
8. Europäischer Datenschutztag
28. Januar 2014
01100101 01100001
01100110 01110100
011B1G D0T0
101F0R 01001000
011B0ND 2.0
01101110 01110011
01100110 01110100
10101010 01010101
01111010
- Für eine menschenrechtliche Einhegung der Nachrichtendienste in Zeiten von Big Data
Big Data für Bond 2.0
Sammlung, Auswertung – und der Datenschutz?
Marit Hansen
Stv. Landesbeauftragte für Datenschutz Schleswig-Holstein
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein


ULD
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

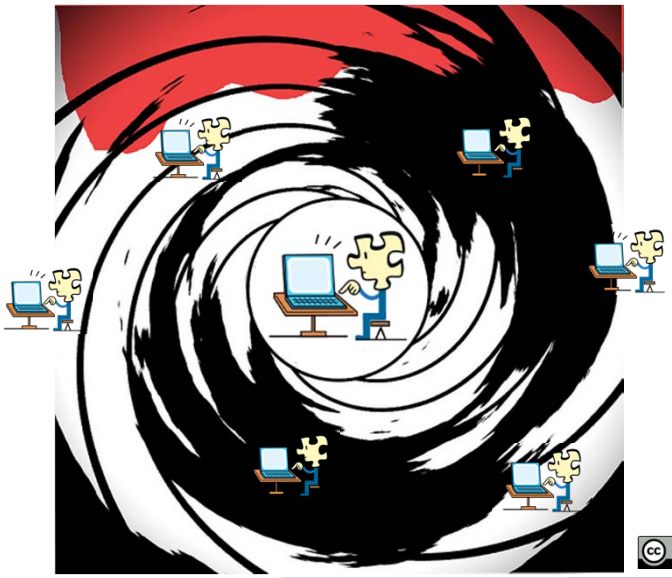
Bond 1.0

Foto: Themeplus

Sammlung, Auswertung – und der Datenschutz?

ULD www.datenschutzzentrum.de

Bond 2.0



Quelle: Guillom

Foto: Themeplus

Sammlung, Auswertung – und der Datenschutz?

ULD www.datenschutzzentrum.de

Summer of Snowden – Datensammlung

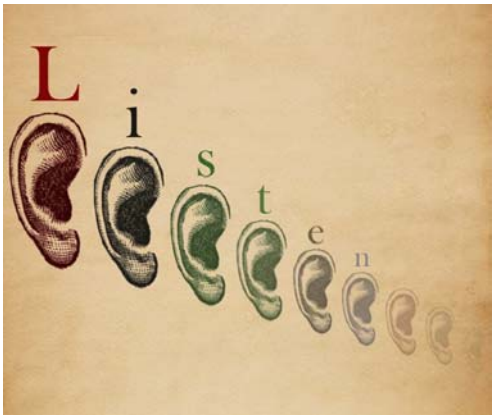
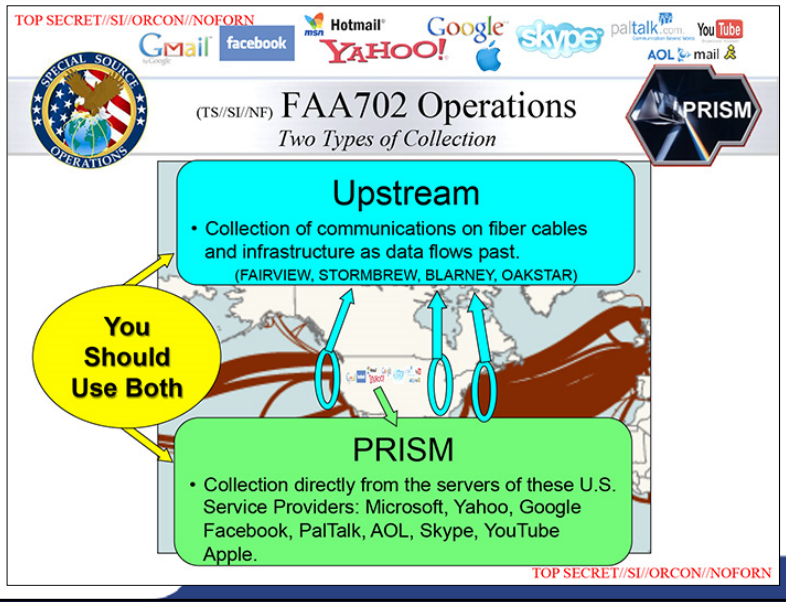


Bild: Ky Olsen

Sammlung, Auswertung – und der Datenschutz?

