

# Digitale Selbstverteidigung

Anton + Gunter + Olaf

Barcamp Graz, 12.4.2014

CRYPTO  
PARTY

# Überblick

- Daten-Spuren im Netz
  - Wer sammelt Daten?
  - Wo wird gesammelt?
  - Was wird gesammelt?
- Schutzmöglichkeiten
  - Was kann ich dagegen tun ?

# Wo hinterlasse ich Spuren im Netz?

1. Der Staat als Datensammler
2. Geheimdienste als Datensammler
3. Firmen als Datensammler
4. ICH als Datensammler

Unsere Daten werden von Firmen aus **wirtschaftlichem** Interesse gesammelt

# **1. Der Staat als Datensammler**

# 1. Der Staat als Datensammler

## Vorratsdatenspeicherung

- 27. **Bundesgesetz** zur Änderung des Telekommunikationsgesetzes 2003 –  
TKG 2003 BGBl. I Nr. 27/2011  
[http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA\\_2011\\_I\\_27](http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2011_I_27)
- Umsetzung der **EU-Richtlinie** 2006/24/EG

Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur **Registrierung von elektronischen Kommunikationsvorgängen**, (ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren, wie z.B. eine terroristische Bedrohungssituation, bestehen).

# Vorratsdatenspeicherung in Österreich

## Was wird gespeichert ?

- es müssen ausschließlich sog. „**Verbindungsdaten**“ (Telefon und Internet) erfasst werden
- Kommunikations**inhalte** sind von dieser Pflicht nicht betroffen
- diese **Metadaten** werden ein halbes Jahr lang gespeichert
- auf gerichtliche Anordnung bei Verdacht einer schweren Straftat müssen sie den Strafverfolgungsbehörden übermittelt werden (unter Geltung des Vier-Augen-Prinzips)
- Einführung der Vorratsdatenspeicherung in Ö: 1.4.2012
  - [https://de.wikipedia.org/wiki/Vorratsdatenspeicherung#Umsetzung\\_in\\_.C3.96sterreich](https://de.wikipedia.org/wiki/Vorratsdatenspeicherung#Umsetzung_in_.C3.96sterreich)

## Wer speichert ?

- Netzbetreiber

## Aufhebung ?

- Am 8.4.2014 entschied der EuGH: Regeln zur Vorratsdatenspeicherung verstoßen gegen EU-Recht

→ Änderungsbedarf in EU-Ländern; VfGH muß weitere österr. Vorgangsweise festlegen

# Wer darf auf die Vorratsdaten zugreifen ?

Zugriff auf die Daten haben

- Polizei,
- Staatsanwaltschaft und
- ausländische Staaten, die sich davon eine verbesserte Strafverfolgung versprechen. (gilt für D)

# Was kann man mit Metadaten machen ?

Mithilfe der über die gesamte Bevölkerung gespeicherten Daten können

- **Bewegungsprofile** erstellt,
- **geschäftliche Kontakte** rekonstruiert und
- **Freundschaftsbeziehungen** identifiziert

werden.

**Rückschlüsse** auf

- den Inhalt der Kommunikation,
- auf persönliche Interessen und
- die Lebenssituation der Kommunizierenden

werden möglich.



