NSA/BND/GCHQ-Skandal auf einen Blick

c1/4h by sPhErE,
2015-07-30

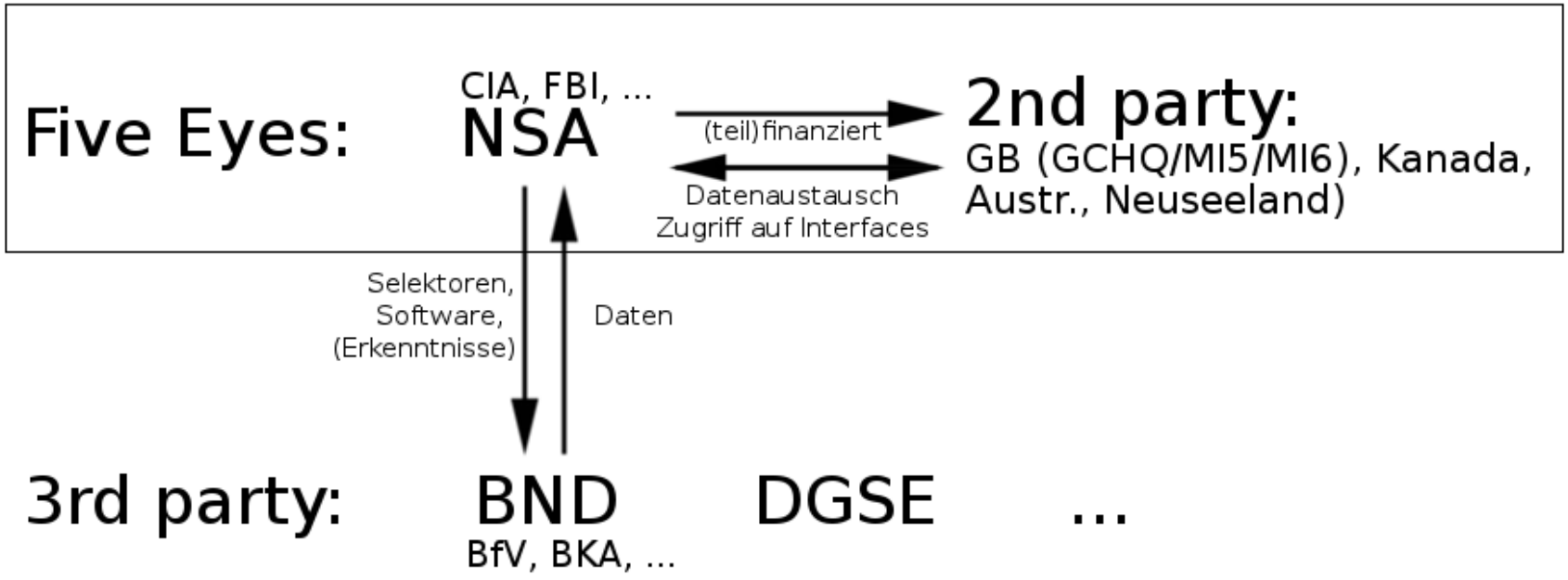
powered by LaTeX

Diese c$^{1}/_{4}$h auf einen Blick:

- Wer belauscht wen?
- Abhörprogramme, insbesondere:
  - Prism
  - Upstream
  - Tempora
  - XKeyscore

Wer lauscht?

- Mindestens:



Wer lauscht?

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL
Approved SIGINT Partners
Second Parties
Australia
Canada
New Zealand
United Kingdom
Coalitions/Multi-lats
AFSC
NATO
SSEUR
SSPAC
Third Parties
Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE
TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Wer lauscht?

- Diensteanbieter:
  - Zwang zur Herausgabe (Anordnung von Geheimgericht)
  - Aber: Strategische Partnerschaften

Wer lauscht?