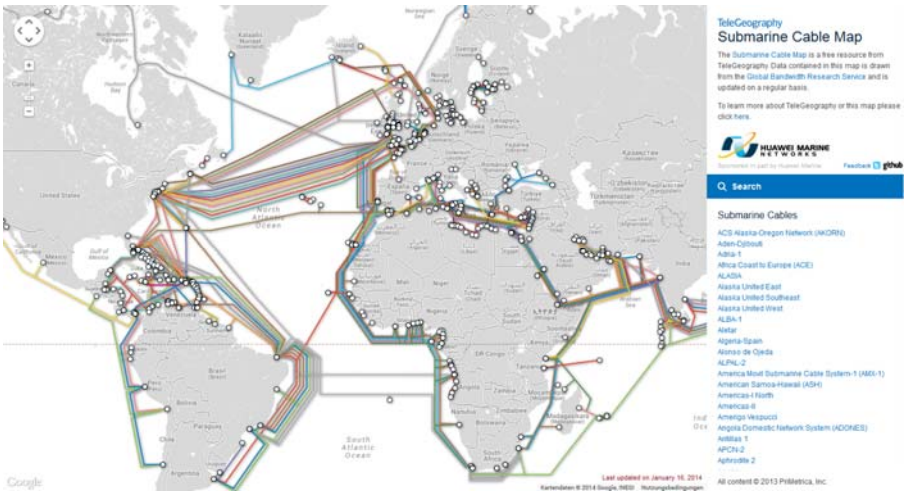
ULD www.datenschutzzentrum.de

Leitungen und Server



ULD www.datenschutzzentrum.de

Unterwasserkabel



Sammlung, Auswertung – und der Datenschutz?