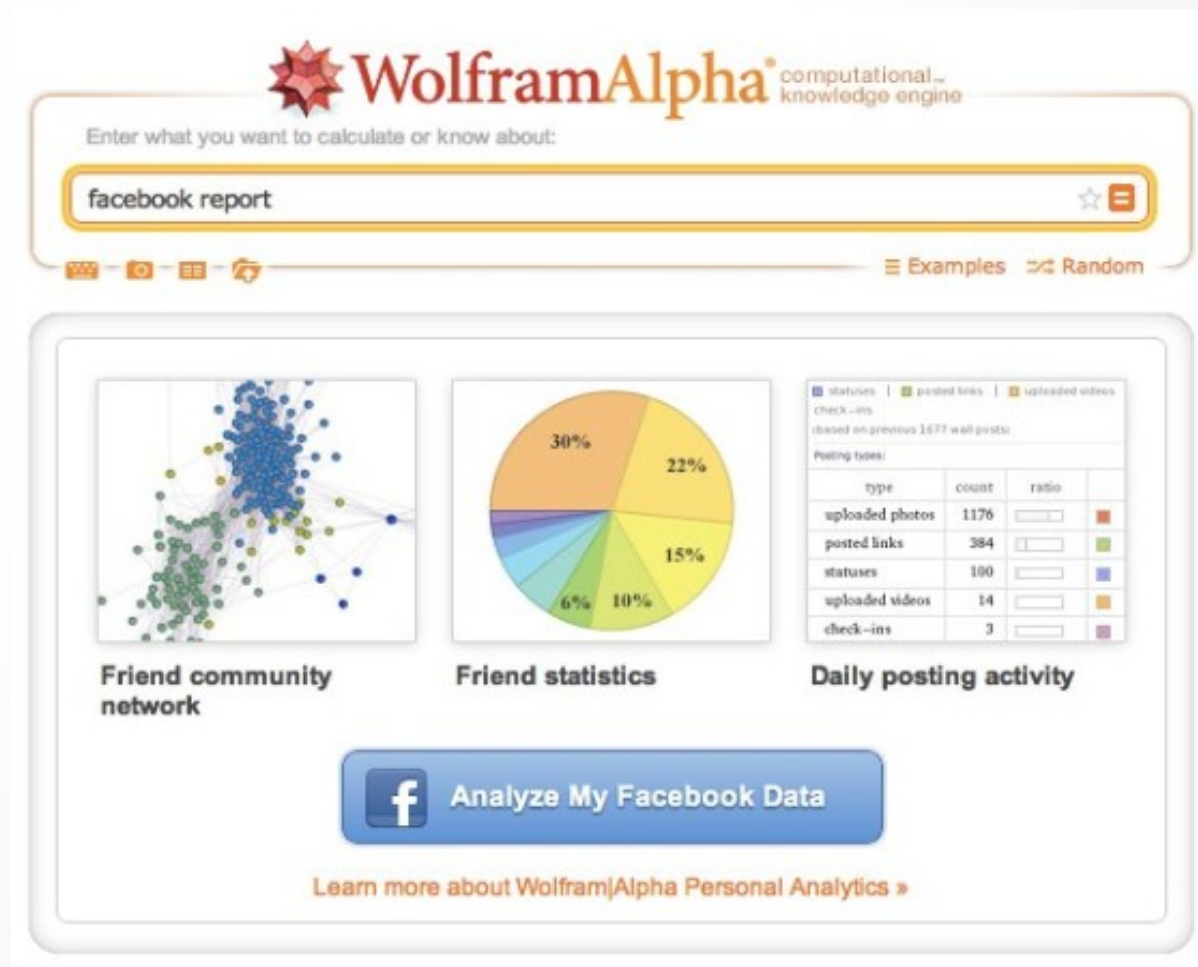
# Metadaten-Auswertungs-Studie

von Jonathan Mayer et. al. (Stanford)

- versuchten Methoden und Datensammeln der NSA nachzustellen
- 500 Telefonnutzer, 5 Monate lang mitgetrackt
- nur Metadaten erfasst
- Aus diesen Metadaten sind Schlussfolgerungen möglich über menschliche Verfehlungen:
  - \_ außereheliche Affären
  - \_ Geschlechtskrankheiten
  - \_ Waffenbesitz
  - \_ Drogenhandel

# Facebook-Profilanalyse

verwenden kann man als einfaches Tools die Suchmaschine Wolfram Alpha (<http://www.wolframalpha.com>)