TOP SECRET//COMINT//X1
NSA Strategic Partnerships
Alliances with over 80 Major Global Corporations Supporting both Missions
• Telecommunications & Network Service Providers
• Network Infrastructure
• Hardware Platforms Desktops/Servers
• Operating Systems
• Applications Software
• Security Hardware & Software
• System Integrators
AT&T
Qwest
EDS
H-P
Motorola
CISCO
Qualcomm
Oracle
IBM
Intel
Microsoft
Verizon
TOP SECRET//COMINT//X1

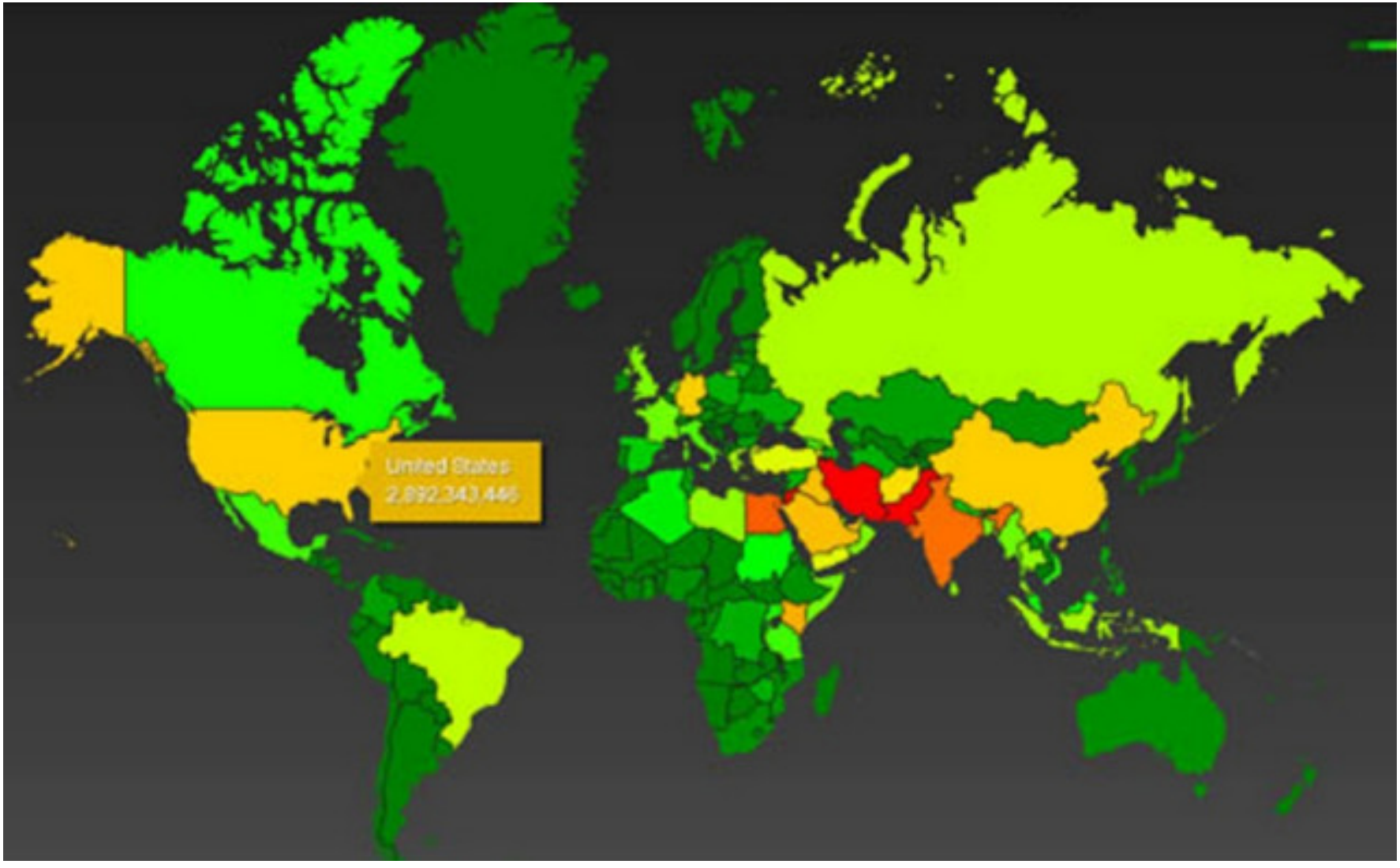
Wer lauscht?

