

Aber ich habe doch nichts zu verbergen!

Wege zu digitaler Mündigkeit



CryptoParty Graz

Wer ist die CryptoParty Graz ?

- Vorstellung CryptoParty Graz

CryptoParties gibt es seit 2012 auf der ganzen Welt, in Graz seit 2013

- Die **CryptoParty Graz** besteht aus einer Kerngruppe von etwa 10 Personen, die sich regelmäßig treffen

<https://cryptoparty.at/graz>



SICHERE DEINE
KOMMUNIKATION

UND LASSE
DIE HERZKÖNIGIN
MIT IHRER
WÜTENDEN
TRAGIK STEHEN?

CRYPTOPARTY

im SPEKTRAL
Lendkai 45

WAS MACHEN WIR?

WIR ZEIGEN, WIE MAN SICHER
ONLINE KOMMUNIZIERT,
UND DABEI DEN SPASS UND
DIE PARTY NICHT ZU KURZ
KOMMEN LÄSST!

Jeden ersten
Montag
im Monat
ab 19.00

cryptoparty.at/graz

Unsere „Themen“

- Bewusstseinsbildung
- Email-Verschlüsselung
- Web-Tracking und Gegenmaßnahmen
- Passwörter und Tresore
- Festplatten-Schutz durch Verschlüsselung
- Sicherheit am Handy



Cryptoparty-Montag

(1. Montag im Monat)

Nächste Termine:

- **5.10.2015**
- **2.11.2015**
- **7.12.2015**

Ab 19 Uhr im **Spektral**, Lendkai 45



Hilfe, Tipps, Party und mehr !



CryptoParty-Montag in Graz



Überblick über den URANIA-Kurs

- Heute:
Einführung in den Themenbereich (Gunter)
- 8.10.:
Sichere Passwörter (Bernhard)
- 15.10.:
Sicheres Email durch Verschlüsselung (Olaf)
- 22.10.:
Sicheres Web-Surfen / Web-Tracking und Gegenmassnahmen (Anton)



Seit den Aufdeckungen von Edward Snowden wissen wir, dass unsere digitale Kommunikation weltweit von Geheimdiensten überwacht wird.

- Manche wussten / vermuteten das auch schon vorher...

- vor 25 Jahren:

- z.B. Der Spiegel vom 20.2.1989

- “NSA: Amerikas großes Ohr“

- <http://www.spiegel.de/spiegel/print/d-13494509.html>

-

Echelon-System = globales elektronisches Aufklärungssystem

- Siehe z.B. Erich Moechel, www.fuzo-archiv.at/artikel/1652079v2



Totalüberwachung

- Warum wird überwacht ?
- Wer überwacht uns?
- Wo wird überwacht ?
- Was kann man/frau dagegen tun ?

Warum Überwachung ?

- Staatliche Überwachung:
 - Schutz vor Verbrechen und Terrorismus („Krieg gegen Terror“)

Warum Überwachung ?

- **Firmen als Überwacher:**
 - Wir wollen den KundInnen maßgeschneiderte, optimierte Produkte anbieten.
 - Deshalb sollten wir die Wünsche der KundInnen genau kennen.
 - Und deshalb sammeln wir
 - Interessensprofile
 - Tätigkeitsprofile
 - Persönlichkeitsprofile

Und:

- Prognosen über zukünftiges Verhalten können gemacht werden

Wer sammelt Daten ?

- Der Staat als Datensammler
- Geheimdienste als Datensammler
- Firmen als Datensammler
- Internet der Dinge
- Kriminelle
- Ich selbst



Der Staat als Datensammler

Vorratsdatenspeicherung in Ö und EU gekippt, aber wieder in Diskussion

(keine präventive Wirkung gegen Terroranschläge)

- Melderegister der Gemeinden
- Finanzämter
- Versicherungen
- Grundbuch
- ...

Verknüpfung von online und offline Daten

Vorteile und Nachteile – die wichtigen Fälle sind so oft nicht greifbar



Geheimdienste als Datensammler

Geheimdienst NSA:

- 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)
- aktuell anfallende Datenmenge im Internet:

$2,5 \cdot 10^{18}$ Bytes pro Tag = 2.500.000 Terabytes pro Tag

(Quelle: www1.logistik.fh-dortmund.de/IT-Sicherheit/IW_und_Ueberwachungsstaat.pdf)



