Die Sicherheitsdebatte seit NSA, GCHQ & Co

Marit Hansen

Stv. Landesbeauftragte für Datenschutz
Schleswig-Holstein

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Überblick

- „... seit NSA, GCHQ & Co“
- Der Summer of Snowden
- Die Sicherheitsdebatte
- Fazit

… seit NSA, GCHQ & Co

- „seit“
  - NSA seit 1952 (Vorläufer im 2. Weltkrieg)
  - GCHQ seit 1919 (als „Gov. Code and Cypher School“)
  - „& Co“ seit mind. 100 Jahren
- Fokus auf SIGINT
- Hier: seit 6/5 (5. Juni 2013)

Der Summer of Snowden – Datensammlung

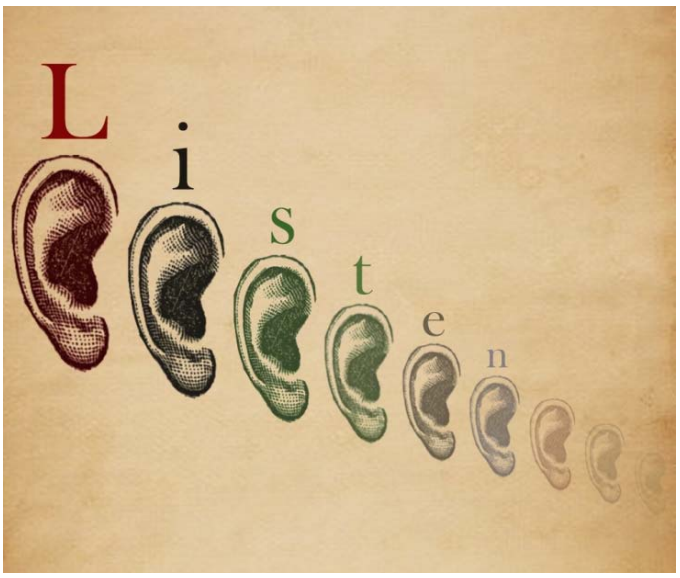
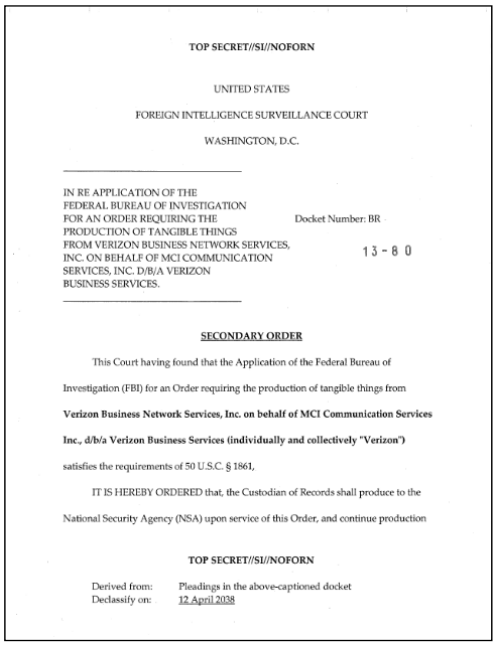


 Bild: Ky Olsen

Die ersten Snowden-Enthüllungen: Verizon – 05.06.2013

- Geheimer Gerichtsbeschluss an Verizon zur massenhaften Herausgabe von Verbindungsdaten der Kunden in den USA
- Später: nicht nur Verizon



TOP SECRET//SI//NOFORN

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION 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.

