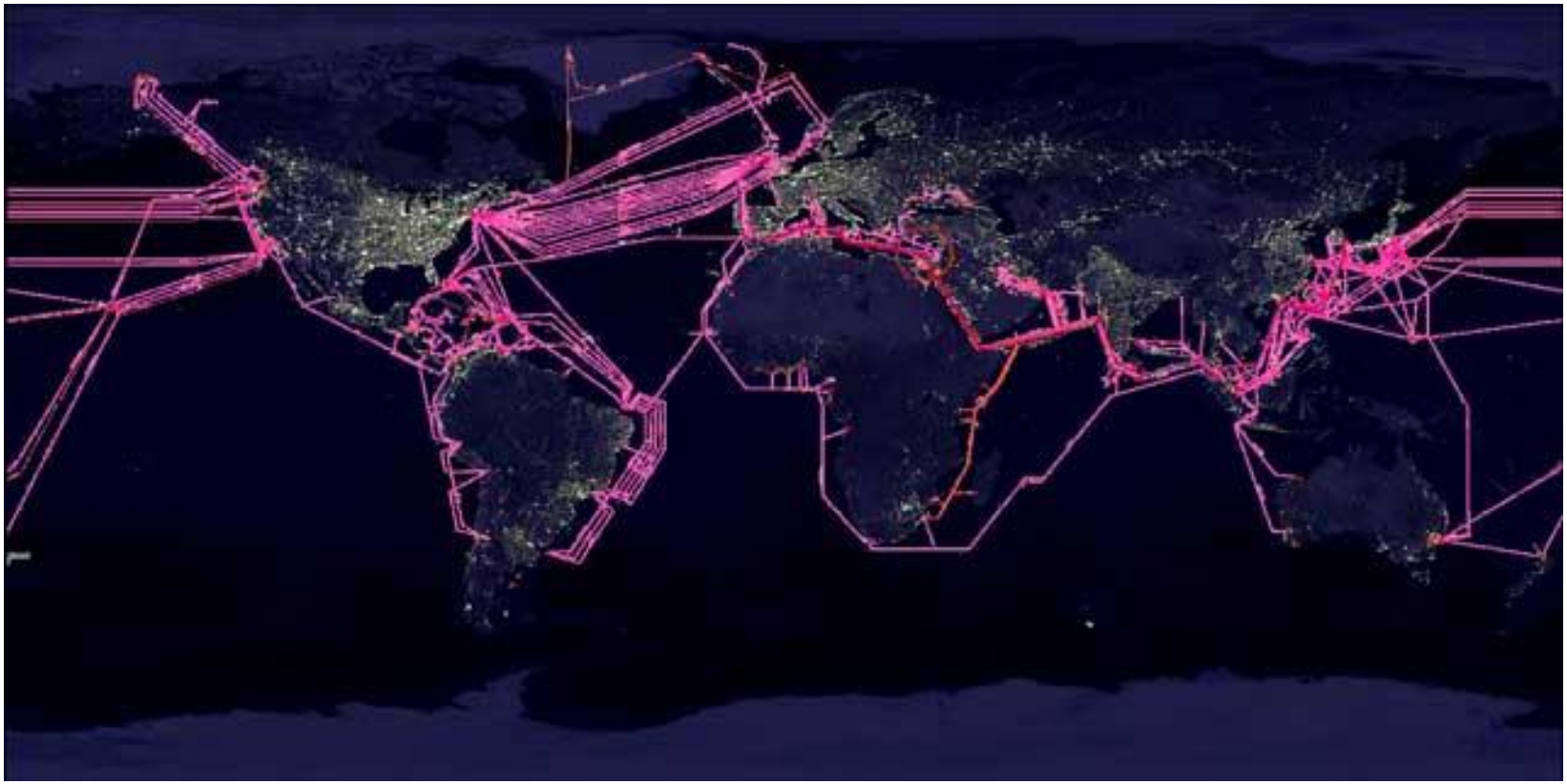
PAN EUROPEAN FIBEROPTIC NETWORK ROUTES PLANNED OR IN PLACE

http://www.lboro.ac.uk/gawc/rb/rb136.html



Today, virtually all long distance communications is carried over the installed fiber optic network.

http://www.thefoa.org/tech/ref/appln/FTTH.html



EDWARD SNOWDEN CASE

Whistleblower or traitor?

Major source: http://www.theguardian.com/commentisfree/series/glenn-greenwald-security-liberty

Edward Joseph Snowden

(born June 21, 1983)

NSA headquarters building in Fort Meade, Maryland, USA

(By Jaikumar Vijayan, Computerworld, Jun 5, 2014)

No one knows exactly how many documents Edward Snowden illegally accessed and downloaded while working as a contract employee for a National Security Agency (NSA) signals intelligence facility in Hawaii; some estimate as many as 1.3 million.

As a contracted NSA systems administrator with top-secret Sensitive Compartmented Information (SCI) clearance, Snowden certainly had access to millions of classified documents.

NSA officials claim the majority of the documents Snowden stole had little or nothing to do with domestic surveillance. But it is precisely the documents describing the NSA's purported domestic spying -- and those related to its surveillance of foreign leaders -- that have garnered the most attention.

Here are 10 of them.

1 PRISM

NSA documents obtained by Snowden described Prism as a program for collecting user data from Microsoft, Google, Facebook, Skype and several other major Internet companies. It allows analysts from the FBI's Data Intercept Technology Unit and the NSA's Special Source Operations group to search for and inspect specific items of interest flowing through the data streams of each of the companies.

Under the program, the NSA purportedly collects audio, video, email, photographs, documents and connection logs to help counterterrorism analysts track the movements and interactions of foreign nationals of interest.

In PowerPoint slides leaked by Snowden, NSA officials described Prism as the single biggest source of information used to prepare intelligence reports, including those prepared for White House daily briefings.