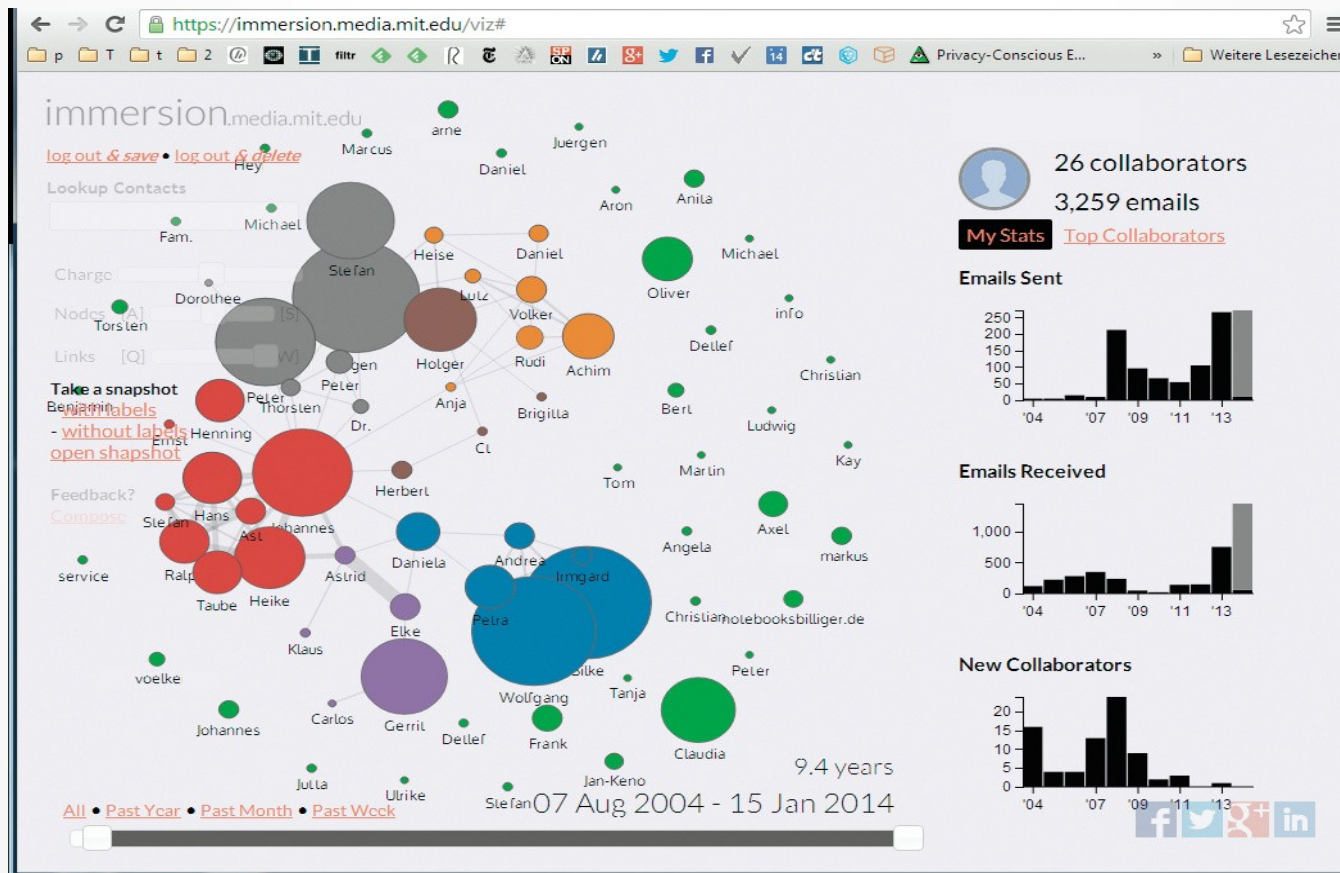
# Facebook-Profilanalyse

Beispiele zur Facebook-Profilanalyse findet man hier:

- <http://t3n.de/news/facebook-profilanalyse-wolfram-411847/>
- <http://www.wolframalpha.com/facebook/>
- <http://www.wolframalpha.com/fbfaqs.html>
- <http://blog.stephenwolfram.com/2013/04/data-science-of-the-facebook-world/>

