

8. Europäischer Datenschutztag  
28. Januar 2014

01100101 01100001  
01100110 01110100  
011B1G D0T00000  
101F0R 01001000  
011B0ND 2. 0111101  
01101110 01110011  
01100110 01110100  
10101010 01010101  
01111010

# Big Data für Bond 2.0

## Sammlung, Auswertung – und der Datenschutz?

- Für eine menschenrechtliche  
Einhebung der Nachrichtendienste  
in Zeiten von Big Data

Marit Hansen  
Stv. Landesbeauftragte für Datenschutz  
Schleswig-Holstein



Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein

ULD  [www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

## Überblick

- Big Data für Bond 2.0
- Summer of Snowden – Datensammlung
- Autumn of Snowden – Manipulation der Infrastruktur
- Winter of Snowden – noch mehr Power
- Und der Datenschutz?

Sammlung, Auswertung – und der Datenschutz?

ULD  [www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

*Bond 1.0*

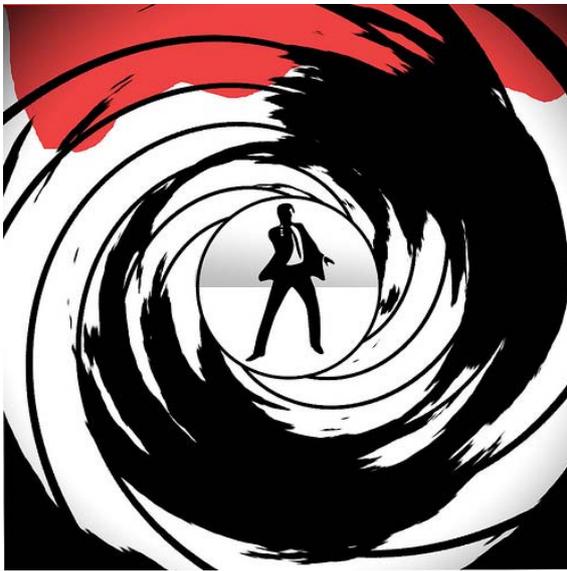


 Foto: Themeplus

Sammlung, Auswertung – und der Datenschutz?

ULD  [www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

*Bond 2.0*



 Quelle: Guillom

 Foto: Themeplus

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## Summer of Snowden – Datensammlung



 Bild: Ky Olsen

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## Leitungen und Server

TOP SECRET//SI//ORCON//NOFORN

 (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)

**PRISM**

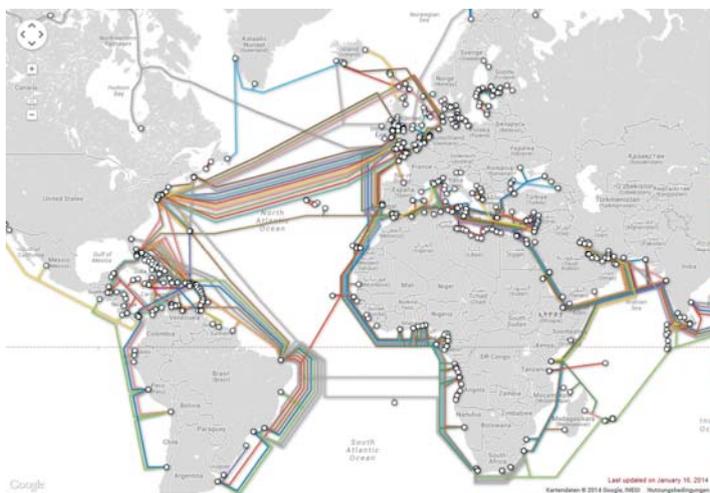
- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

**You Should Use Both**

TOP SECRET//SI//ORCON//NOFORN

ULD  www.datenschutzzentrum.de

## Unterwasserkabel



**TeleGeography Submarine Cable Map**  
The Submarine Cable Map is a free resource from TeleGeography. Data contained in this map is drawn from the Global Bandwidth Research Service and is updated on a regular basis.  
To learn more about TeleGeography or this map please click here.

