# Digitale Emanzipation

## Datenschutz und Bürgerrechte

Katharina Spiel
*Sprecherin der LAG Medien*

20. Mai 2014

BÜNDNIS 90
DIE GRÜNEN
LANDESVERBAND THÜRINGEN

# Vorschau

## No Scandal Ahead

- Wann?
- Was?
- Wie?
- Wo?

## Was war da mit meinen Rechten?

- Privatsphäre
- Bürgerrecht vs. Menschenrecht
- Was macht der Staat?
- Digitale Integrität

## Und was jetzt?

- Surveillance Shift
- Kryptographie, aber wie?
- Komplex(itätsproblem)e
- Die da oben machen ja eh nix.

# No Such Agency

# Wer?

- National Security Agency (NSA)
- Auslandsgeheimdienst
- Analog zu einer Mischung aus Bundesnachrichten Dienst (BND) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Zwei Aufgaben:
  - Klassische Spionage in einem technischen Umfeld
  - Kryptographische Forschung (Entwicklung neuer Algorithmen und Kontrolle existierender)
    aber: Meist Closed oder Partly-Closed Source

# Wann?

- 1952 – Gründung der NSA durch President Truman
- 1973 – Oberster Gerichtshof der Vereinigten Staaten entscheidet, dass für innerstaatliche Abhörmanöver ein Durchsuchungsbefehl vorliegen muss
- 1975 – US-Senat bekommt das erste Mal Hinweise auf innerstaatliche Abhörmanöver
- 1978 – Foreign Intelligence Surveillance Act (FISA)
- ...

# Wann?

- ...
- 2001 – 11. September führt zu erweiterten Befugnissen für die NSA
- 2002 – 2012 – Weitere Erweiterungen der Befugnisse
- 2005 – Bush bestätigt NSA
- 2005 – *heute* – erfolglose Gerichtsverfahren und politische Projekte durch die Electronic Frontier Foundation (EFF) und andere
- 05/2013 – Edward Snowden flieht nach Hong Kong

# Was?

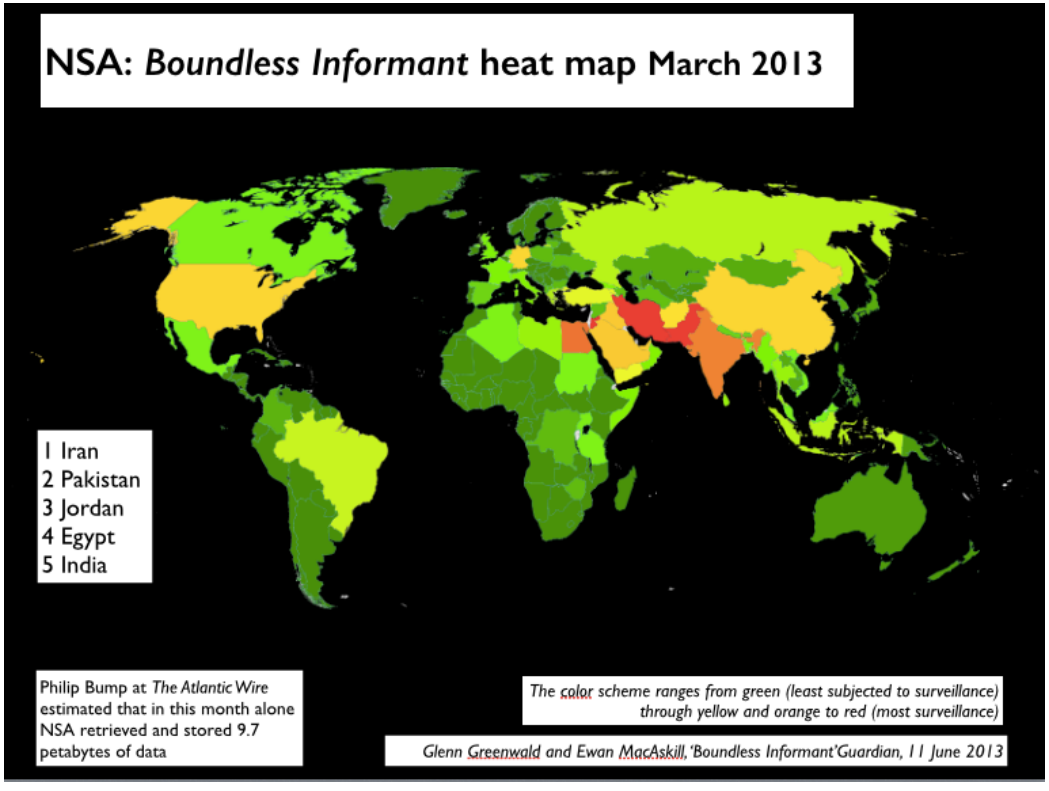
- Telephonische Kommunikation
- Digitaler Datentransfer
- Fokus auf 'Terrorist*innen' und Wirtschaftsspionage