- Diensteanbieter:
  - Zwang zur Herausgabe (Anordnung von Geheimgericht)
  - Aber: Strategische Partnerschaften
  - und: Zahlungen für Filterungs- und zugriffserleichternde Software

Wer wird belauscht?

- Mindestens:
  - **NSA,GCHQ,BND:** Bevölkerung weltweit

NSA's most wanted:



- Mind. 6 Mrd Metadatensätze täglich weltweit (Spiegel)

Wer wird belauscht?

- Mindestens:
  - **NSA,GCHQ,BND:** Bevölkerung weltweit
  - **NSA,BND:** Ministerien und Regierungschefs weltweit (Merkel, Schröder, Kohl,...)
  - **NSA:** Gebäude der Europäischen Union, Vereinte Nationen, Europäische Botschaften
  - **NSA:** internationale Mainstream-Presse
  - **NSA:** NSA Untersuchungsausschuss

Abhörprogramme

- **NSA operated:**
  - **Prism:** Internetdienste (Frontdoor)
  - **Upstream:** Untersee-Glasfaserkabel
  - **XKeyscore:** Vor-Ort-Analyse aller Daten
  - **Eikonal/Transit (mit BND und u.a. Telekom):** Abgriff bei deutschen Internetknoten (2004 - 2008)
  - **Bullrun:** Knacken von Verschlüsselungen, Manipulation von Standards, Infiltration von Certificate Authorities
  - **Mystic, Tarex, Dishfire, Globe...**
- **GCHQ operated:**
  - **Tempora:** Untersee-Glasfaserkabel
  - **Muscular (mit NSA):** Internetdienste (Backdoor)
- **DGSE operated:**
  - Anzapfen von Unterseekabeln

PRISM

- **Prism I:** NSA intern, zur "Aktenverwaltung“
- **Prism II:** NATO-Programm
- **Prism III:** von Snowden enthüllt (nachfolgend nur "Prism")
  - Wichtigste Frontdoor-Quelle für NSA Berichte
  - Erzwungener Zugriff auf "ausländische“ Inhalte über Konzerne
  - Echtzeiterfassung von 100000 aktiven Zielpersonen