 [Facebook](#) [globe](#)

Q Search

**Submarine Cables**

- ACS Alaska Oregon Network (AKORIN)
- Aden-Oman
- Alba 1
- Africa Coast to Europe (ACE)
- ALCANTARA
- Alaska United East
- Alaska United Southeast
- Alaska United West
- ALBA 1
- Alcatel
- Algeria-Spain
- América de Océano
- ALPN-2
- America Most Submarine Cable System-1 (MOS-1)
- American Samoa-Hawaii (ASOH)
- Americas 4 North
- Americas 6
- Amigo-Wireless
- Angola Domestic Network System (ADONES)
- Aruba 1
- ARCA-2
- Aphrodite 2

Map updated on January 16, 2014  
Kartenbild © 2014 Google, NED - Nutzungsbedingungen  
All content © 2013 Probelica, Inc.

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## Web-Nutzung



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

Why are we interested in HTTP?

facebook YAHOO! twitter

myspace.com  
a place for friends

Because nearly everything a typical user does on the Internet uses HTTP

CNN.com

Google Earth

Gmail

@mail.ru

WIKIPEDIA  
The Free Encyclopedia

ULD  www.datenschutzzentrum.de

**Smartphone-Nutzung**

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...



TS//SI//REL to USA, FVEY

ULD  www.datenschutzzentrum.de

**Smartphone-Nutzung**

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) ...that this would be big brother...



TS//SI//REL to USA, FVEY

ULD  www.datenschutzzentrum.de

## Smartphone-Nutzung

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services



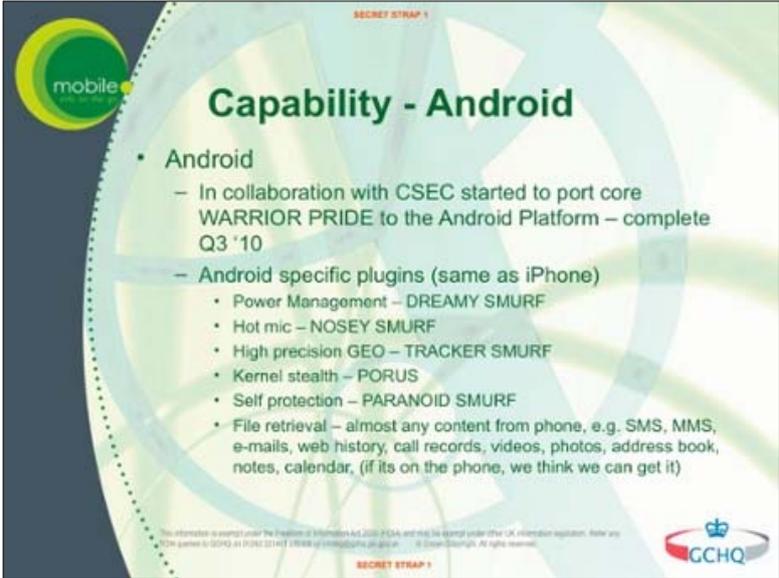
(U) ...and the zombies would be paying customers?

TS//SI//REL to USA, FVEY

ULD  www.datenschutzzentrum.de

## Smartphone-Nutzung

SECRET STRAP 1



### Capability - Android

- Android
  - In collaboration with CSEC started to port core WARRIOR PRIDE to the Android Platform – complete Q3 '10
  - Android specific plugins (same as iPhone)
    - Power Management – DREAMY SMURF
    - Hot mic – NOSEY SMURF
    - High precision GEO – TRACKER SMURF
    - Kernel stealth – PORUS
    - Self protection – PARANOID SMURF
    - File retrieval – almost any content from phone, e.g. SMS, MMS, e-mails, web history, call records, videos, photos, address book, notes, calendar, (if its on the phone, we think we can get it)

This information is exempt under the Freedom of Information Act, 2001 (FOIA) and this is exempt under other UK information legislation. Refer any FOIA queries to GCHQ at FOIR 22147 19888 or info@gchq.gsi.gov.uk © Crown Copyright. All rights reserved.