# Immersion: Auswertungs-Tool für Email-Kommunikation

Ein weiteres Tool, das die Email-Kommunikation auswertet und visualisiert ist Immersion  
<https://immersion.media.mit.edu/>



<http://t3n.de/news/weis-google-dich-immersion-479005/>

<http://abcnews.go.com/Technology/app-week-immersion/story?id=19993754>

# Abgefragte Vorratsdaten nach Delikten

(Zeitraum: 1.4.2012 bis 31.3.2013)

Anzahl	Delikt
106	Diebstahl (gewerbsmäßig, schwer, durch Einbruch, im Rahmen einer kriminellen Vereinigung)
40	Suchtgifthandel
36	beharrliche Verfolgung
31	Raub, schwerer Raub
29	Betrug (schwer, gewerbsmäßig)
16	unerlaubter Umgang mit Suchtgift
13	gefährliche Drohung
10	kriminelle Vereinigung

# Abgefragte Vorratsdaten nach Delikten

(Zeitraum: 1.4.2012 bis 31.3.2013)

Anzahl	Delikt
8	versuchte Nötigung
je 7	Sachbeschädigung; schwere Sachbeschädigung; Urkundenunterdrückung; Vorbereitung von Suchtgifthandel
je 6	versuchter Diebstahl (gewerbsmäßig, schwer, durch Einbruch); Entfremdung unbarer Zahlungsmittel
je 5	Körperverletzung; schwere Körperverletzung; versuchte Erpressung; Brandstiftung; falsche Beweisaussage; Missbrauch der Amtsgewalt; Schlepperei
je 4	Nötigung, schwere Nötigung; betrügerischer Datenverarbeitungsmissbrauch; vorsätzlicher Eingriff in Monopolrechte
je 3	Mord; Erpressung, schwere Erpressung; Hehlerei; Verleumdung