PRISM

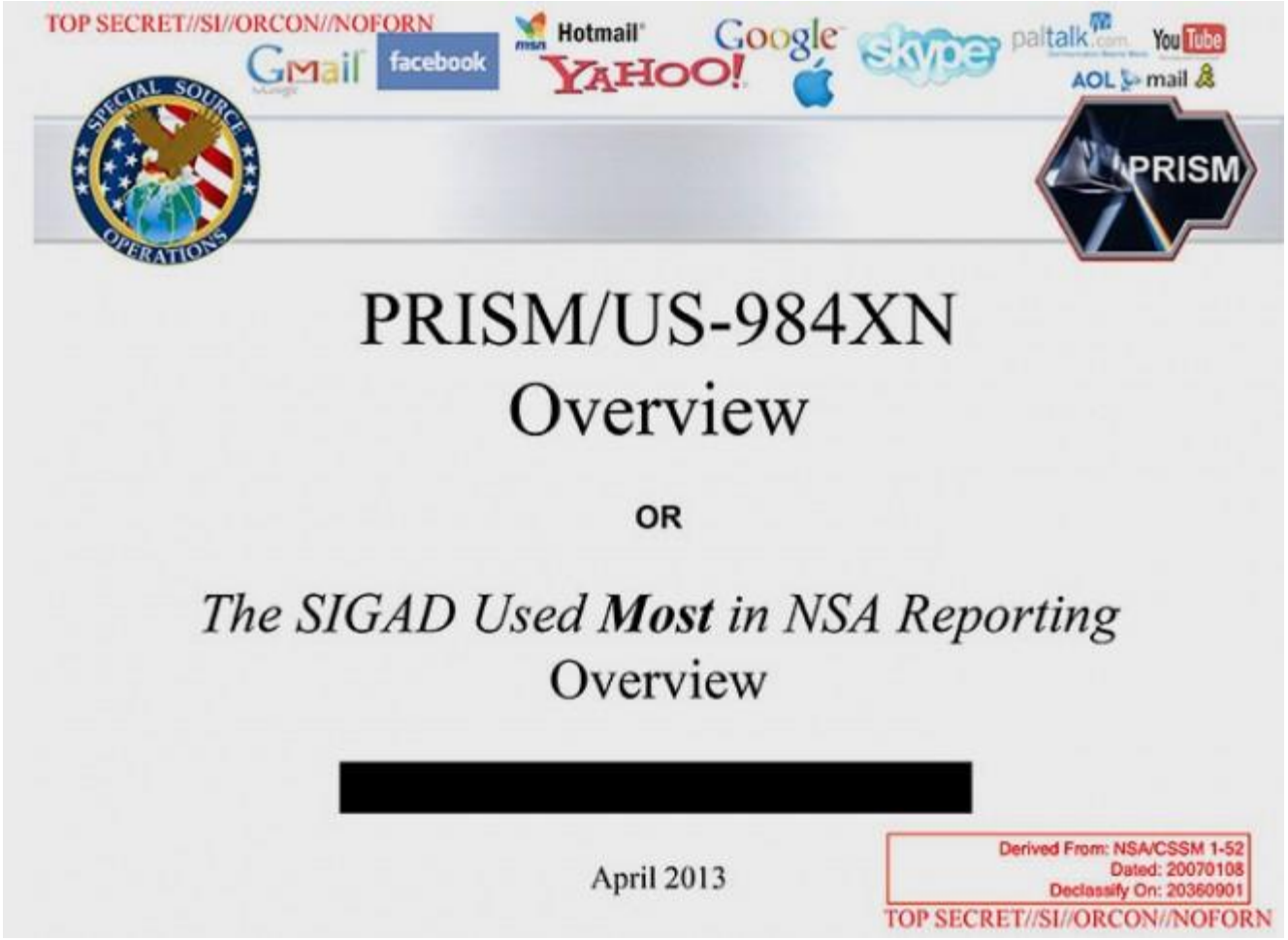


Photo: The Washington Post

NSA Prism program taps in to user data of Apple, Google and others

- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007

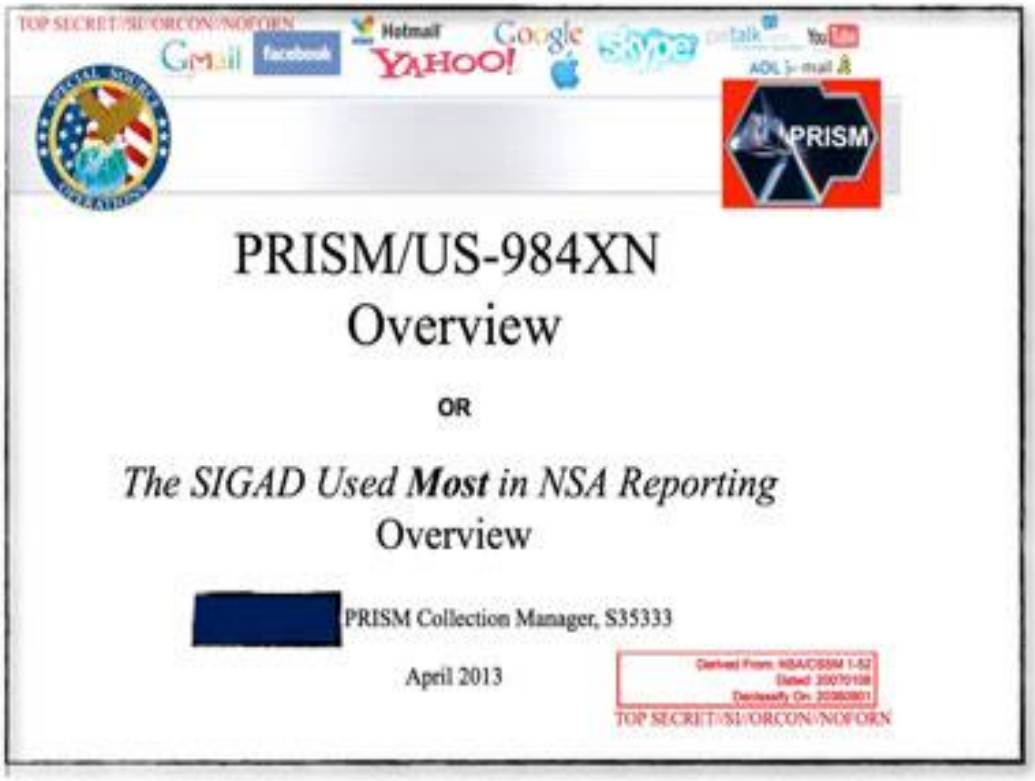


Photo: The Washington Post

Types of data that Prism can collect

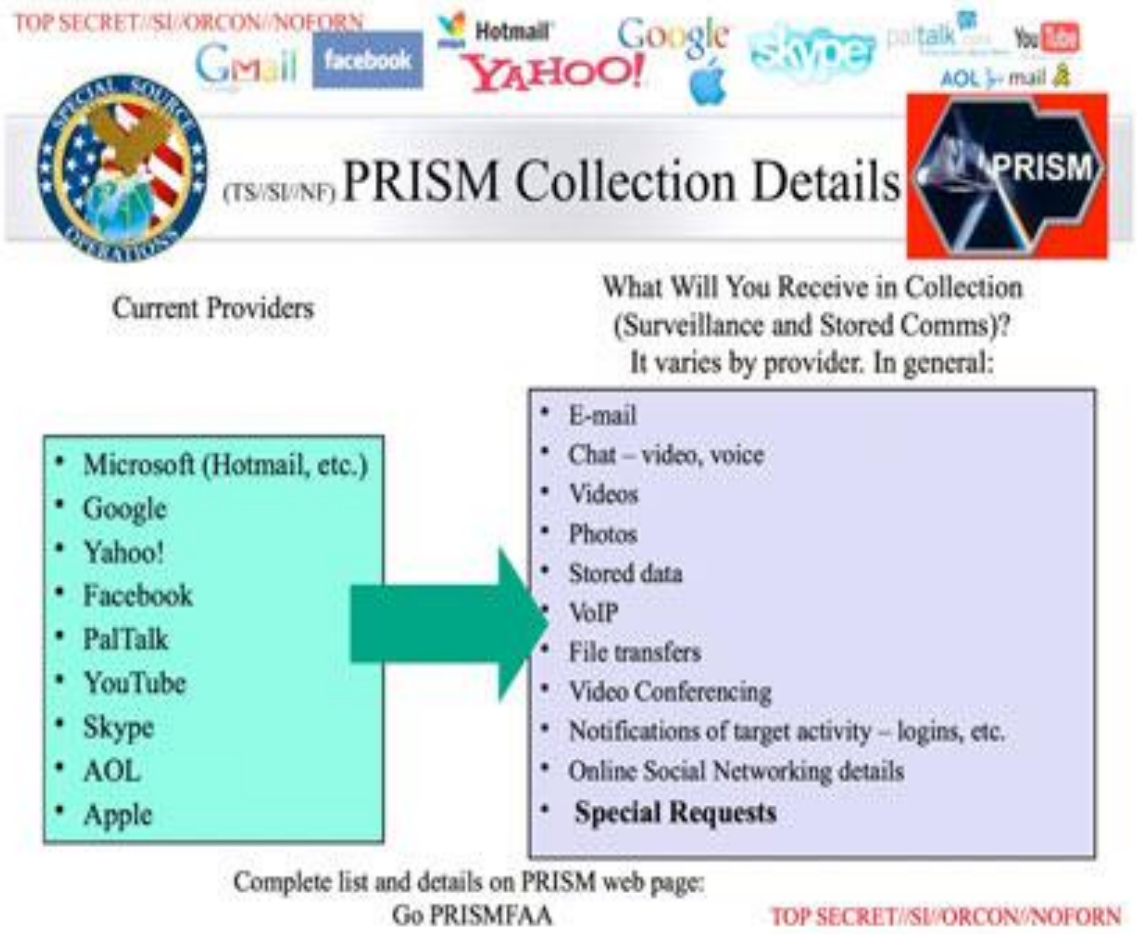


Photo: The Washington Post

2 Bulk phone metadata collection program

A secret court order obtained by Snowden revealed the existence of an NSA program for collecting daily phone metadata records from U.S. phone companies.

Under the program, the NSA collects records such as the originating and called numbers, call time and duration, location data, calling card numbers, International Mobile Station Equipment Identity numbers and other data pertaining to all domestic and international calls made from within the U.S.