SECRET STRAP 1



ULD  www.datenschutzzentrum.de

## Smartphone-Nutzung

**theguardian**  
News | Sport | Comment | Culture | Business | Money | Life & style  
News > World news > NSA

### NSA and GCHQ target 'leaky' phone apps like Angry Birds to scoop user data

- US and UK spy agencies piggyback on commercial data
- Details can include age, location and sexual orientation
- Documents also reveal targeted tools against individual phones

James Ball  
The Guardian, Monday 27 January 2014 17.30 GMT  
[Jump to comments \(869\)](#)



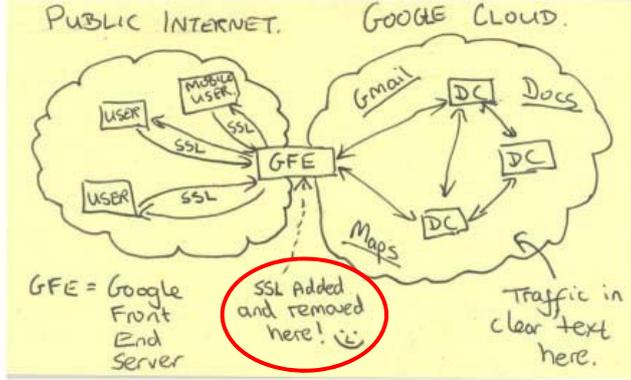
...ertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## Unverschlüsselte Server-Kommunikation

TOP SECRET//SI//NOFORN

 **Current Efforts - Google**



PUBLIC INTERNET.      GOOGLE CLOUD.

GFE = Google Front End Server

SSL Added and removed here! :)

Traffic in clear text here.

TOP SECRET//SI//NOFORN

ULD  www.datenschutzzentrum.de

## *Autumn of Snowden – Manipulation der Infrastruktur*



 Foto: anyjazz65



 Foto: Nic McPhee

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## *Geschwächter Sicherheitsstandard*

09/2014: 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.

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## **NSA-Abteilung 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“
- Bullrun (NSA) & Edgehill (GCHQ): Projekte zur Kryptoanalyse
- OTN (Owning the Net) Project



Sammlung, Auswertung – und der Datenschutz?

ULD  www.

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

## Forward-based Defense NSA TURBULENCE Architecture



**SENSORS**

- TURMOIL**  
Passive SIGINT
- TUTELAGE**  
Active Defense
- TURBINE**  
Active SIGINT

**TURBULENCE INTEGRATION**

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

## **„Vorwärtsverteidigung“**

Sammlung, Auswertung – und der Datenschutz?

ULD  WWW.

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

## Forward-based Defense NSA TURBULENCE Architecture

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

### TURBINE: Active Mission Management

(TS//SI//REL) TURBINE provides centralized automated command/control of a large network of active implants

**Accesses**

- TURMOIL
- TUTELAGE
- Implants (TAO)



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

TURBULENCE INTEGRATION

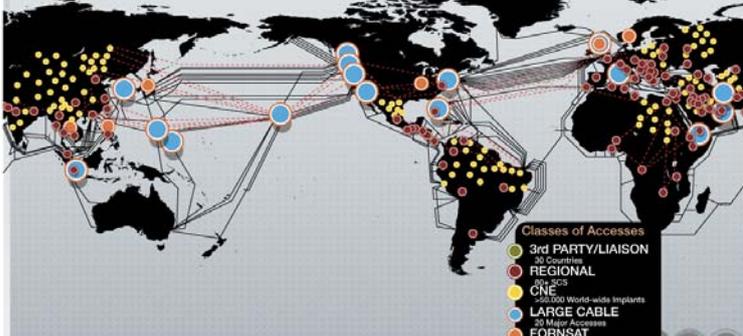
ULD  www.datenschutzzentrum.de

**2008: mehr als 50.000 „Implantate“**  
**2014: ca. 100.000**

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

### Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable	Regional	FORNSAT
Covert, Classification or Cooperative Large Accesses	Caracas Havana Kinshasa Sofia	STELLAR INORA
20 Access Programs Worldwide	Beijing Bogota London New Delhi	SCANDER IRONSAND
	Alaska Mexico City Budapest Paris	SNACK JACKKNIFE
	Rome Brasilia Prague Vienna	MOONPEN CARBOY
	Quito Managua Lagos Vienna	NY TRADEFLIN
	San Jose	LADYLOVE E