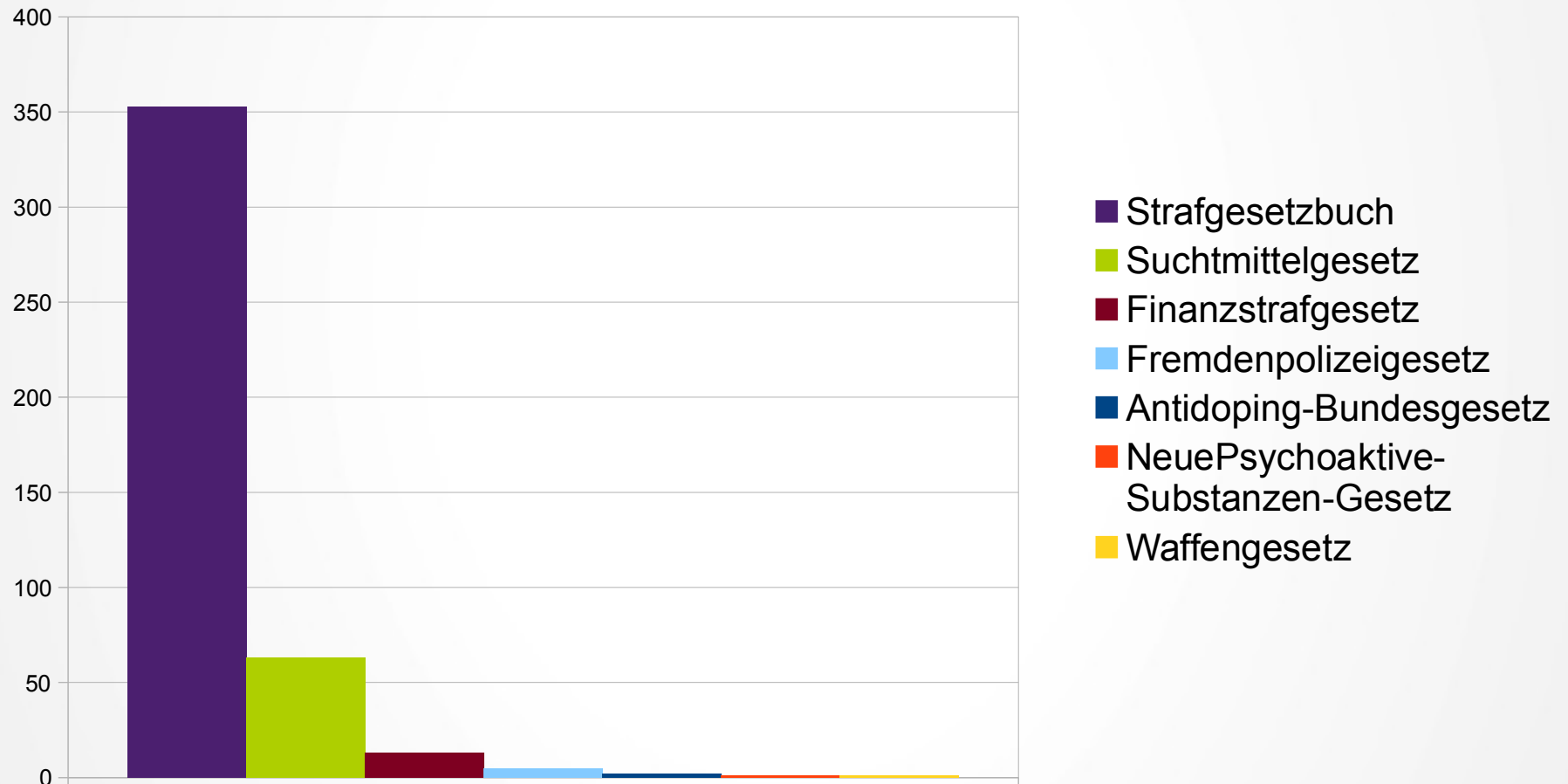
# Abgefragte Vorratsdaten nach Delikten

(Zeitraum: 1.4.2012 bis 31.3.2013)

Anzahl	Delikt
je 2	versuchter Mord; Veruntreuung; versuchter Raub; versuchter Betrug (schwer, gewerbsmäßig); Geldwäscherei; Vergewaltigung; schwerer sexueller Missbrauch von Unmündigen; Missbrauch eines Autoritätsverhältnisses; Urkundenfälschung, Fälschung besonders geschützter Urkunden; Fälschung unbarer Zahlungsmittel; Vortäuschung einer mit Strafe bedrohten Handlung; gerichtl. Strafbare Handlungen zu Zwecken des Dopings; Abgabenhinterziehung (als Mgl. einer Bande oder unter Gewaltanwendung); Abgabenhhehlerei, gewerbsmäßige Abgabenhhehlerei
je 1	Körperverletzung mit tödlichem Ausgang; versuchte absichtliche schwere Körperverletzung; Raufhandel; fortgesetzte Gewaltausübung; räuberischer Diebstahl; Unterschlagung; unbefugter Gebrauch von Fahrzeugen