# Wie?

- Speichern, Speichern, Speichern
- Kontextuelle Textanalyse
- Hacken, Hacken, Hacken (oder zumindest der Versuch)

# Wo?

## Weltweit.




Bildquelle: `http://geographicalimaginations.files.wordpress.com/2013/10/boundless-informant-march-2013-heat-map.png`

# Privatsphäre

- Unterscheidung öffentliches und nicht-öffentliches Leben
- Recht auf Privatheit und damit Recht auf Geheimnisse
- Konsequenz: Recht auf die Kontrolle über die eigenen Daten
- Privatsphäre ist ein Menschenrecht!

# Bürgerrecht vs. Menschenrecht

- Bürgerrecht: Exklusive Angelegenheit von (Staats)bürgern
- Menschenrecht: Inklusiv und allgemein gültig
- Menschenrechte gelten jenseits von Staatsgrenzen!

# Was macht der Staat?

Festgeschriebene Rechte im Persönlichkeitsbereich

- Schutz personenbezogener Daten (Landesrecht, aber weitgehend vereinheitlicht)
- Post- und Fernmeldegeheimnis (Art. 10, GG)
- Unverletzlichkeit der Wohnung (Art. 13, GG)

... und zusätzlich: Landes- und Bundesdatenschutzbeauftragte (mit limitierten Beratungsrechten)

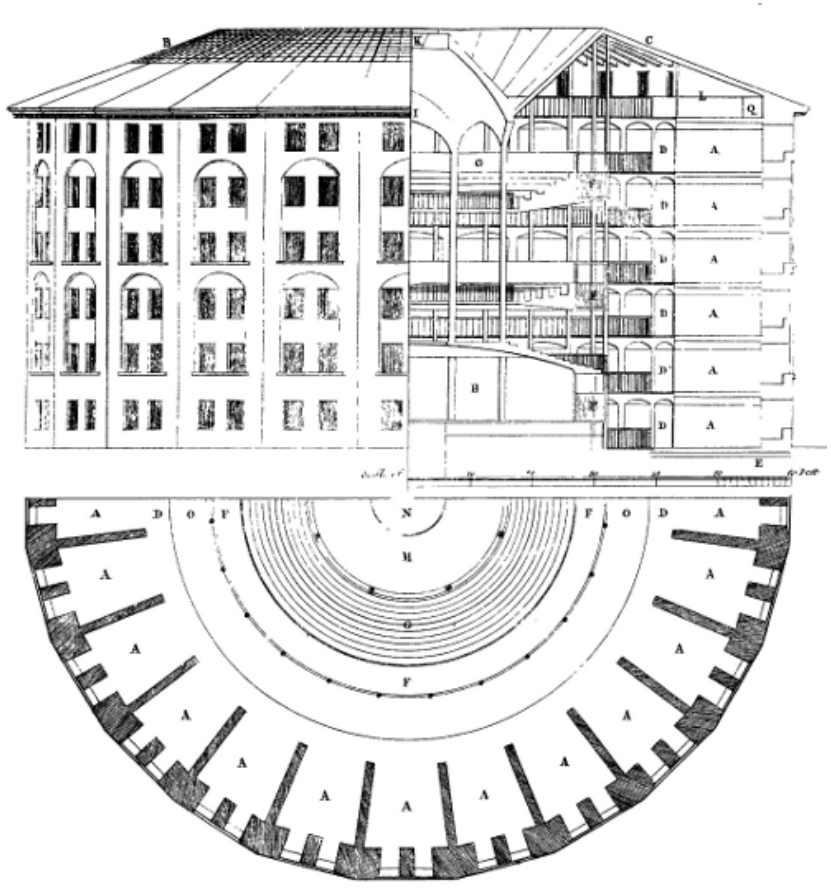
# Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