The government says the data it is collects helps U.S. intelligence keep track of the communications of known or suspected terrorists.

Concerns over the program prompted President Barack Obama to announce changes aimed at restricting the data collected and the manner in which collected data is stored.

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

3 Xkeyscore

Documents and presentation slides obtained by The Guardian described Xkeyscore as a program that lets the NSA collect virtually any information about an individual's Internet activity anywhere in the world.

The program purportedly lets NSA analysts sift through enormous databases to gather data on emails, browsing and search histories, online chats and other online activity of any Internet user anywhere in the world.

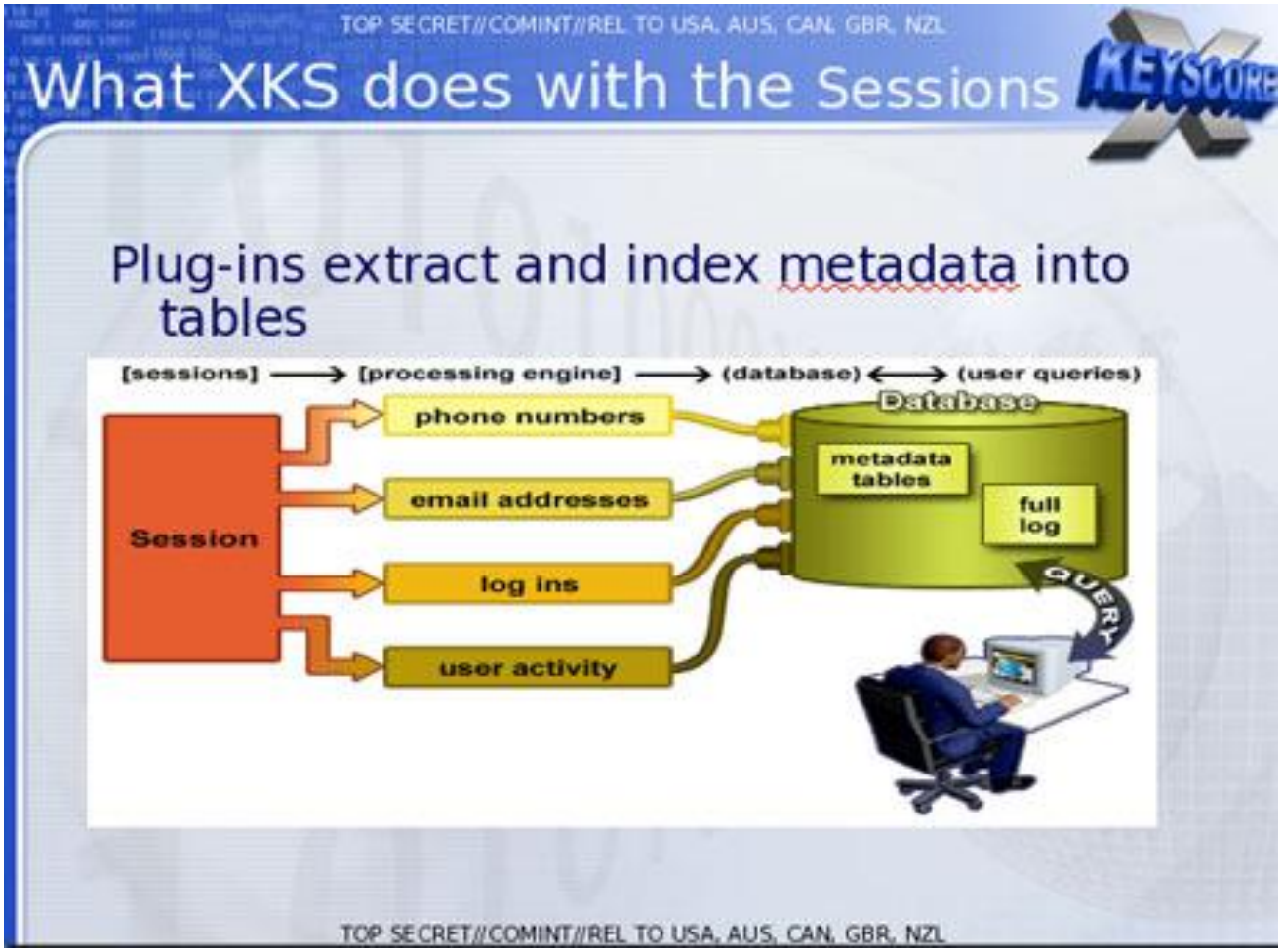
The XKeyscore system collects so much data that the vast majority of it can only be stored a few days at a time.