# Vorratsdaten nach Gesetzen

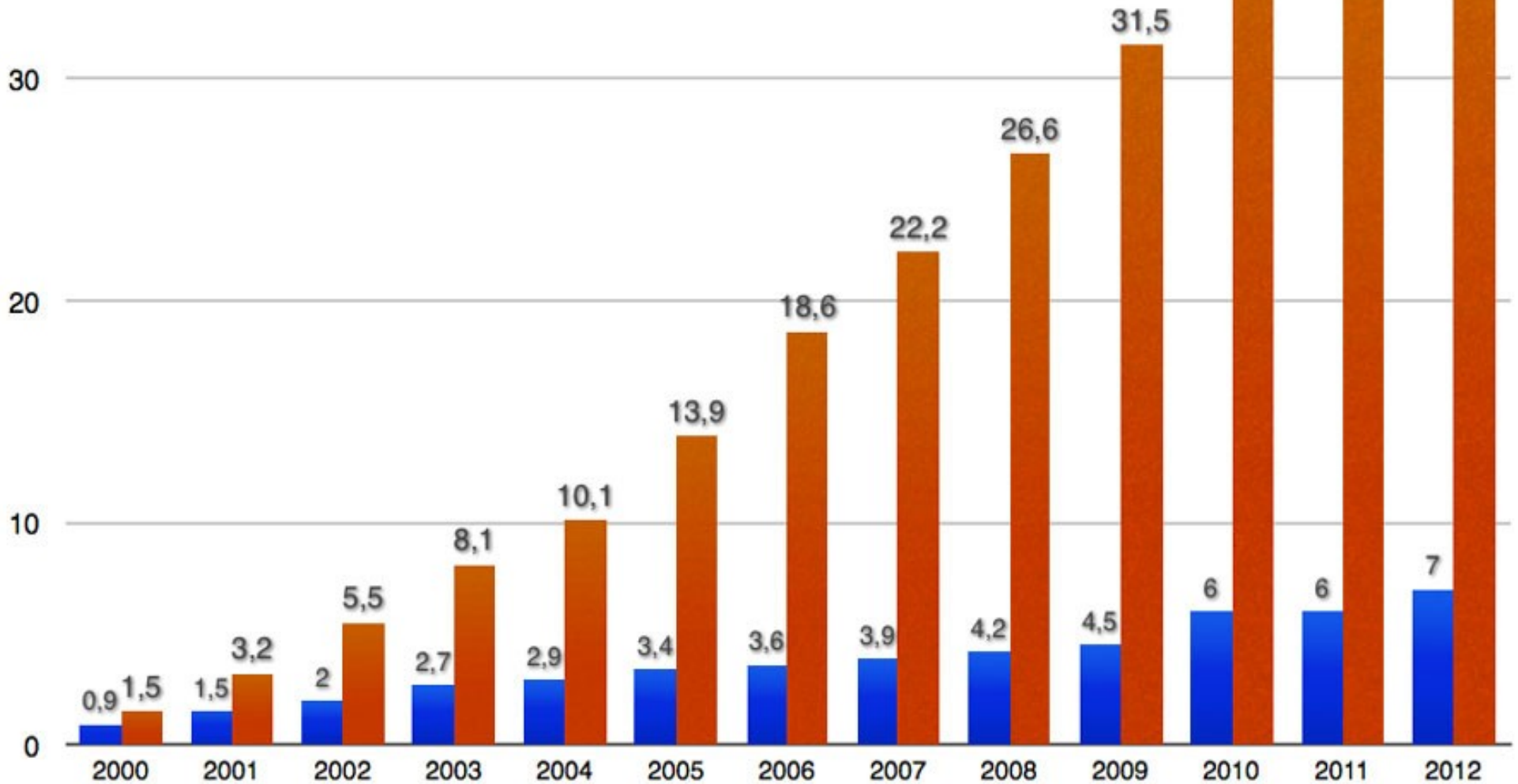


# Abfragen der Sicherheitsbehörden von Bestandsdaten in Deutschland

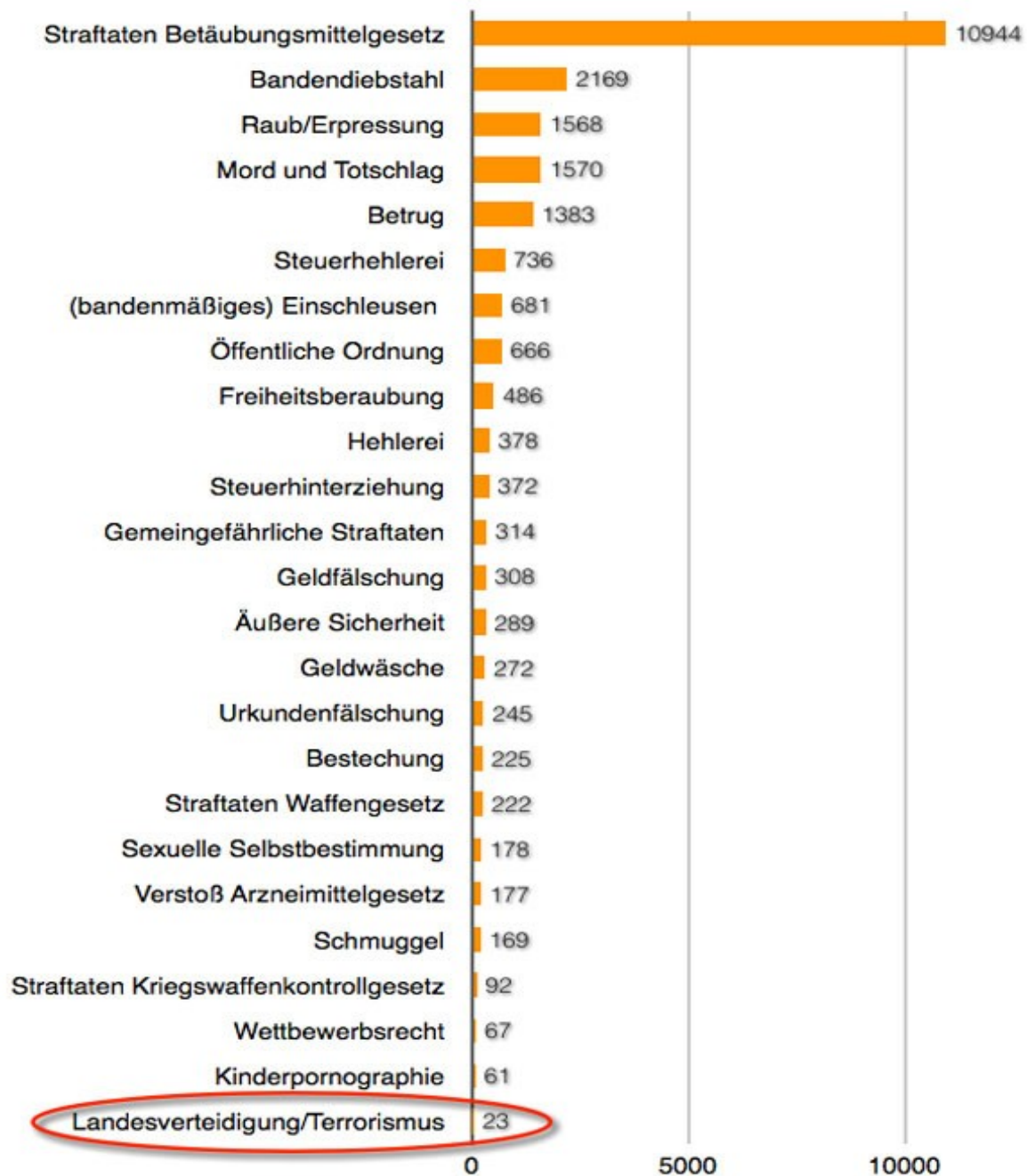
40

Millionen

■ Ersuchen von Sammelstellen ■ Abfragen bei TK-Diensteanbieter



## Anlässe für Telekommunikationsüberwachung in Deutschland 2012



# Probleme

- beim Erstellen der Profile können **falsche Schlüsse** gezogen werden
- aus Maßnahmen zur Terrorbekämpfung wird eine **Generalüberwachung**
- das Grundvertrauen des Staats gegenüber dem Bürger wird zu einem **Grundmisstrauen**
- wer kontrolliert die Behörden gegen **Missbrauch** ?
  - <https://www.netzkinder.at/wer-schutzt-unsere-vorratsdaten/>

## **2. Geheimdienste als Datensammler**

# „Big Data“

- NSA speichert täglich **6 Milliarden Metadaten** (Emails, Telefonate, SMS)
- das entspricht etwa der Menge von **500 Millionen Büchern** pro Tag

(Quelle: Heise-Newsticker 31.3.2014, <http://www.heise.de/newsticker/meldung/NSA-sammelt-angeblich-sechs-Milliarden-Metadaten-am-Tag-2158633.html>)

- Seit Anfang dieser Woche wird vermutet: Österreich wird durch die NSA wahrscheinlich „totalüberwacht“

<http://www.format.at/articles/1414/524/374054/nsa-oesterreich>

- Was machen andere Geheimdienste ?