- 2007 – Verfassungsbeschwerden gegen das Gesetz zur Online Durchsuchung in NRW
- 2008 – vom Bundesverfassungsgericht als Ausbildung des allgemeinen Persönlichkeitsrechtes definiert
- Rechtlich Auffanggrundrecht mit Art. 10 und Art. 13 GG als Grundlage

Aber: Praktische Umsetzung fehlt immer noch

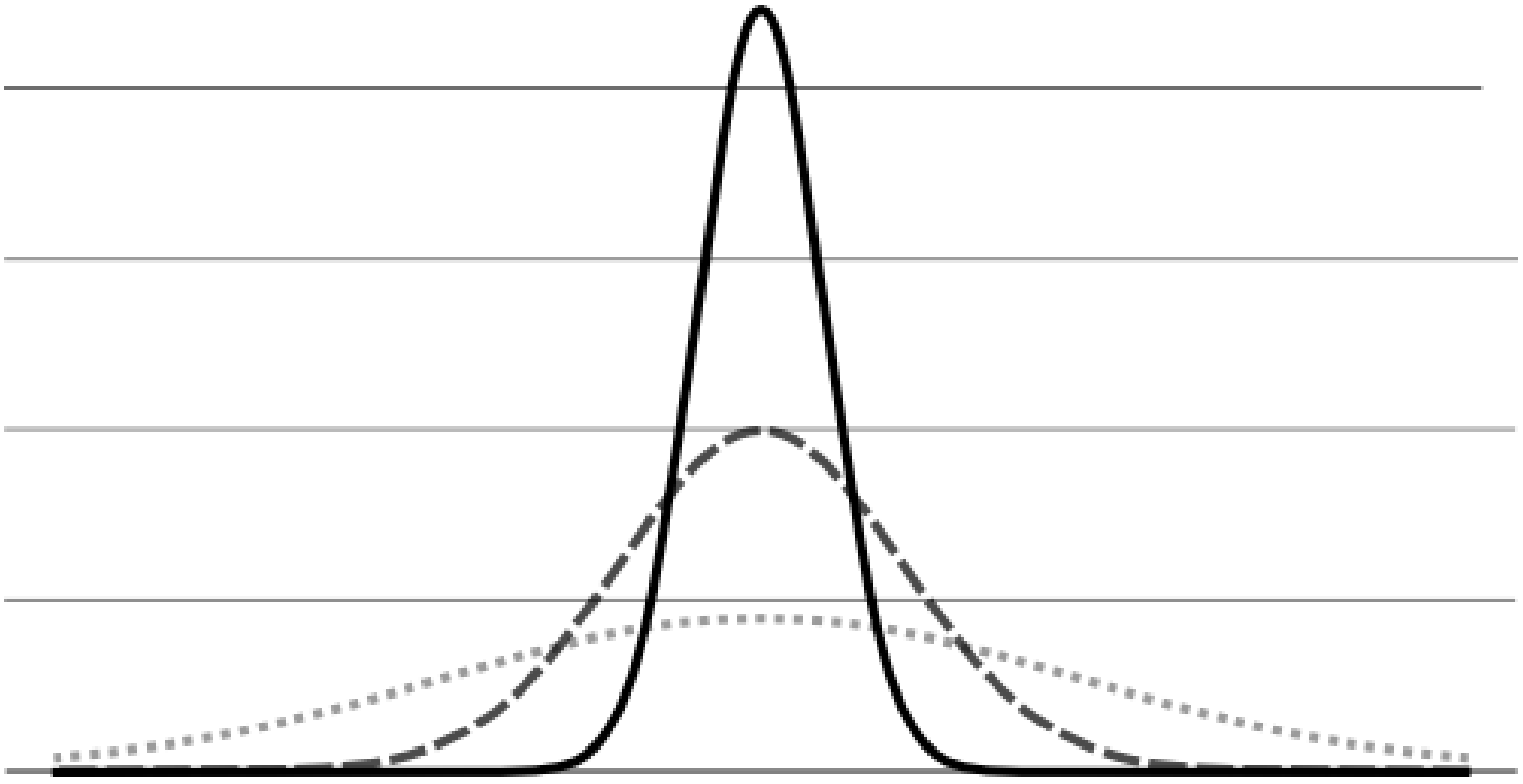
# Surveillance Shift

## Aus Discipline and Punish...



# Surveillance Shift

... wird Observe and Calculate.