Docket Number: BR 13-80

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,

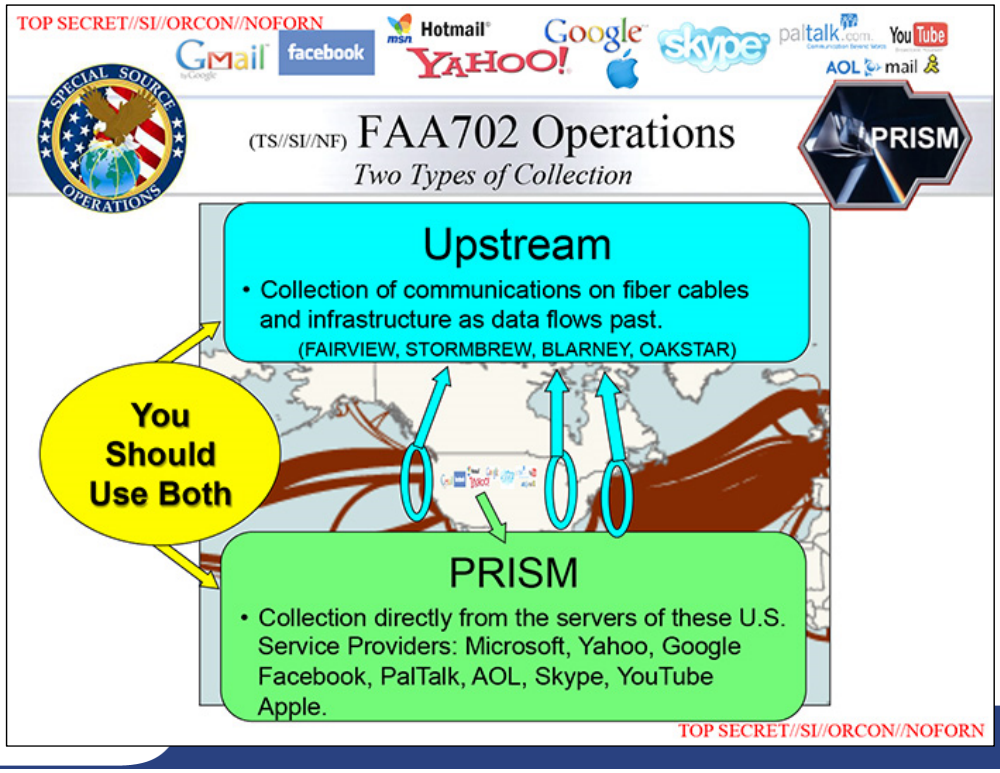
IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

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

ULD www.datenschutzzentrum.de

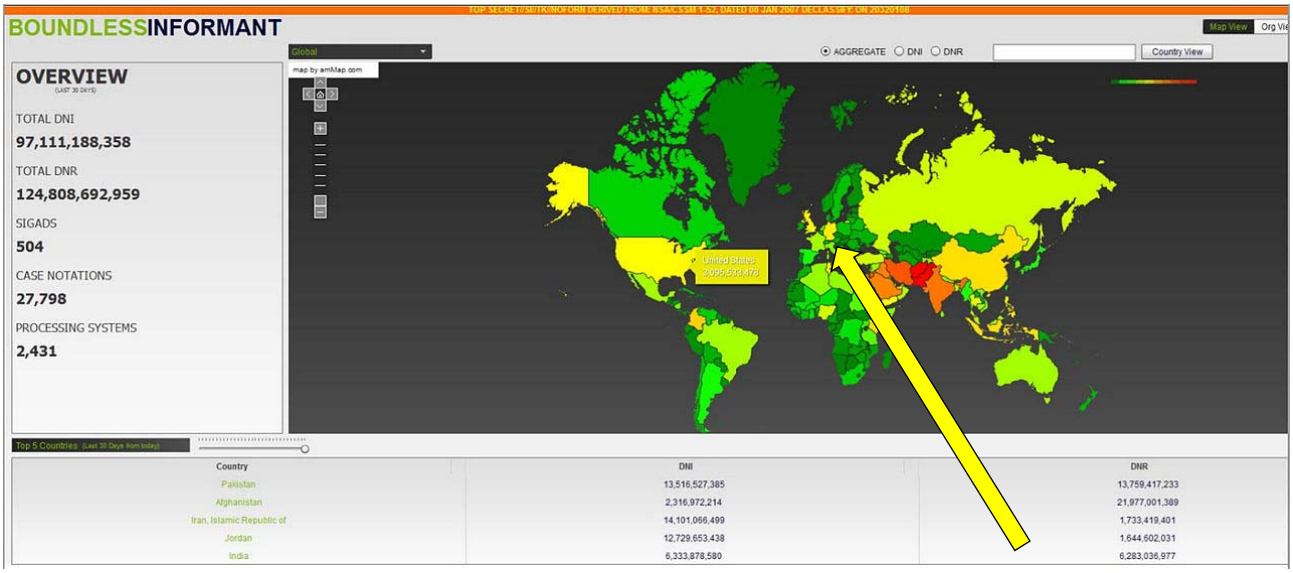
Die ersten Snowden-Enthüllungen: PRISM – 06.06.2013