# **3. Firmen als Datensammler**



# Apps speichern Daten

## **Video: Apple. Google. Facebook. Amazon**

- <https://www.youtube.com/watch?v=7EscDalw0tg#t=24>

Apps speichern diverse Daten aus den Handies:

- Adressbücher,
- Geodaten,
- Surf- und Leseverhalten,
- Bookmarks,
- Privatfotos...
- Bsp.: Taschenlampen-App, WhatsApp

# Spezielle Datensammel-Hardware

- eBook-Reader
  - [https://www.unwatched.org/20121216\\_Datenschutz\\_Welche\\_E-Book-Reader\\_ihre\\_Leser\\_tracken](https://www.unwatched.org/20121216_Datenschutz_Welche_E-Book-Reader_ihre_Leser_tracken)
  - <http://www.welt.de/wirtschaft/webwelt/article114505544/E-Book-Reader-senden-Nutzerdaten-in-die-Zentrale.html>
- Navigationssystem im Auto
  - <http://www.zeit.de/digital/datenschutz/2011-04/navi-polizei-radarfalle>
- Personal Tracking-Geräte
  - <http://www.heise.de/tp/artikel/41/41323/1.html>
- Zombie-Haushaltsgeräte ?
  - [https://www.telefoniert-nach-hause.de/index.php/Chinesische\\_B%C3%BCgeleisen](https://www.telefoniert-nach-hause.de/index.php/Chinesische_B%C3%BCgeleisen)

Liefern Daten über das Nutzungsverhalten an den Hersteller

# **4. Soziale Netzwerke und der Datenschutz**

# Überwacher: YOU

JedeR liefert selbst freiwillig viele Informationen über sich und sein persönliches Umfeld durch Postings in Sozialen Netzen ab. Dabei ist man Kunde und Lieferant der Daten, die meist an Drittfirmen weitergegeben werden.

Titelbild von TIME vom 25.12.2006:

- <http://content.time.com/time/covers/0,16641,20061225,00.html>

„You — Yes, You — Are TIME's Person of the Year

- In 2006, the World Wide Web became a tool for bringing together the small contributions of millions of people and making them matter.“
- <http://content.time.com/time/magazine/article/0,9171,1570810,00.html>

Siehe auch:

- [https://en.wikipedia.org/wiki/You\\_%28Time\\_Person\\_of\\_the\\_Year%29](https://en.wikipedia.org/wiki/You_%28Time_Person_of_the_Year%29)
- [http://en.wikinews.org/wiki/Time\\_magazine%27s\\_2006\\_Person\\_of\\_the\\_Year\\_is\\_%22you%22](http://en.wikinews.org/wiki/Time_magazine%27s_2006_Person_of_the_Year_is_%22you%22)

# Lösungsebenen

- **Politisch**

- Netzpolitik: Datenschutz, Vorratsdatenspeicherung, Netzneutralität

- **Technisch**

- Datenschutz by default
- Hardware und Software überwachungssicher machen
- dezentrale Netzwerke nutzen

- **Individuell**

- Die Spuren, die wir im Netz hinterlassen auf ein Minimum beschränken

# Was können wir selbst konkret tun?

- Verschiedene Browser verwenden
- Online-Banking nicht vom Handy
- Eigene Kreditkarte für online-Käufe  
(Verknüpfung online – offline erschweren)
- Freie Software verwenden
- Datenschutzeinstellungen anpassen
- Sichere Passwörter finden
- Emails verschlüsseln → Workshop
- Digitalen Fingerprint verbessern → Workshop