NSA officials have strongly denied many of the claims pertaining to the program's purported capabilities and the manner in which it is allegedly used.

One NSA presentation claims the XKeyscore program covers 'nearly everything a typical user does on the internet'

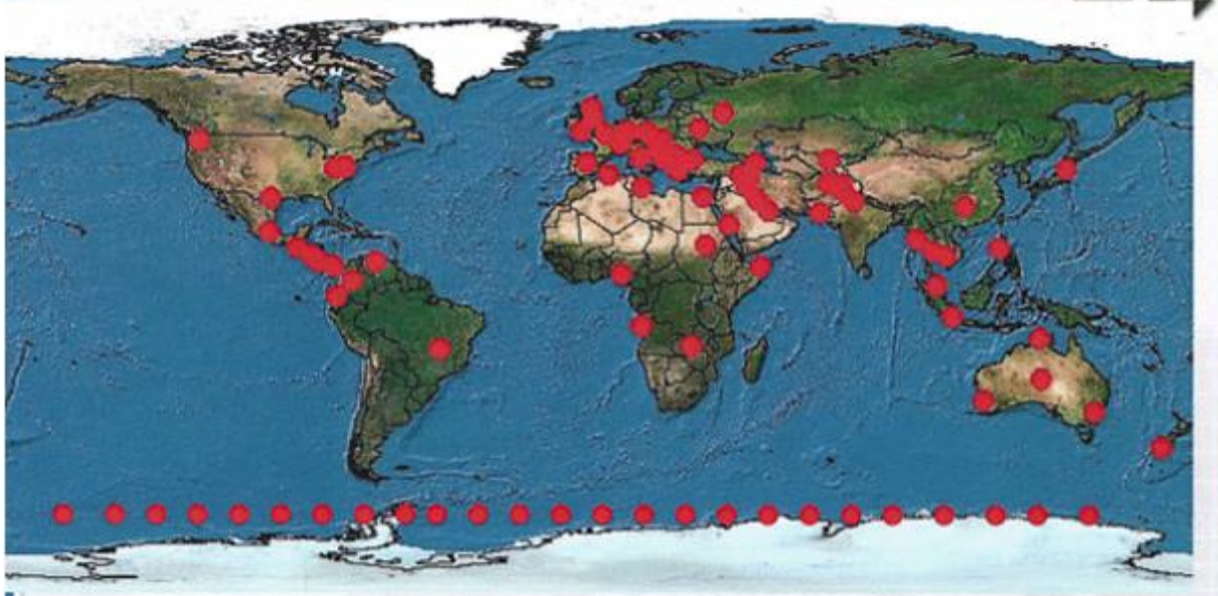
A top secret National Security Agency program **allows analysts** to **search with no prior authorization** through vast databases containing **emails, online chats and the browsing histories** of millions of individuals, according to documents provided by whistleblower Edward Snowden.

Real-time interception and storage of traffic data (metadata) as well as substantive data access



Communications that **transit** the United States and communications that **terminate** in the United States

Where is X-KEYSCORE?



Approximately 150 sites

Over 700 servers

4 Tempora

The secret surveillance programs revealed by Snowden included a massive data collection program named Tempora, which is run by Britain's Government Communications Headquarters (GCHQ) in cooperation with the NSA.

Under the program, the GCHQ collects petabytes worth of information daily from data interceptors placed directly on regional and transatlantic fiber-optic cables carrying huge volumes of Internet data into and outside the U.K. from exchanges and Internet servers in North America and elsewhere.

Data intercepted under the program include email content, records of phone calls, Facebook entries and Internet browsing histories.

The leaked documents showed that as of May 2012, the NSA had assigned 250 analysts -- and the GCHQ had 300 -- to pore over data gathered under Tempora.