**Classes of Accesses**

- 3rd PARTY/LIAISON
- 26 Countries REGIONAL
- 30+ 2CS CNE
- 25-300 World-wide Implants
- 20 Major Accesses LARGE CABLE
- FORNSAT
- 12+40 Regional

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

ULD  www.datenschutzzentrum.de

## Winter of Snowden – noch mehr Power



 Foto: Swilsonmc

- Intelligence Community Comprehensive National Cybersecurity Initiative Data Center in Utah
- Aufgaben: Sammlung, Auswertung, Kryptoanalyse
- Entwicklung von Quantencomputern?

Sammlung, Auswertung – und der Datenschutz?

 nschutzzentrum.de

## Weitere Informationsquellen



**Spion im Wohnzimmer**  
Privatsphäre und Stillschauen bei rostigen Fallgruben TV?



 Foto: Arcom Control Systems

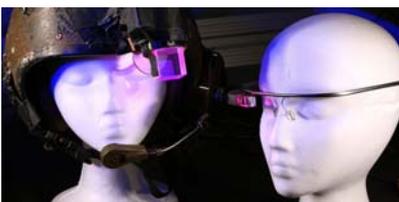


 Foto: Glogger



 Foto: Jan Prucha



**Вести в субботу**  
Foto: Rossiya 24

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## *Auswertung durch die NSA*

- **Sammlung**
  - 1,7 Mrd. Datensätze / Tag (Stand: 2010)
  - Dishfire: 200 Mio SMS / Tag
  - In Deutschland: ca. 20 Mio Telefonverbindungen + 10 Mio Internetdatensätze / Tag
- **Auswertung**
  - Ca. 20 Mio Anfragen / Monat (600.000 / Tag)
  - Bekannte von Bekannten (von Bekannten) („two degrees of separation“, „a 2<sup>nd</sup> or 3<sup>rd</sup> hop query“)
  - Auch: LOVEINT, „economic well-being“

**Erfolg???**

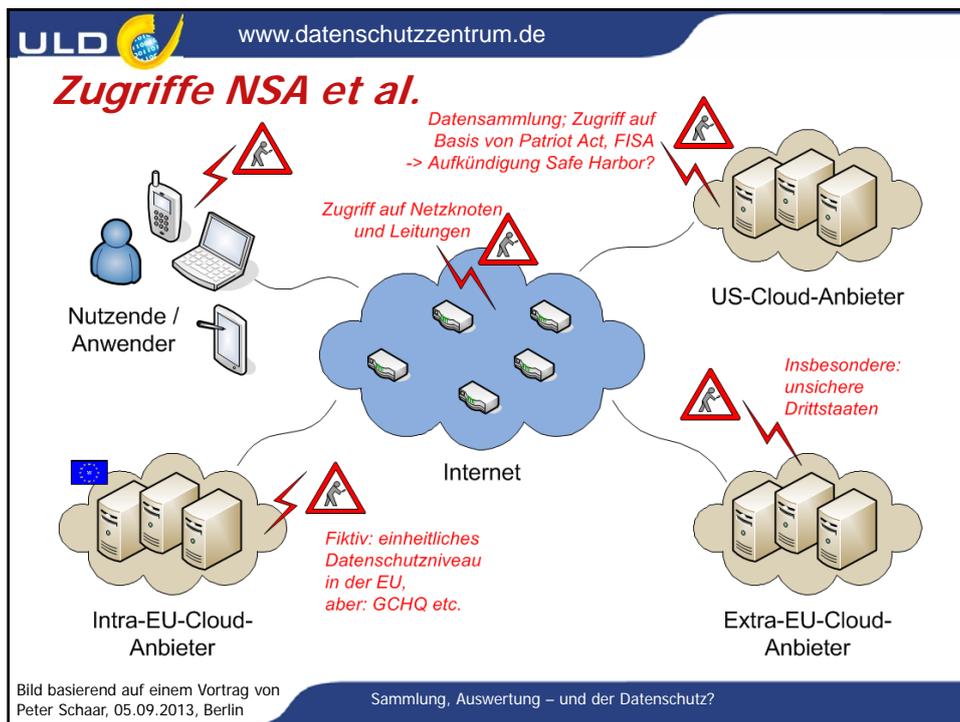
Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