(TS//SI//NF) FAA702 Operations

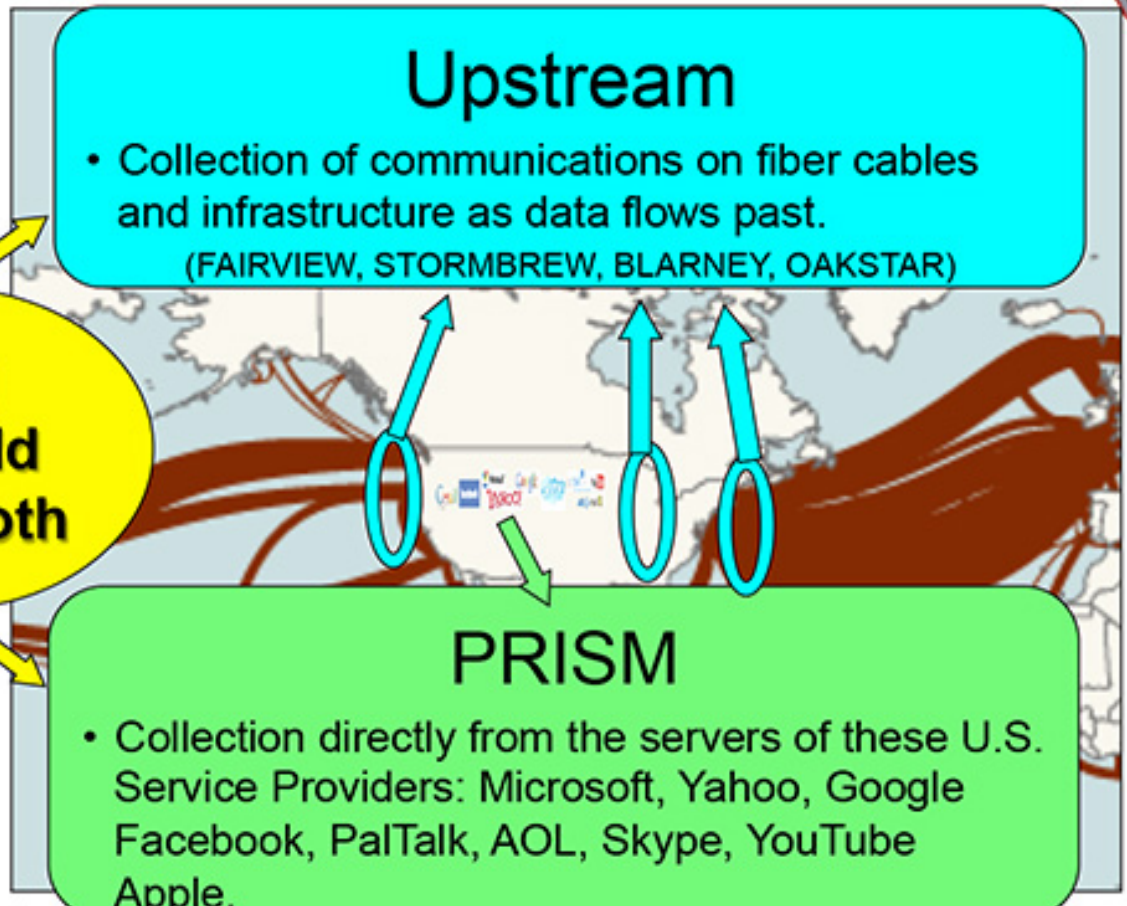
Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