ULD www.datenschutzzentrum.de

Web-Nutzung

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

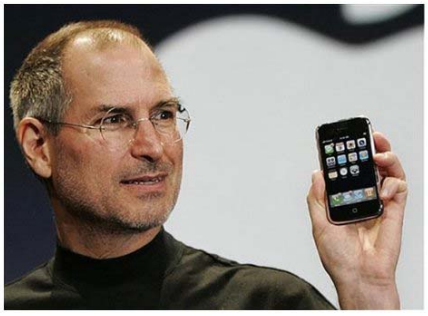
ULD www.datenschutzzentrum.de

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

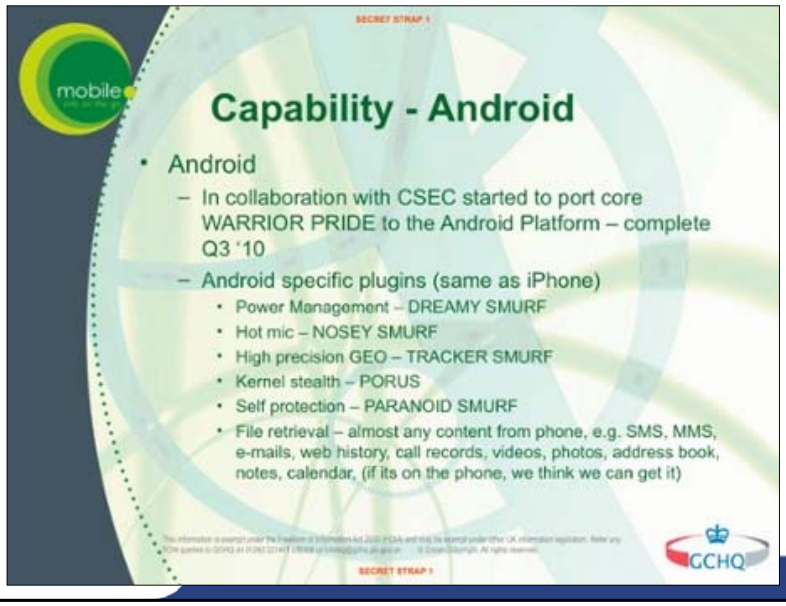
(S//REL) iPhone Location Services

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

TS//SI//REL to USA, FVEY

ULD www.datenschutzzentrum.de

Smartphone-Nutzung



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

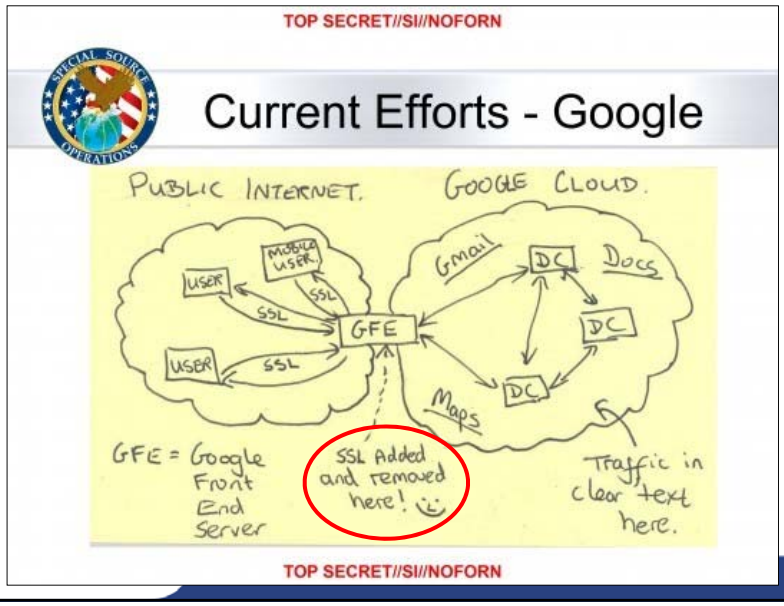
- US and UK spy agencies piggyback on commercial data
- Details can include age, location and sexual orientation
- Documents also reveal targeted tools against individual phones

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



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

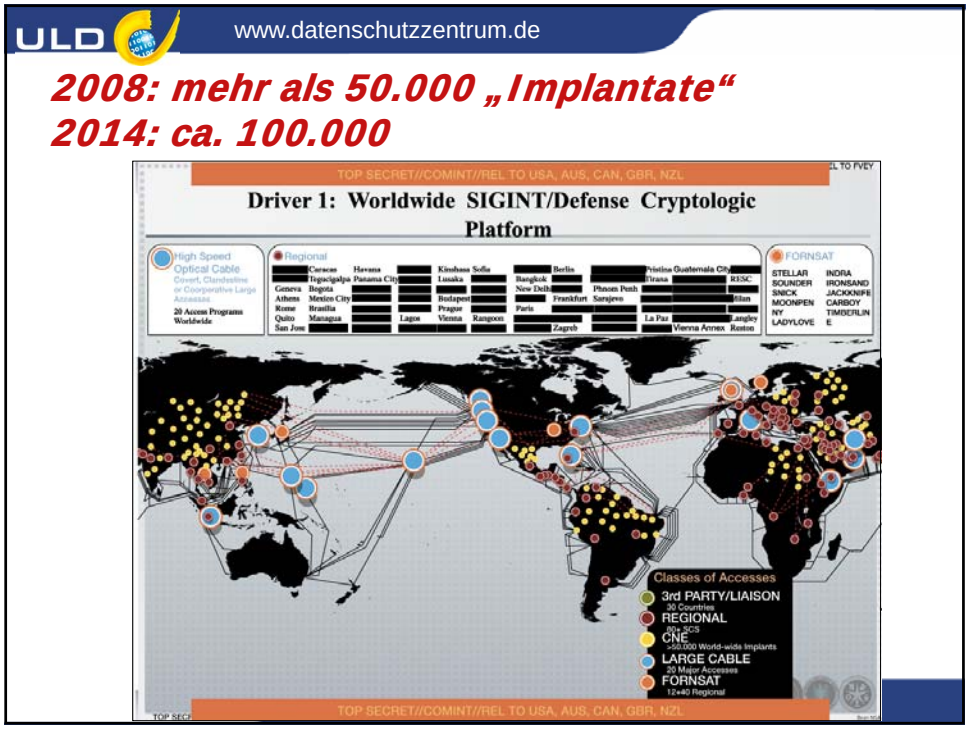
Sammlung, Auswertung – und der Datenschutz?

ULD www.

„Vorwärtsverteidigung“

Sammlung, Auswertung – und der Datenschutz?