# Warum meine Mutter kein PGP benutzt...

- Emails und Postkarten
- Users' Mental Models vs. Realität
- Was ist eigentlich dieser unleserliche Block unterhalb deiner Email?

# Brief und Siegel

Bildquelle: Justin Henry via flickr

# Kryptographie, aber wie?

Kryptographische Forschung beschäftigt sich maßgeblich mit:

- der Verschlüsselung von Datenströmen
- der Sicherung von Authentizität und Integrität von Datenströmen
- der Kombination der beiden Ansätze

# Probleme mit Kryptographie

- Wer konzipiert kryptographische Protokolle?
- Wer implementiert Kryptobibliotheken?
- Wer kontrolliert Kryptobibliotheken?
- Wer benutzt Kryptobibliotheken?

# Goto Fail

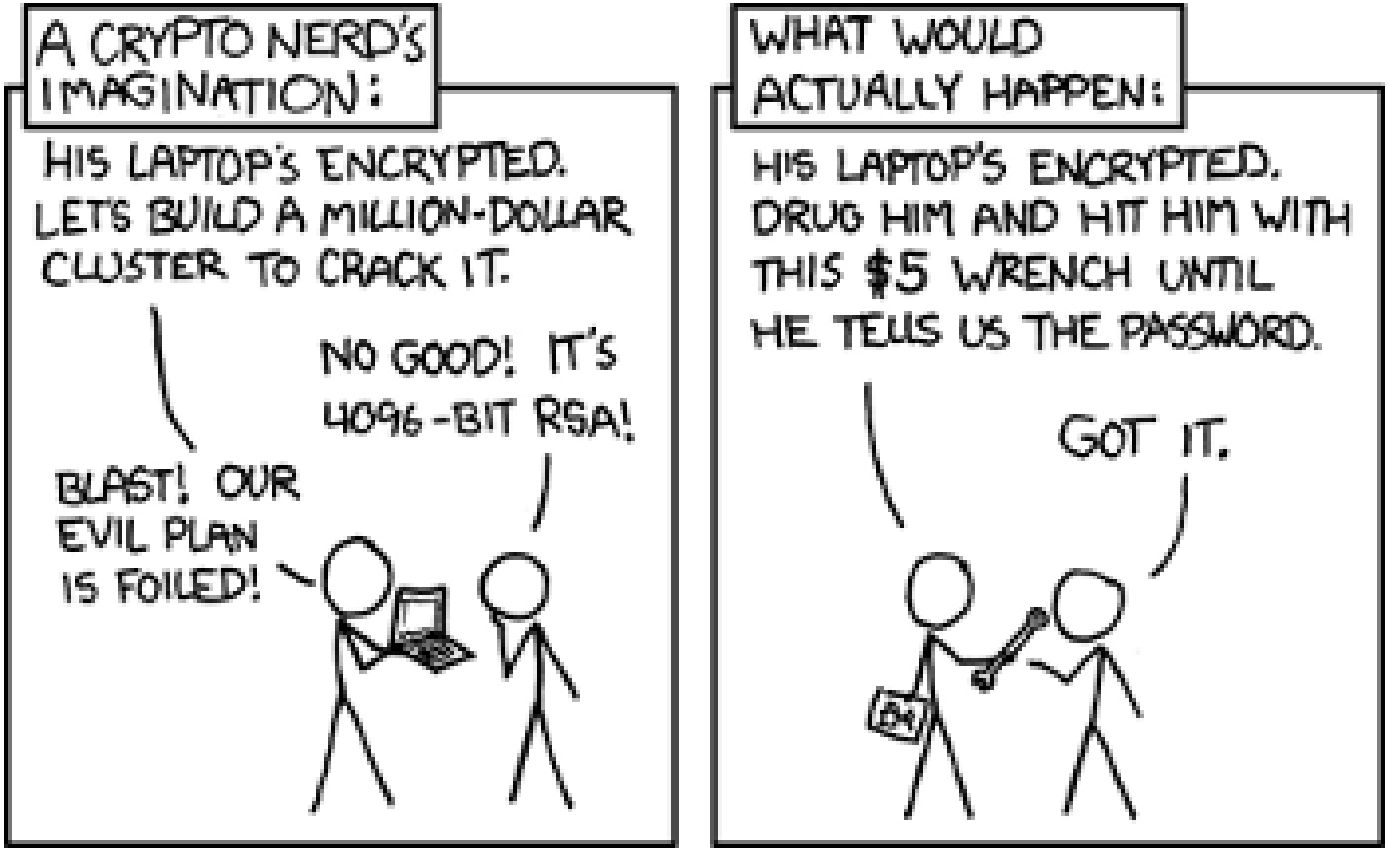
```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParam
                                 uint8_t *signature, UInt16 signatureLen)
{
    OSStatus        err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

# Konzeptuelle Probleme mit Kryptographie

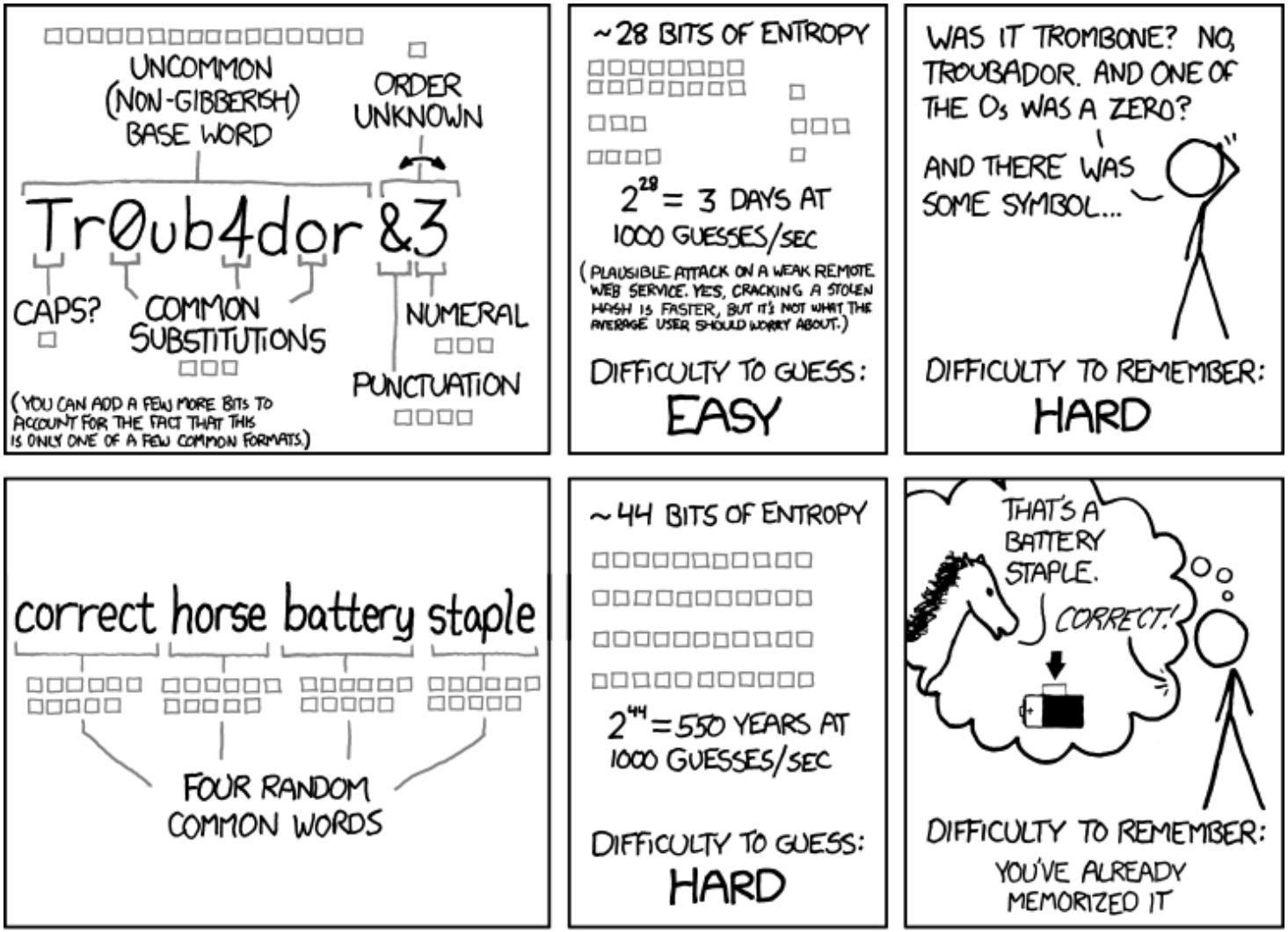
Paranoia vs. reale Welt als Angriffsszenario



# Was kann passieren?

| | | | |
|---|---|---|---|
| **Gefahr** | Ex-Freund*in will in den Emailaccount | Organisiertes Verbrechen will Spam über dich senden | Der Mossad |
| **Lösung** | Starke Passwörter | Starke Passwörter & gesunder Menschenverstand | Vergiss es |