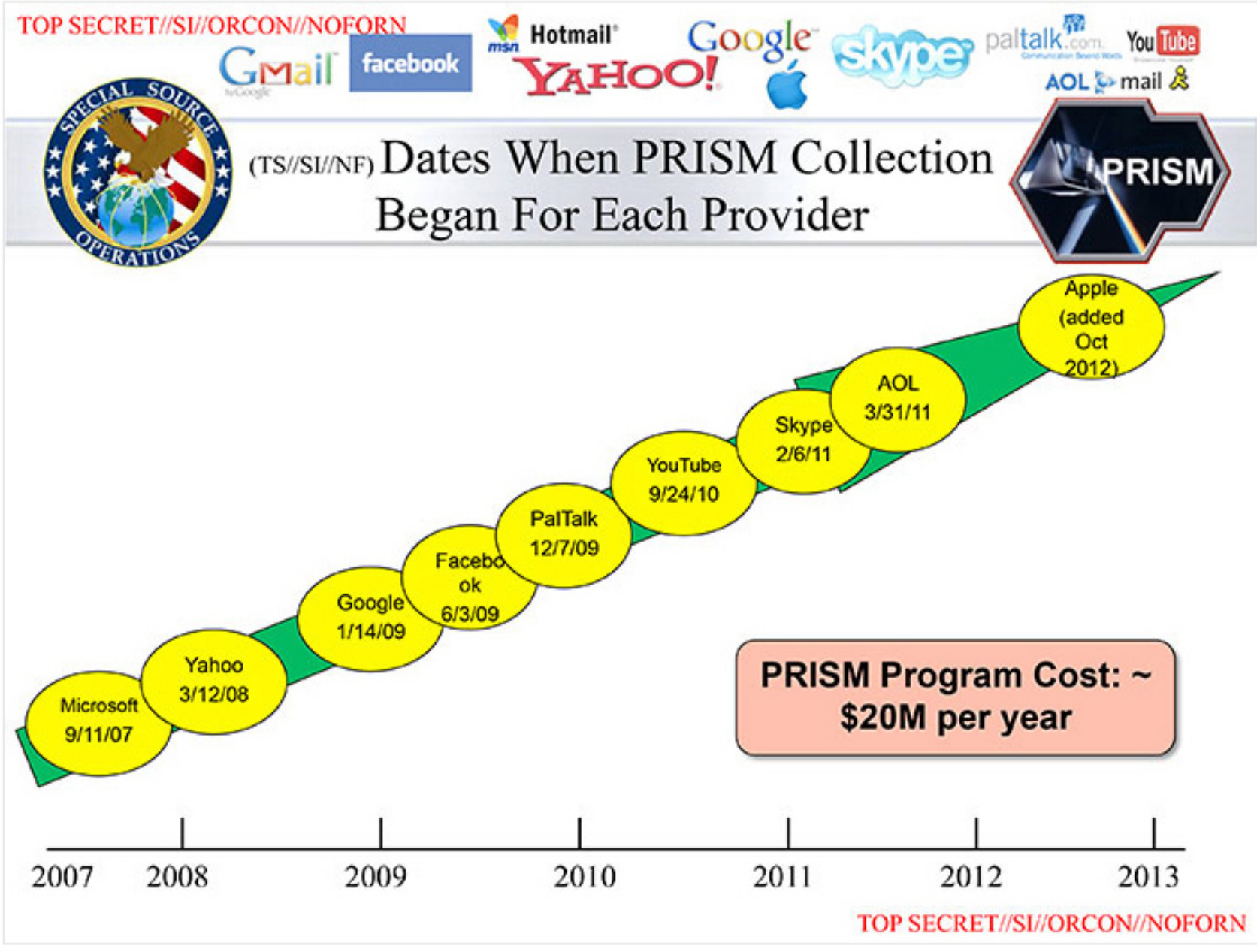
You Should Use Both