ULD
www.
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Forward-based Defense
NSA TURBULENCE Architect
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
TURBINE: Active Mission Management
Accesses
TURMOIL
TUTELAGE
Implants (TAO)
(TS//SI//REL) TURBINE provides centralized automated command/control of a large network of active implants
Internet Cloud
DoD Network
MHS
Internet
Internet Cloud
TURBULENCE INTEGRATION
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL


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
STELLAR
SOUNDER
SNICK
MOONPEN
NY
LADYLOVE
INDRA
IRONSAND
JACKKNIFE
CARBOY
TIMBERLIN
E
Classes of Accesses
3rd PARTY/LIAISON
REGIONAL
CNE
LARGE CABLE
FORNSAT
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

Foto: Glogger

Foto: Arcom Control Systems

Foto: Jan Prucha

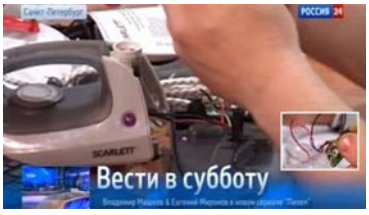


Foto: Rossiya 24

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

Erfolg???

- Auswertung
  - Ca. 20 Mio Anfragen / Monat (600.000 / Tag)
  - Bekannte von Bekannten (von Bekannten) („two degrees of separation“, „a 2nd or 3rd hop query“)
  - Auch: LOVEINT, „economic well-being“

Sammlung, Auswertung – und der Datenschutz?