Geheimdienste als Datensammler

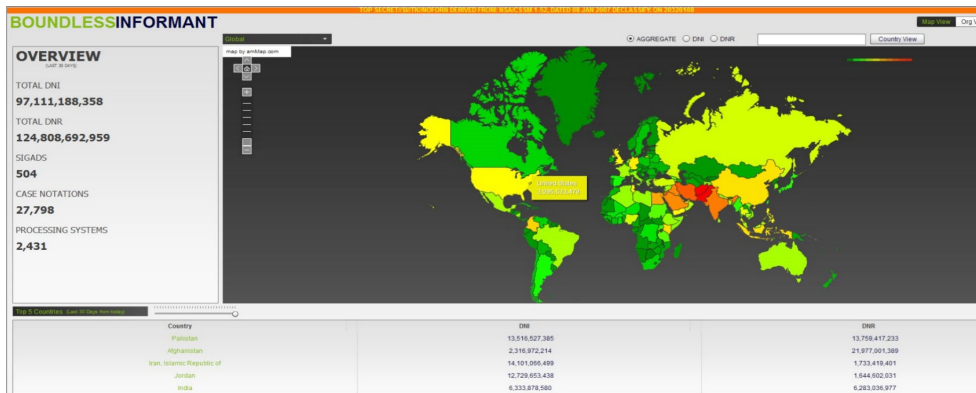
Britischer Geheimdienst GCHQ:

- Speicherte 2012 **täglich 50 Milliarden Metadaten** (Emails, Telefonate, SMS, Suchabfragen, Telefonstandorte, ...)
- Bis Jahresende 2012 war eine Verdopplung der Datenmenge geplant
- Die Datensammlung erfolgt bei grossen Webseiten
- Auswertung geschieht beinahe in Echtzeit
- Metadaten werden 1 – 6 Monate gespeichert, Kommunikationsinhalte 3 - 30 Tage lang
- Diese Daten stehen auch anderen Geheimdiensten zur Verfügung

Quelle: The Intercept, Der Standard 25.9.2015



Boundless Informant (eines der Überwachungsprogramme der NSA)

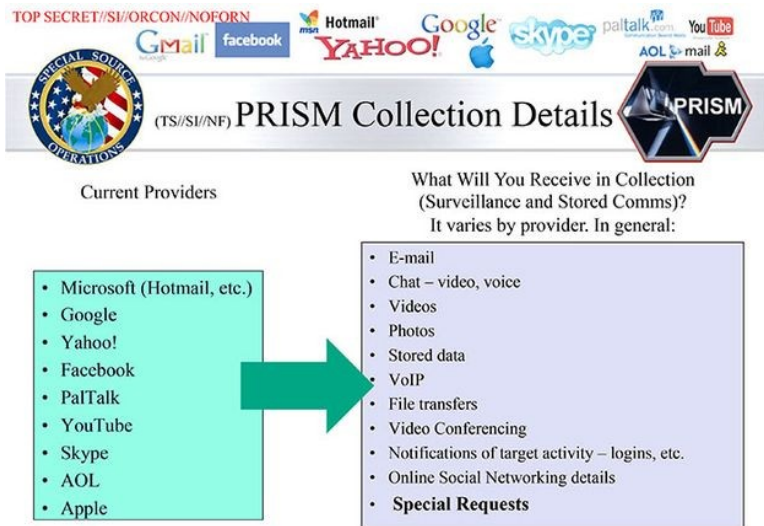


During a 30-day period, 97 billion internet data records (DNI) and 124 billion telephony data records (DNR) were collected.

Quelle: http://en.wikipedia.org/wiki/Boundless_Informant



PRISM (eines der Überwachungsprogramme der NSA)



Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN



Firmen als Datensammler

Bei **Anmeldung im Internet**:

- Sind die Angabe von Name, Vorname, Straße, Ort, Postleitzahl und E-Mail- Adresse nötig ?!?

Firmen benötigen **Kundendaten** für „Rechtsgeschäfte“
(z.B. Online-Einkauf)

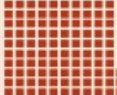
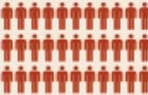
- Wohin sonst sollen sie die Ware schicken?
- Woher sonst sollen sie ihr Geld bekommen?

Daten-Sammelwut :

- bei vielen Anmeldungen würde nur ein Bruchteil der abgefragten Informationen genügen.



Die Macht der Internetkonzerne

	Umsatz ¹ 2013	Gewinn ¹ 2013	Beschäftigte 2013
 Apple	 191,9	 41,6	 80.300
 amazon	 83,7	 0,3	 117.300
 Google	 67,2	 14,5	 47.756
 Facebook	 8,8	 1,7	 6.337
Alle 20 ATX-Konzerne	 113,1	 5,1	 334.450

Quelle: „Vorstandsvergütung in ATX-Unternehmen“ AK (2014);
 U.S. Securities and Exchange Commission; Statista; AK/ÖGB-Darstellung.