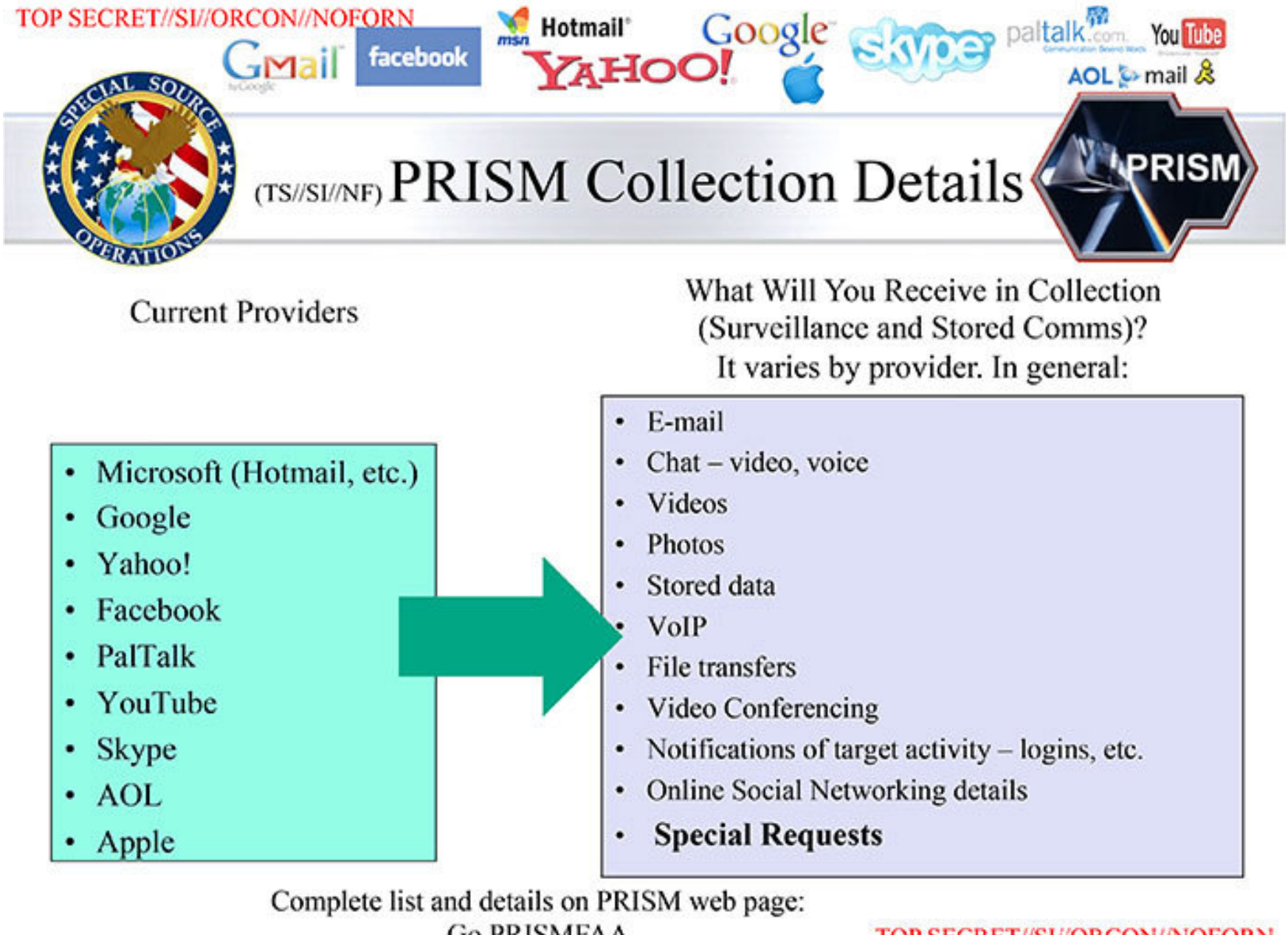
PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