Die ersten Snowden-Enthüllungen: Boundless Informant – 08.06.2013

Data-Mining-Analyse-Tool der NSA

97 Mrd. Internet-Datensätze, 124 Mrd. Telefonie-Datensätze in 30 Tagen



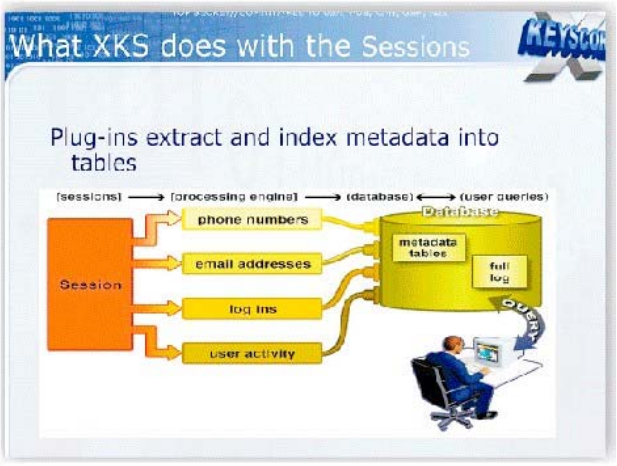
März 2013

Die ersten Snowden-Enthüllungen: Tempora – 21.06.2013

Programm des GCHQ zur Überwachung des weltweiten Telekommunikations- und Internet-Datenverkehrs, der über Großbritannien fließt (auch Inhaltsdaten)

Die ersten Snowden-Enthüllungen: XKeyscore – 08.07.2013

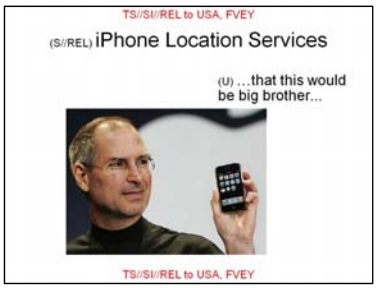
- Auswertungssoftware über Metadaten und (kurzzeitig/teilweise) Inhaltsdaten

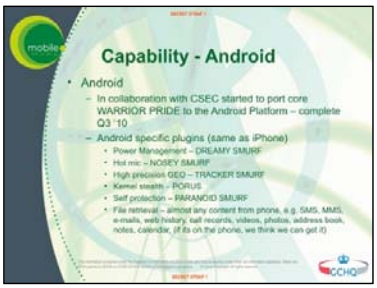


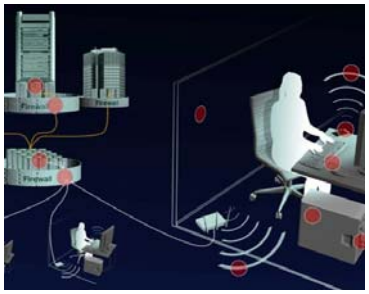
- Angeblicher Source-Code kursiert im Internet, z.B.:

```
fingerprint('anonymizer/tor/torpoject_visit')=http_host
('www.torproject.org') and not(xff_cc('US' OR 'GB' OR
'CA' OR 'AU' OR 'NZ'));
```


Geheimdienstliches Hacking auf Endgeräte und Netzkomponenten







http://www.spiegel.de/netzwelt/netzpolitik/interaktive-grafik-hier-sitzen-die-spaeh-werkzeuge-der-nsa-a-941030.html

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Der Summer of Snowden – Manipulation der Infrastruktur

Foto: anyjazz65

Foto: Nic McPhee

Geschwächter Sicherheitsstandard

09/2013: NIST (National Institute of Standards and Technology) warnt vor Dual_EC_DRBG (Pseudozufallszahlengenerator)

NIST works to publish the strongest cryptographic standards possible, and uses a transparent, public process to rigorously vet its standards and guidelines. If vulnerabilities are found, NIST works with the cryptographic community to address them as quickly as possible.

In light of the concerns expressed regarding Dual_EC_DRBG, ITL is taking the following actions:

Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation: NIST strongly recommends that, pending the resolution of the security concerns and the re-issuance of SP 800-90A, the Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A, no longer be used.

Re-issuing SP 800-90A as a draft for public comment: Effective immediately, NIST Special Publication 800-90A is being re-issued as a draft for public comment for a period ending November 6, 2013. Any concerns or recommendations for improvement regarding the *Recommendation for Random Number Generation Using Deterministic Random Bit* Generators are solicited (http://csrc.nist.gov/publications/PubsDrafts.html). NIST will review, analyze, and adjudicate all comments received during this 60 day period.

NSA-Abt. TAO
(Tailored Access Operations)

SIGINT Enabling Project:

- „insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets“
- „influence policies, standards and specification for commercial public key technologies“

GCHQ-Abt. JTRIG
(Joint Threat Research Intelligence Group)

Manipulation:

- „using online techniques to make something happen in the real or cyber world“

ULD www.datenschutzzentrum.de

Die Sicherheitsdebatte

Die Sicherheitsdebatte seit NSA, GCHQ & Co

Sicherheitsdebatte I

- Zunächst: reflexartiges Abstreiten und Abwiegeln
- Diskussion über #Neuland

- 16.07.2013: Innenminister Friedrich: *„Sicherheit ist ein Supergrundrecht, und ich glaube, dass wir auch dieses Grundrecht in der Abwägung aller Dinge ganz nach vorne stellen müssen.“*

<Exkurs Grundrechte>

Was ist ein Supergrundrecht?