¹ Mrd. Euro

Firmen als Datensammler

Daten sammeln als Geschäftsmodell

Wenn der Dienst gratis ist, sind wir die Waren
(aber auch, wenn er nicht gratis ist...)



Apps: Spione in der Hosentasche

Top-100-Apps



Android



iOS

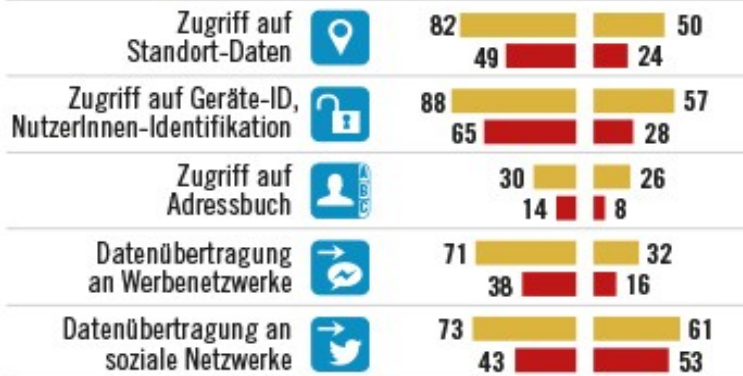
Anteil in %



kostenlos



kostenpflichtig



Einige Datensammler & Datenhändler

DISPLAY LUMAscape



 http://www.heise.de/tp/bild/43/43207/43207_1.html

© 2014 MA Partners LLC 2014



Internet der Dinge

- Smartmeter – Stromverbrauch
- Wasserverbrauch
- Kühlschränke: kennen unser Ernährungsverhalten
- Autoversicherung: Sensoren im Auto erfassen Fahrverhalten
- Smart Cities



Kriminelle

- Kriminelle, die an unsere Kennwörter und Konten heranwollen

z.b.

- Phishing-Mails
- Nigeria-Connection

Ich

Wir selber „liefern“ viele Daten:

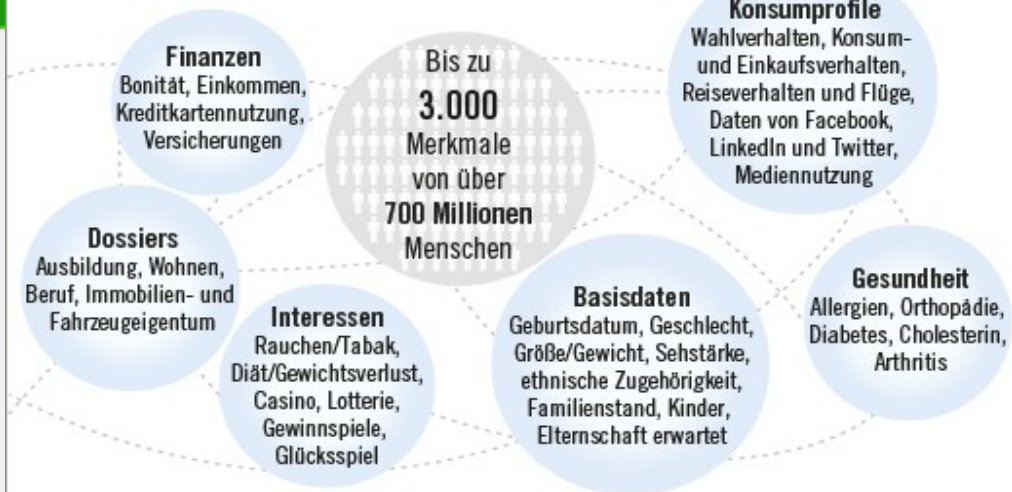
- durch Postings in Sozialen Netzen
- durch Verwendung von
 - Kreditkarten
 - Kundenkarten
 - Life-Tracker



Datenprofile

- Aus den gesammelten Daten werden Profile der Internet-Benutzer erstellt
 - „digitaler Schatten“
 - „digitales Ich“
- Diese **Datenprofile** mit tausenden Persönlichkeitsmerkmalen werden an Firmen verkauft (Versicherungen, Arbeitgeber, Internet-Werber ...)