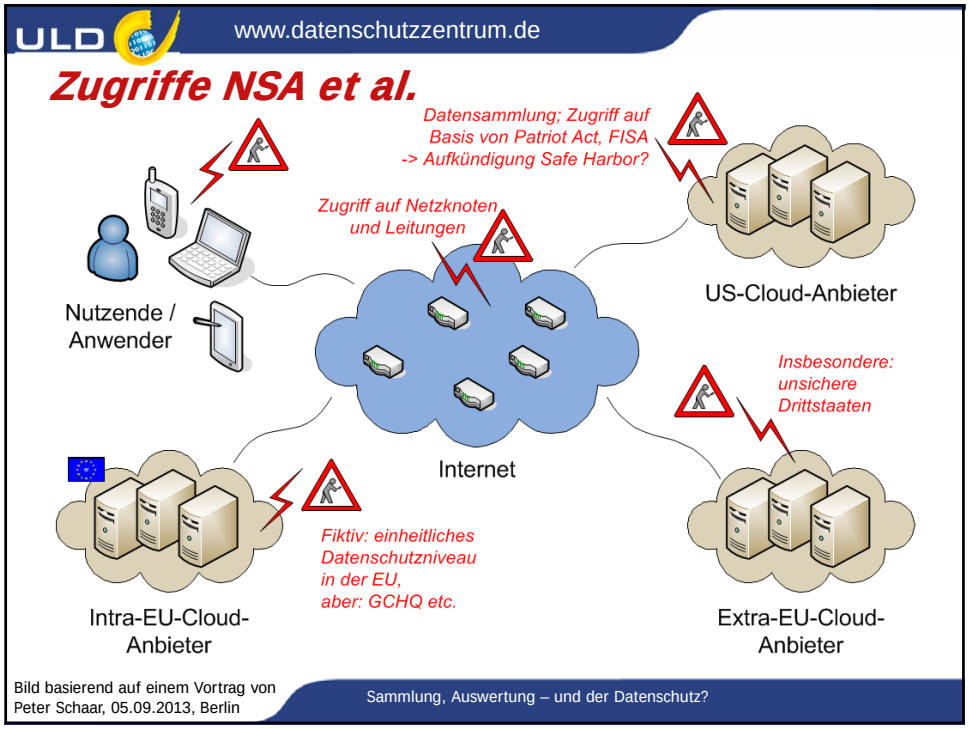
ULD www.datenschutzzentrum.de

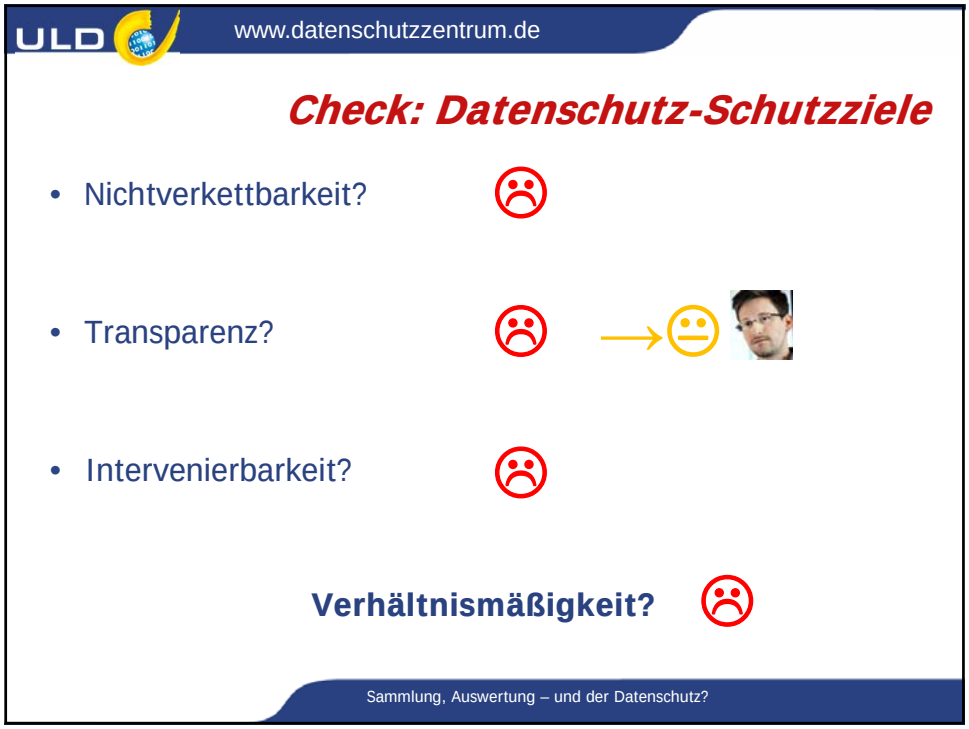
Datenschutz?

- 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
Zugriffe NSA et al.
Datensammlung; Zugriff auf Basis von Patriot Act, FISA -> Aufkündigung Safe Harbor?
Zugriff auf Netzknoten und Leitungen
US-Cloud-Anbieter
Nutzende / Anwender
Internet
Insbesondere: unsichere Drittstaaten
Fiktiv: einheitliches Datenschutzniveau in der EU, aber: GCHQ etc.
Intra-EU-Cloud-Anbieter
Extra-EU-Cloud-Anbieter
Bild basierend auf einem Vortrag von Peter Schaar, 05.09.2013, Berlin
Sammlung, Auswertung – und der Datenschutz?


ULD
www.datenschutzzentrum.de
Check: Datenschutz-Schutzziele
• Nichtverkettbarkeit?
• Transparenz?
• Intervenierbarkeit?
Verhältnismäßigkeit?
Sammlung, Auswertung – und der Datenschutz?

Vielen Dank für die Aufmerksamkeit!

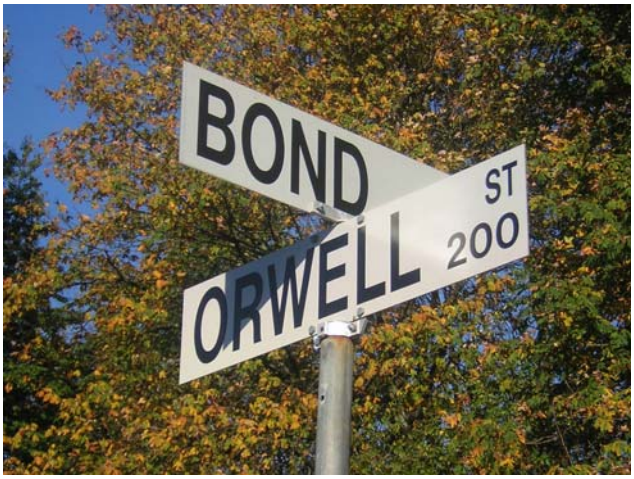


Foto: id

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://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


ULD
www.datenschutzzentrum.de
Annex: Beispiele für Selbstschutz-Tools
E-Mails verschlüsseln
GnuPG
https://www.gnupg.org/
OpenPGP ALLIANCE
http://www.openpgp.org/
Datensparsam suchen
ixquick
https://ixquick.de/
start page
https://www.startpage.com/
Festplattenbereiche verschlüsseln
TRUECRYPT
https://www.truecrypt.org/
Anonym surfen & Browser datensparsam konfigurieren (auch mobil)
JonDonym
https://www.anonym-surfen.de/
https://www.anonym-surfen.de/jondofox.html
BROWSER BUNDLE
https://www.torproject.org/
https://www.torproject.org/projects/torbrowser.html
https://guardianproject.info/apps/orbot/
Mobile Messaging verschlüsseln
Threema.
https://threema.ch/
Neue Entwicklungen:
Attributbasierte Berechtigungsnachweise
ABC4TRUST
https://abc4trust.eu/
Sammlung, Auswertung – und der Datenschutz?