## *Datenschutz?*

- Privacy and Civil Liberties Oversight Board (23.01.14):  
Überwachung von Telefonverbindungen durch die NSA im eigenen Land **unrechtmäßig** 
- Europäische Gerichtshof für Menschenrechte (EGMR) bearbeitet **Klage gegen GCHQ** – Stellungnahme der britischen Regierung bis 02.05.14 angefordert
- EU LIBE Committee (Draft, 08.01.14): „oversight of intelligence services' activities should be based on both **democratic legitimacy [...] and an adequate technical capability and expertise**“ – dies fehle mehrheitlich 

Sammlung, Auswertung – und der Datenschutz?



ULD  www.datenschutzzentrum.de

### Check: Datenschutz-Schutzziele

- Nichtverkettbarkeit? 
- Transparenz?  →  
- Intervenierbarkeit? 

**Verhältnismäßigkeit?** 

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

***Vielen Dank für die Aufmerksamkeit!***

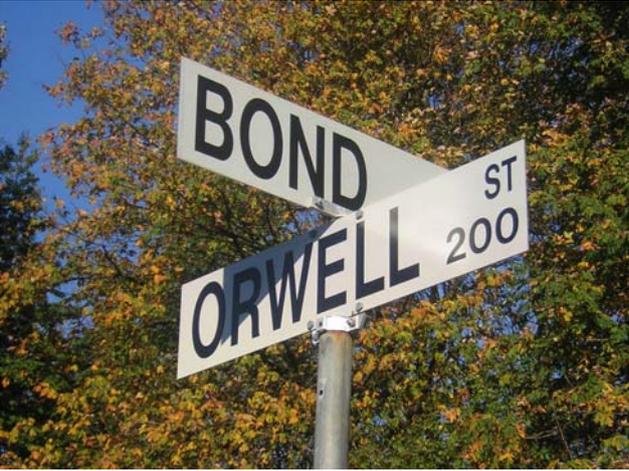


 Foto: id

Sammlung, Auswertung – und der Datenschutz?

ULD  www.datenschutzzentrum.de

***Annex: Quellen***

- Die Dokumente: <http://cryptome.org/>
- Berichterstattung:
  - <http://www.theguardian.com/world/nsa>
  - [http://topics.nytimes.com/top/reference/timestopics/organizations/n/national security agency/](http://topics.nytimes.com/top/reference/timestopics/organizations/n/national_security_agency/)
  - [http://www.spiegel.de/thema/nsa ueberwachung/](http://www.spiegel.de/thema/nsa_ueberwachung/)
  - <http://www.spiegel.de/netzwelt/netzpolitik/interaktive-grafik-hier-sitzen-die-spaeh-werkzeuge-der-nsa-a-941030.html>
  - <http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal>

Sammlung, Auswertung – und der Datenschutz?

**ULD**  [www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

## *Annex: Beispiele für Selbstschutz-Tools*

**E-Mails verschlüsseln**

 <https://www.gnupg.org/>  <http://www.openpgp.org/>

**Datensparsam suchen**

 <https://ixquick.de/>  <https://www.startpage.com/>

**Festplattenbereiche verschlüsseln**

 <https://www.truecrypt.org/>

**Anonym surfen & Browser datensparsam konfigurieren (auch mobil)**

 <https://www.anonym-surfen.de/>  
<https://www.anonym-surfen.de/jondofox.html>

  <https://www.torproject.org/>  
<https://www.torproject.org/projects/torbrowser.html>

**Mobile Messaging verschlüsseln**

 <https://threema.ch/>

**Neue Entwicklungen:  
Attributbasierte Berechtigungsnachweise**

 <https://abc4trust.eu/>

 <https://guardianproject.info/apps/orbot/>

Sammlung, Auswertung – und der Datenschutz?