Image courtesy The Government Communications Headquarters (GCHQ) operates "Tempora. Credit: Ministry of Defence (Open Government Licence v1.0)

5 Efforts to weaken data encryption

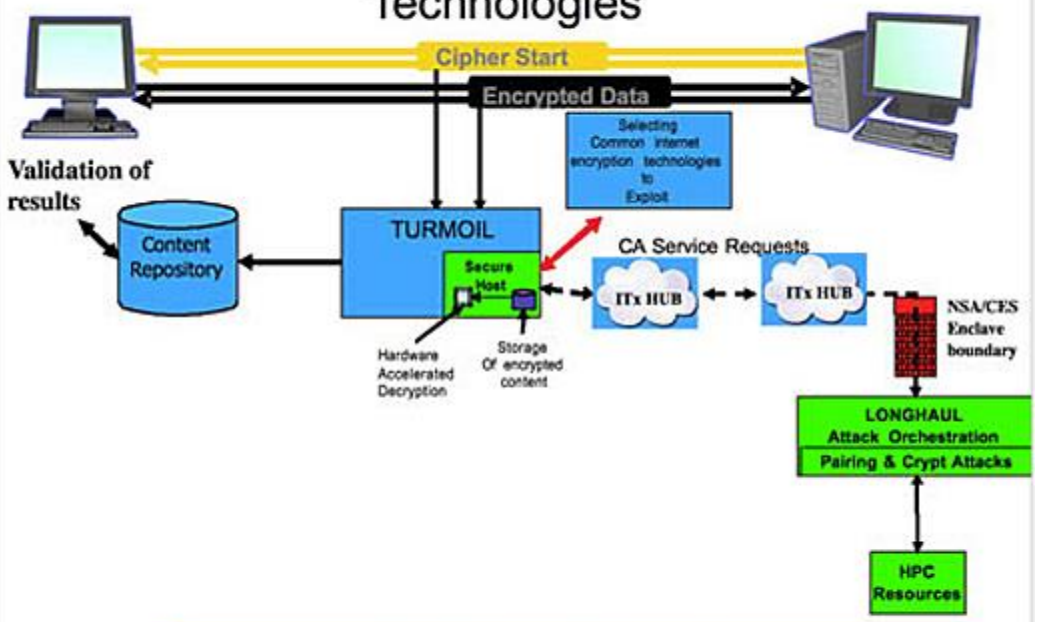
One of Snowden's most controversial leaks involved apparent efforts by the NSA and GCHQ to systematically weaken the commercial encryption tools designed to protect everything from emails to highly sensitive documents.

The methods included building backdoors into technology projects, using sophisticated supercomputers to crack encryption algorithms and forcing vendors to hand decryption keys using secret court orders.

Documents obtained from Snowden showed the U.S. intelligence community reportedly spending 20% of its nearly $53 billion annual budget on cryptographic projects and operations.

The NSA spends $250 million a year on a program under which it tries to work with vendors of encryption technologies to allegedly make the products more easily exploitable.

Exploitation of Common Internet Encryption Technologies



6 Tapping smartphones

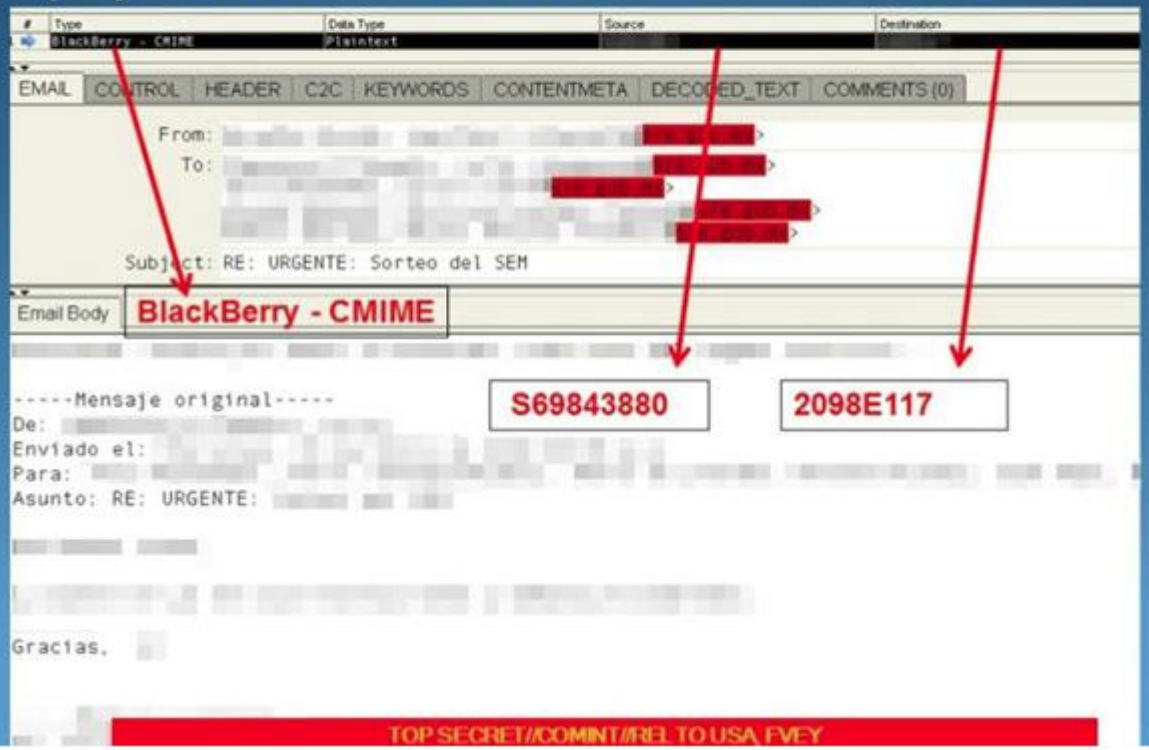
The Snowden leaks showed that in addition to collecting phone metadata and Internet data, the NSA and the GCHQ are also capable of harvesting data directly from BlackBerrys, iPhones, Android-powered phones and other smartphones.

Der Spiegel, which was one of the first to break the story, noted that the agencies have the ability to tap a lot of smartphone data, including contact lists, location information, SMS traffic and notes.

The NSA apparently has set up separate teams that specialize in gathering information from specific mobile operating systems.