PRISM: Prominente beteiligte Konzerne



PRISM: Inhalte



PRISM: Ablauf

- NSA oder GCHQ Analyst gibt Selektoren in System
- Review by Supervisor, Abgleich mit US-Prominenten
- FBI Data Intercept Technology Unit sendet Selektoren zu Diensten, empfängt gefilterte Daten
- Weitere NSA Filter-/Sortiersysteme
- Zugriff auf Anfrage: CIA, FBI, Geheimdienste befreundeter Länder

Upstream

- Abhörschnittstellen bei Netzbetreibern
- Technologie:
  - "Narus nSystem": Echtzeitmitschnitt und -filterung an 100 GBit Glasfaserleitungen mithilfe von Supercomputern
  - "Glimmerglass" Schnittstellen: Social Media Analyse in Echtzeit
  - Verteilte Datenbanken, Verarbeitung auf Tausenden Clusterknoten

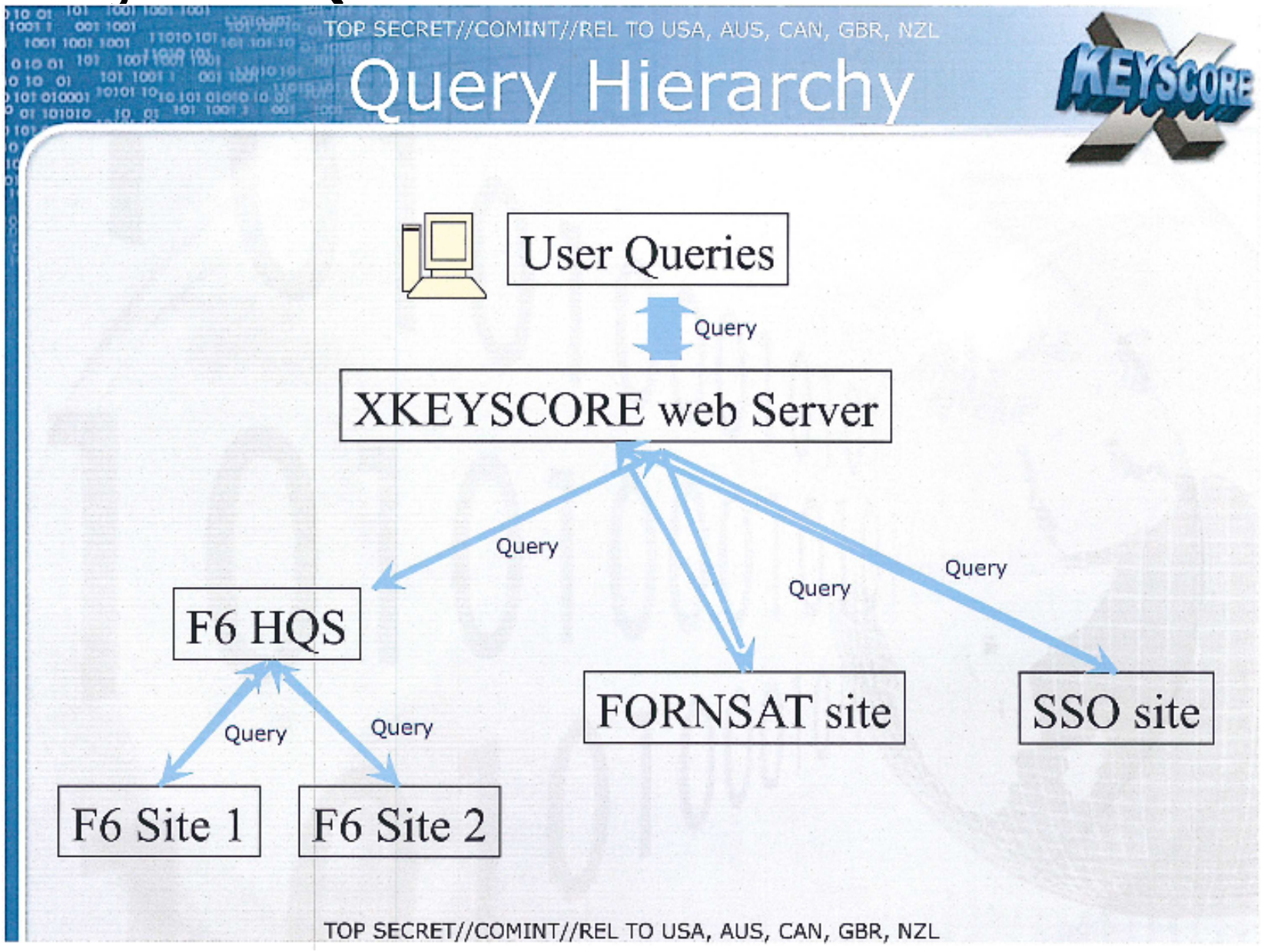
Tempora

- Snowden: "Größtes Programm verdachtsunabhängiger Überwachung"
- GCHQ zapft über 200 transatlantische Glasfaserkabel an
- 30 Tage Buffer von Rohdaten
- Zugriff: Regierung, britische und US-Geheimdienste

XKeyscore

- Vor Ort Abspeicherung, Indizierung, Analyse, und Durchsuchung rohen globalen Traffics
  - Komplettkopie von Metadaten (bis zu 1 Monat) und Inhalten (3-5 Tage) an min. 150 collection sites auf min. 700 Servern weltweit
  - Frontend für selektiven Zugriff über Index in Echtzeit
  - Beliebige Suchkriterien
  - Ohne Review
- Einsatz auch von BND in DE ($\sim$ 180 Mio Datensätze/Monat)

XKeyscore Quellen



Quellen und weiterführende Links:

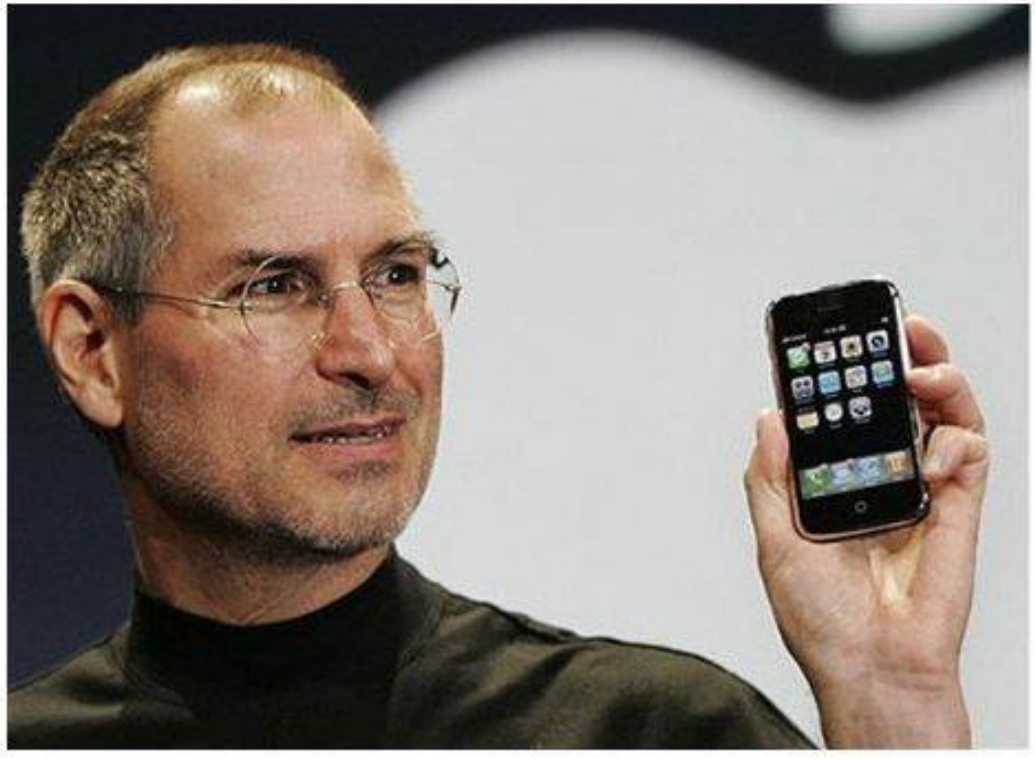
- The Guardian: http://www.theguardian.com/us-news/nsa
- Heise online Timeline – NSA-Skandal: Das Jahr 2013
  http://www.heise.de/extras/timeline-2013/
- Heise online Timeline – NSA-Skandal: Das Jahr 2014
  http://www.heise.de/extras/timeline/

(S//REL) iPhone Location Services

(U) Who knew in 1984...

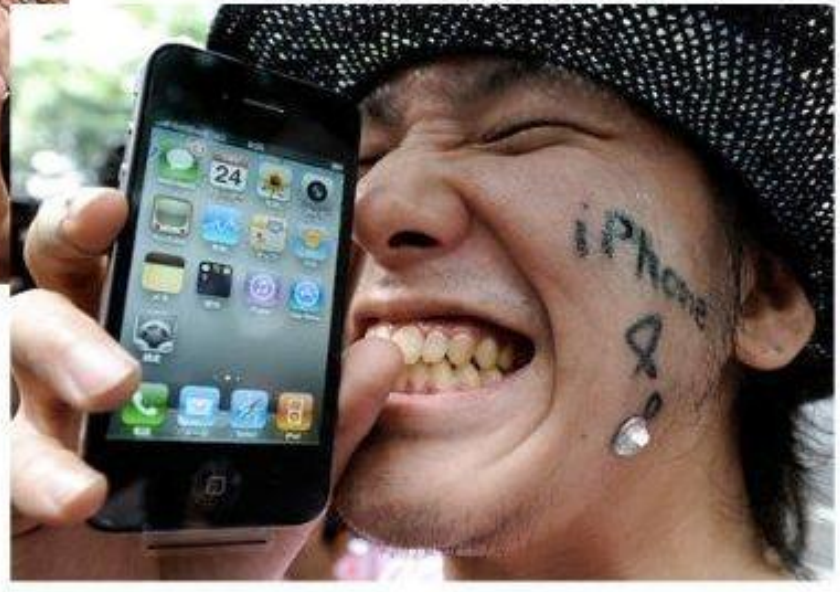
(S//REL) iPhone Location Services

(U) …that this would be big brother…



(S//REL) iPhone Location Services

(U) ...and the zombies would be paying customers?



Fragen?