Vielleicht:

Art. 0 [Sicherheit]

(1) Sicherheit ist das wichtigste Grundrecht (Supergrundrecht).

(2) Grundrechte sind gegenüber einem Supergrundrecht nachrangig.

???

Was ist ein Grundrecht?

- Primär: Abwehrrecht des Bürgers gegen staatliche Eingriffe in seinen Freiheitsbereich
- Leistungsrecht: Der Bürger hat einen Anspruch gegenüber dem Staat
- Mitwirkungsrecht

Art. 1 Abs. 1 Satz 1 GG

Allgemeines Persönlichkeitsrecht

Freie Entfaltung der Persönlichkeit

- Abgeleitet aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

Schutz der Menschenwürde

- Daraus abgeleitet:
  - Recht auf informationelle Selbstbestimmung
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Wenn schon ein „Supergrundrecht“, dann Schutz der Menschenwürde

- Art. 1 Abs. 1 GG
- Art. 1 EU-Grundrechte-Charta

- „Sicherheit“?
  - Nicht in GG
  - Aber in Art. 6 EU-Grundrechte-Charta: „Jeder Mensch hat das Recht auf Freiheit und Sicherheit.“

```
</Exkurs Grundrechte>
```

Sicherheitsdebatte II

In Großbritannien:

- Vorgehen gegen Journalisten
  - Symbolisches Zerstören von Speichern
  - Schikane gegen Lebenspartner
- Kein Aufschrei der Bevölkerung

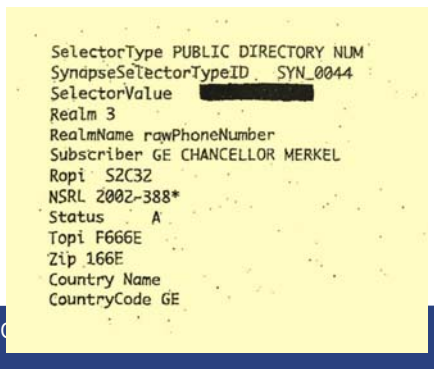
The remains of a computer that held files leaked by Edward Snowden to the Guardian and destroyed at the behest of the UK government. Photograph: Roger Tooth

Quelle: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

Sicherheitsdebatte III

- 12.08.2013: Kanzleramtsminister Pofalla erklärt auf Basis eines Schreibens von NSA und GCHQ:
  „Es gibt in Deutschland keine millionenfache Grundrechtsverletzung, wie immer behauptet wird.“
- 23.10.2013: Kanzlerin Merkel beschwert sich bei Obama, dass ihr Handy abgehört wird

 Foto: Armin Linnartz



SelectorType PUBLIC DIRECTORY NUM
SynapseSelectorTypeID SYN_0044
SelectorValue [redacted]
Realm 3
RealmName rawPhoneNumber
Subscriber GE CHANCELLOR MERKEL
Ropi S2C32
NSRL 2002-388*
Status A
Topi F666E
Zip 166E
Country Name
CountryCode GE

Abhören von Spitzenpolitikern und Staatschefs

- Gängige geheimdienstliche Praxis (nicht nur NSA)
- Wenn nicht gezielt, dann „Beifang“ möglich
  (z.B. Hillary Clinton und John Kerry durch BND)

Daher: Regierungsmitglieder erhalten besonders sichere Endgeräte und können über abgesicherte Infrastrukturen kommunizieren.

Und die Bevölkerung?

- Grundrechtliches Fazit:
  Der Staat muss seine Bürger vor Zugriffen aus dem Ausland schützen und dafür das Mögliche tun.

- Datenschutzgarantien nötig:
  - Auf Infrastrukturebene[1]
  - Auf Anwendungsebene[2]
  - In der (eigenen+fremden) Geheimdienstkontrolle

[1,2] Siehe auch Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ vom 17.03.2014

Fazit

- EU LIBE Committee (21.02.14): “oversight of intelligence services’ activities should be based on both democratic legitimacy [...] and adequate technical capability and expertise” – majority of EU and US bodies lack both

- Zwischenergebnis:
  - Zu spät, zu wenig, zu unkonkret
  - Glaubwürdigkeits- und Kommunikationsproblem
  - Massives Risiko für die Informationsgesellschaft, wenn die Basis (Technik, Vertrauen) geschwächt wird