It also has the ability to read messages sent via BackBerry's Enterprise Server, the publication said, quoting documents obtained from Snowden

(U) Post Processed BES collection



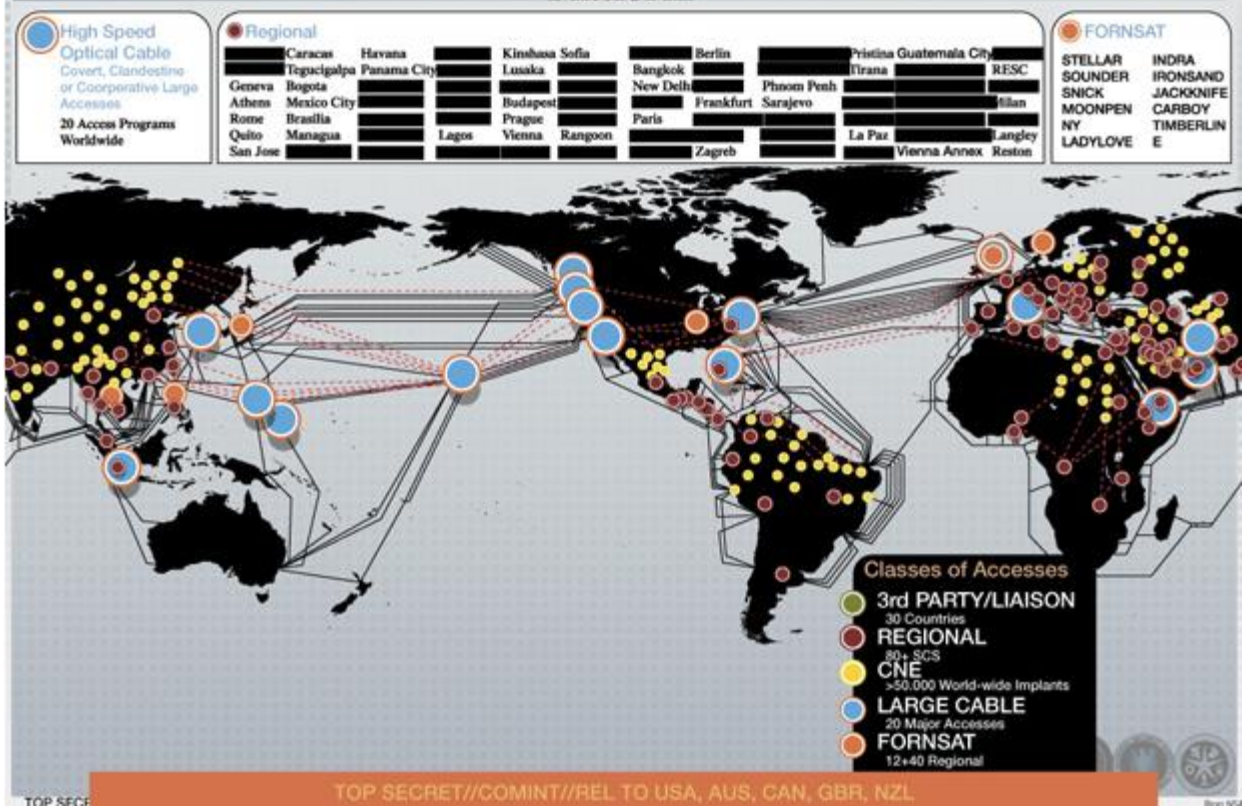
7 NSA hacked 50,000 computers worldwide

An elite NSA hacking united known as Tailored Access Operations has infected at least 50,000 computers worldwide with specialized malware referred to as "implants" by the agency, a leaked Snowden slide revealed.

The implants were likened to sleeper cells that could be activated at any time with a single click.

The slide showed that in addition to the 50,000 implants, the NSA's Computer Network Exploitation (CNE) unit also has dozens of special data collection facilities spread out across the globe for collecting Internet data and foreign satellite communications.

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform



8 Role of private companies in NSA data collection

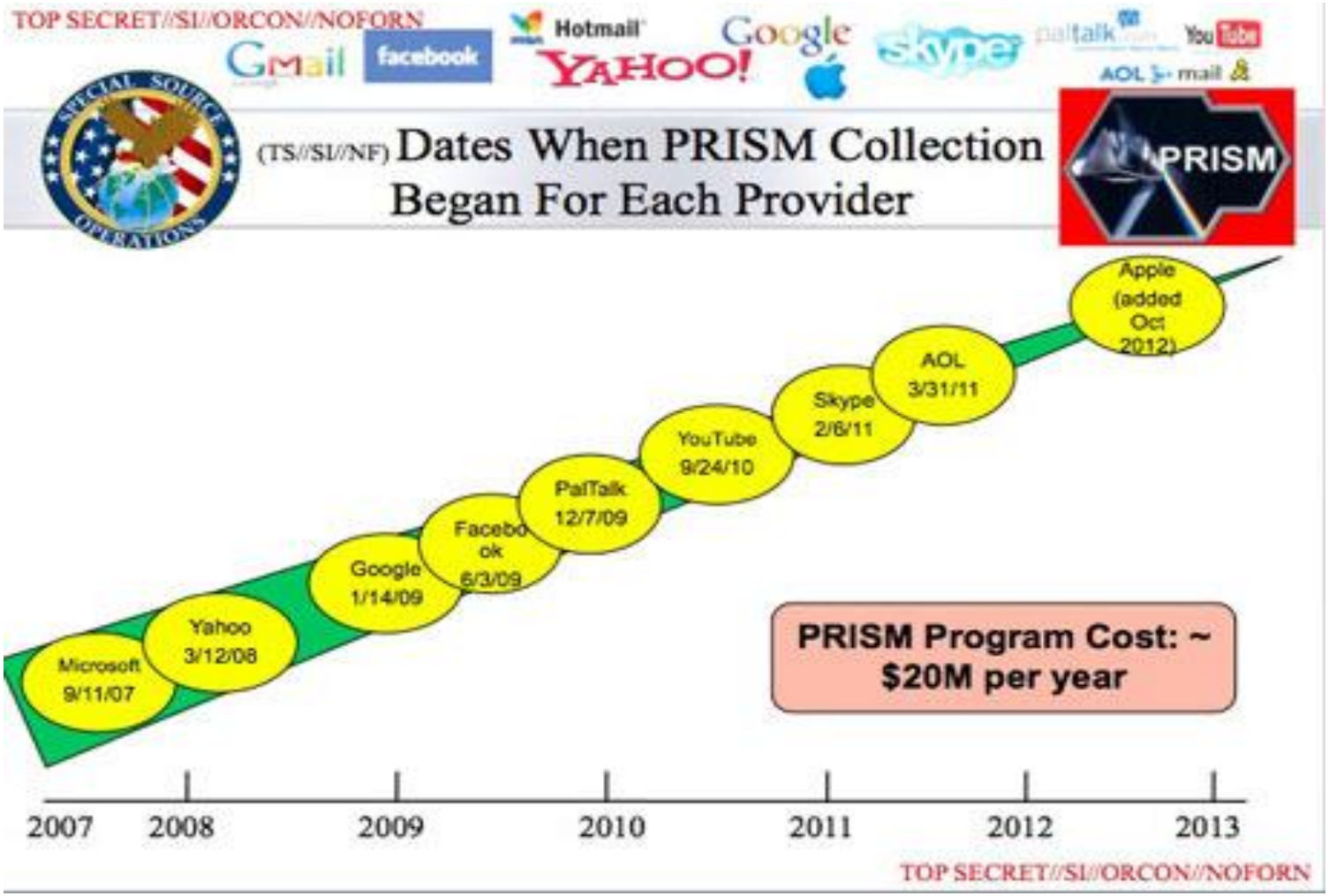
Snowden's leaks raised several questions about the role private companies played in helping the NSA collect data.