# Starke Passwörter?



# Rule 34

Rule 34: If it exists, there is porn of it. No exceptions.

Für Passwörter: Wenn du es dir vorstellen kannst, hat es irgendjemand schon gepostet.
Zusätzlich: Unterschiedliche Passwörter für unterschiedliche Accounts oder:

> *Now I'm expected to remember both "Gigantic Martian Insect Party"and "Structurally Unsound Yeti Tote-bag" and I have to somehow recall which phrase is associated with my banking web site, and which on e is associated with some other site that doesn't involve extraterrestrial insects or Yeti accoutrements.*

# Die da oben machen ja eh nix.

Oder doch? ...

- Schlandnet
- Gute Beziehungen zu den USA
- Anti-Spionage Vereinbarung

Aber seit über einem Jahr ist noch nichts effektiv passiert.

# Forderungen an die Politik

- Zertifiziertes Code-Auditing
- Verhandlung der NSA-Affäre vor dem Internationalen Gerichtshof
- Medienbildung nicht nur als Contentbildung verstehen

# Erwartungen an die Wissenschaft

- Usability und Kryptographie stärker in den Mittelpunkt rücken
- Starke Passwörter, aber wie?
- Herangehensweisen beim Design sicherer Systeme
- technisch informierte kulturwissenschaftliche Analysen von Kryptographie und ihren Methoden

# Was kann ich jetzt machen?

- Calm Down, but don't carry on as usual