The concerns peaked last December, when Reuters revealed that EMC Corp.'s security division, RSA, might have enabled a backdoor in one of its encryption technologies at the behest of the NSA.

Companies like Google, Microsoft, Yahoo and Facebook have all vehemently denied that they have voluntarily given customer data to the NSA or any other intelligence agency.

They have claimed that the only circumstances under which they might have provided data is when compelled to do so via court order.

Prism access to providers infrastructure



„Companies are **legally obliged** to comply with requests for users' communications **under US law**, but the **Prism** program allows the intelligence services **direct access to the companies' servers**. The NSA document notes the operations have "assistance of communications providers in the US“.

9 NSA spies on world leaders

A document leaked by Snowden showed that the U.S. secretly monitors the phone conversations of at least 35 world leaders.

Though the document did not identify the leaders being monitored, it lent credibility to claims by various world leaders that the NSA was monitoring their phones.

Among those who claimed they were spied on were German Chancellor Angela Merkel, Brazilian President Dilma Rousseff and Mexico's former president Felipe Calderon.

Meanwhile, in a report that the NSA denied, French newspaper Le Monde claimed that the NSA had gathered data on millions of French citizens by spying on French telecommunications company Alcatel-Lucent.

10 NSA tracks and hacks systems administrators

The Intercept, a publication co-founded by Glen Greenwald, the Guardian reporter who first broke the story on the Snowden leaks, in March claimed that a document provided by Snowden shows the NSA infiltrates computers belonging to systems administrators who work for foreign telecommunications and Internet companies.

The documents show that the NSA aspired to build an international hit list of system administrators to target as part of its surveillance effort.

In addition to trying to get system administrator passwords, the agency also tries to obtain network maps and other data from targeted systems administrators outside the U.S., the publication claimed.

SECRET//SI//REL TO USA, FVEY

(U) I hunt sys admins (part 2)

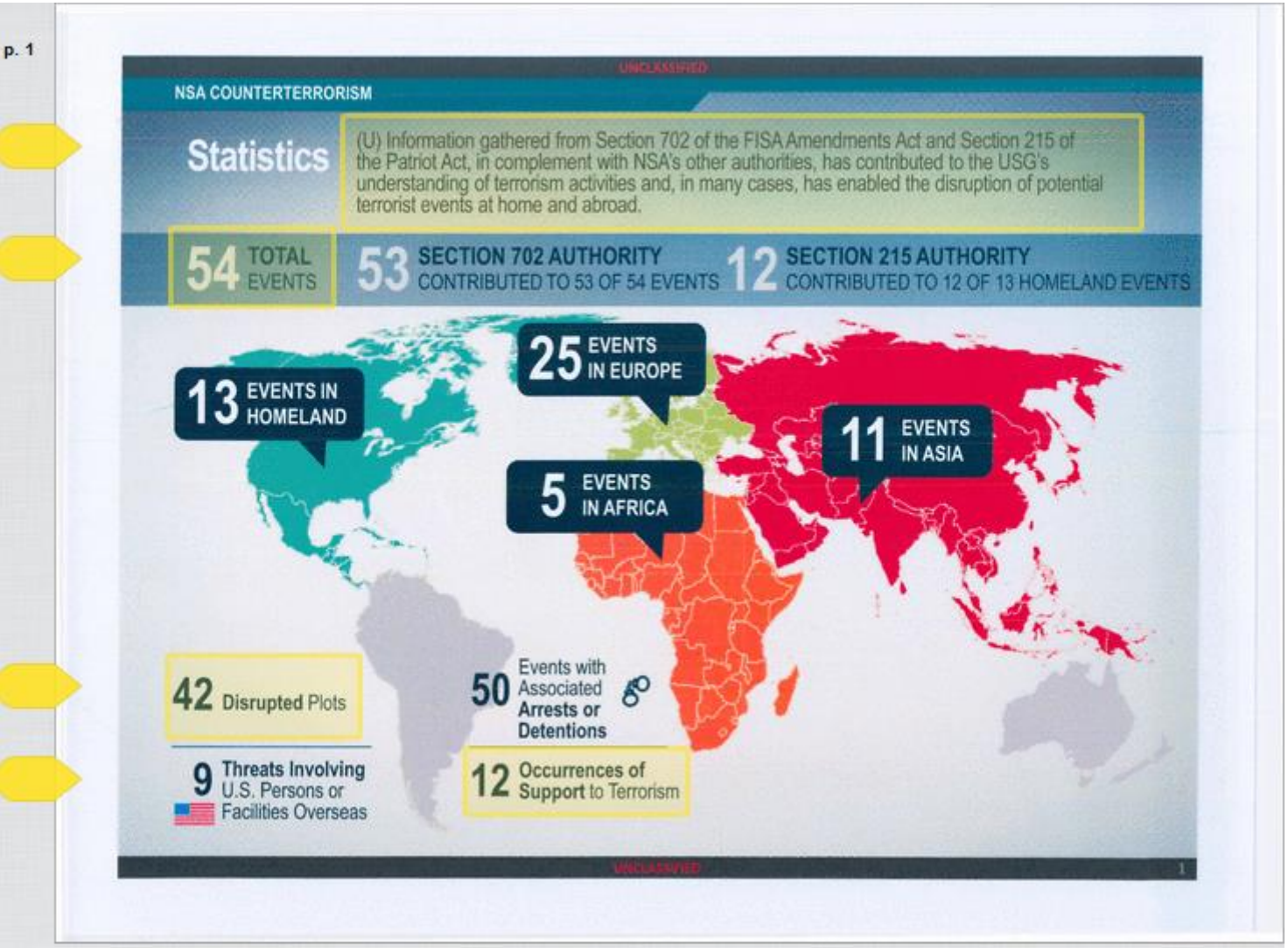
Entry tags: admin, cne, infra

eant to provide a background for *why* it's good
ow this, feel free to skip forward to the next sectio

our overall goal is to produce intelligence to give t
, is whenever a target uses technology to comm
orts on it. Sounds simple enough...except for the
ks we collect. We can't collect everything all the tir

What's in Edward Snowden's 41-slide PowerPoint deck that's so hot that nobody dare publish it?

„NSA Claims Of Snooping Stopping Attacks Fall Flat“



Two weeks after Edward Snowden's first revelations about sweeping government surveillance, President Obama shot back. "We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany," Obama said during a visit to Berlin in June. "So lives have been saved."

QUESTION OF LEGALITY

National law vs. International law

While the **Fisa Amendments Act** of 2008 **requires** an **individualized warrant** for the **targeting of US persons**, NSA analysts are permitted to intercept the communications of such individuals **without a warrant** if they are in **contact** with one of the NSA's **foreign targets**.

NSA said:

"NSA's activities are focused and specifically **deployed against** – and only against – legitimate **foreign** intelligence targets in response to requirements that our **leaders need** for information necessary to **protect** our nation and its **interests**."

"**XKeyscore** is used as a part of NSA's **lawful** foreign signals intelligence collection system."

"Allegations of widespread, unchecked analyst access to NSA collection data are simply **not true**. Access to XKeyscore, as well as all of NSA's analytic tools, is **limited** to only those personnel who **require access for their assigned tasks** … In addition, there are multiple **technical, manual and supervisory checks and balances** within the system to **prevent** deliberate **misuse** from occurring."

"**Every search** by an NSA analyst is **fully auditable**, to ensure that they are proper and within the law."

"These types of programs allow us to collect the information that enables us **to perform our missions successfully** – to defend the nation and to protect US and allied troops abroad."

- The revelation also **supports concerns** raised by **several US senators** during the **renewal of the Fisa Amendments Act in December 2012**, who warned about the **scale of surveillance the law might enable**, and **shortcomings in the safeguards it introduces.**

- When the FAA was first enacted, defenders of the statute argued that a **significant check on abuse** would be the **NSA's inability** to **obtain** electronic communications **without the consent of the telecom and internet companies** that control the data. But the **Prism** program **renders that consent unnecessary**, as it **allows** the agency to **directly** and **unilaterally** seize the communications off the **companies' servers**.

- A senior administration official said in a statement: "The Guardian and Washington Post articles refer to collection of communications pursuant to **Section 702** of the **Foreign Intelligence Surveillance Act**. This **law does not allow** the **targeting** of any **US citizen** or of **any person located within** the **United States**.
- "The program is **subject to oversight** by the **Foreign Intelligence Surveillance Court**, the **Executive Branch**, and **Congress**. It involves extensive procedures, specifically approved by the court, to ensure that **only non-US persons outside the US are targeted**, and that minimize the acquisition, retention and dissemination of incidentally acquired information about US persons.“
- "This **program was recently reauthorized by Congress** after extensive hearings and debate.
- "Information collected under this program is **among the most important and valuable intelligence information we collect**, and is used to **protect** our nation from a wide variety of threats.“
- "The Government may only use Section 702 to acquire foreign intelligence information, which is specifically, and narrowly, defined in the Foreign Intelligence Surveillance Act. This requirement applies across the board, regardless of the nationality of the target."

Snowden:

„In some cases, the so-called **Five Eye Partners** (the intelligence services of United States, Britain, Australia, New Zealand and Canada) go beyond what NSA itself does.

For instance, the **UK's Government Communications Headquarters (GCHQ)** has a system called **TEMPORA**. TEMPORA is the signals intelligence community's first **"full-take"** Internet buffer that doesn't care about content type and pays only marginal attention to the Human Rights Act. It snarfs everything, in a rolling buffer to **allow retroactive investigation** without missing a single bit. Right now the buffer can hold **three days of traffic**, but that's being improved. Three days may not sound like much, but remember that **that's not metadata**. "Full-take" means **it doesn't miss anything**, and ingests the entirety of each circuit's capacity. If you send a single ICMP (Internet Control Message Protocol) packet and it routes through the UK, we get it. If you download something and the CDN (Content Delivery Network) happens to serve from the UK, we get it. If your sick daughter's medical records get processed at a London call center … well, you get the idea.“

International legality?

- Depends on the active / passive role:
  - Lawful from the standpoint of intercepting agency and country to which agency belongs
  - Unlawful from the standpoint of targeted country
- International legislation:
  - Universal Declaration of Human Rights (UDHR)
  - International Covenant on Civil and Political Rights
  - Convention for the Protection of Human Rights and Fundamental Freedoms
  - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  - European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  - Directive 97/66/EC of the European parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
  - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
  - ….

QUESTIONS OF EFFECTIVENES AND EFFICIENCY

LEGISLATIVE OVERSIGHT

Preconditions for the oversight

- Purpose of electronic telecommunication interception
- Domestic / international traffic
- Traffic data / substantive data
- Targeting
  - Strategic interception (non-specific targets)
  - Tactical interception (specific targets)
  - Foreign / domestic targets
  - „Collateral“ damage (correspondents of the target)
- Authorization procedure
  - Initiative (agency management…)
  - Decision (executive, judicial…)
  - Granting (warrant)

Preconditions for the oversight

- Execution (agency, operator, other state body…)
- Data and information processing:
  - Storage
  - Data and information protection
  - Access
  - Collation
  - Analysis
  - Synthesis
  - Reporting
  - Dissemination
  - International intelligence cooperation

Preconditions for the oversight

- Internal supervision
  - Role of management (all levels)
  - Importance of automated log files
- External oversight - ex ante /ex post
  - Judicial
  - Executive (government)
  - Parliamentary
  - Specialized bodies
- Oversight of services and operators
- INTERNATIONAL OVERSIGHT?

Preconditions for the oversight

- Problems of oversight:
  - Responsibilities and powers
  - Access to technical premises
  - Technical knowledge
  - Technical support
  - Mutual trust
  - Finding balance between protection of human right to information privacy and lawful intrusion of this right is not always an easy task
  - Quis custodiet ipsos custodes?