- Zwischenlösung für starke Passwörter: keepass.info oder lastpass.com
- Aufklären!
- Forschen!
- Politisch Einfluss nehmen!

Es gibt viel zu tun. Packen wir's an!

# Quellen


- https://www.eff.org/nsa-spying/timeline
- http://www.nsa.gov/
- Gerhart R. Baum, Constanze Kurz und Peter Schantz: Das vergessene Grundrecht http://www.faz.net/aktuell/feuilleton/debatten/datenschutz-das-vergessene-grundrecht-12095331.html
- Katharina Spiel: Observe and Calculate; in: XII. Conference Culture and Computer Science (2014)
- James Mickens: This World of Ours; in: USENIX ;login: logout, (January 2014)
- Kai Biermann und Marin Majica: Ein Schlandnet würde nur der Telekom nützen http://www.zeit.de/digital/internet/2013-11/schlandnet-telekom-nsa-internet
- heise.de: Verfassungsschutz: Weiter gute Beziehungen zu Geheimdiensten der USA http://www.heise.de/newsticker/meldung/Verfassungsschutz-Weiter-gute-Beziehungen-zu-Geheimdiensten-der-U html
- Dirk Banse und Manuel Bewarder: Deutschland will nicht in den Spionageklub http://www.welt.de/politik/deutschland/article123083267/Deutschland-will-nicht-in-den-Spionageklub.html
- Ladar Levison: Secrets, lies and Snowden's email: why I was forced to shut down Lavabithttp://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email