Das Datenangebot des US-Datenhändlers Acxiom



Persönliche Daten sind bares Geld wert

		Adressen	Beschreibung	Preis pro T.
	Die Zeit	55.900	Shopkäufer und Buchserienkäufer	€ 210,00
	RTL Club	510.000	aktive Kunden	€ 180,00
	Elderly & Disabled	110.000	Spender	€ 175,00
	Tag des Herrn	52.400	Abonnenten katholische Wochenzeitung	€ 170,00
	Lehrer	246.100	mit Privatanschrift	€ 170,00
	Lehrer	367.700	mit Schulanschrift	€ 170,00
	Die Zeit	374.000	aktuelle Leser und ehem. Abonnenten	€ 160,00
	Passive Ältere	3.051.100	Adressen gesamt	€ 155,00
	Versa Distanzhandel	55.700	aktive Käufer 0-6 Monate (Beate Uhse)	€ 150,00
Gewinnspielteilnehmer		215.500	Gewinnspielteiln. Drogerieartikel	€ 150,00
Große Tageszeitung		2.155.000	Werbedatei einer großen Tageszeitung	€ 110,00

CC BY-SA 3.0 Cracked Labs

Beispiele für von AZ Direkt/Bertelsmann im Online-Katalog angebotene Adressen (11/2014)



Zuverlässigkeit, mit der sich **persönliche Eigenschaften** aus durchschnittlich **170 Facebook-Likes** ablesen lassen

Ethnischer
Hintergrund



95 %

Geschlecht



93 %

Sexuelle
Orientierung



88 %

Politische
Einstellung



85 %

Religion



82 %

Beziehungs-
status



67 %

Drogen-
konsum



65 %

Quelle: www.crackedlabs.org; AK/ÖGB-Darstellung.

Arbeit&Wirtschaft 7/2015

ÖGB-VERLAG/APA-AUFTRAGSGRAFIK

Einige aktuelle „Ereignisse“

- **AntiVirenhersteller AVG** verkauft seine gesammelten Nutzerdaten, um weiterhin Gratis-Software anzubieten
 - Werbe-Kennung des Geräts
 - Surfverlauf
 - Suchverlauf
 - Anonymisiert ???

Einige aktuelle „Ereignisse“

- **Windows 10** wird automatisch auf den Computer geladen, ohne dass der Anwender gefragt wird.
- Wegen der grossen Datenmenge (3 - 6 GB) fallen möglicherweise hohe Online-Kosten an.

Einige aktuelle „Ereignisse“

- **Update des iPhone-Betriebssystems** führt zu gravierenden Softwareproblemen:
 - Keine Verbindung zu Mail-Servern
 - VPN geht nicht mehr
 - Aufladen des Akkus geht teilweise nicht mehr
 - ...
- Updates sind aber wichtig, um gegen Angriffe „gewappnet“ zu sein

Einige aktuelle „Ereignisse“

- **Facebook** fällt stundenlang aus
- **Skype** fällt stundenlang aus
-

Nichts zu verbergen?

- Nichts zu verbergen haben, bedeutet nicht, allen alles zu zeigen
- Überwachung verletzt **Menschenwürde** und **Menschenrechte**
- Wir ändern unser Verhalten, wenn wir davon ausgehen, überwacht zu werden
- Schränkt unser demokratisches, politisches Handeln ein
- Auch wenn wir nichts Illegales tun, können wir plötzlich in Verdacht geraten durch die Kombination verschiedener Daten = **Profiling**



Es geht nicht um Datenschutz,
sondern um Menschenschutz.

(Jacob Appelbaum)



Hinweis:

Jacob Appelbaum beim
Festival elevate am
25.10.2015, ab 16 Uhr
im Dom im Berg



Probleme

- **Personalisierte Werbung** – aber das kann ja auch ganz praktisch sein
- Daten über **Krankheiten** können von **Versicherungen** benutzt werden, um **Prämien** zu erhöhen
- Suchst du nach einer **Schuldnerberatung**, fordert möglicherweise deine Bank deinen Kredit zurück.
- Was **illegal** ist kann sich ändern, frühere Daten können **gegen** dich verwendet werden



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** ?



Was tun?

Mögliche Reaktionen auf die täglich neuen
Horormeldungen über Überwachung und Datenklau:

- **Ist mir egal**, ich habe nichts zu verbergen
- **Resignation** – ich kann eh nix machen
- **Paranoia** und Wunsch nach absoluter Anonymität / Komplettverweigerung



Was können wir tun ?

- Es gibt **keine „isolierte“ Maßnahme** – außer als Einsiedler in den Busch zu kehren –die etwas gegen diese Möglichkeit der Überwachung ausrichten könnte.
- Es braucht eine **Fülle von Maßnahmen** – gesellschaftlich wie technologisch –um Europas Abhängigkeit zu verringern.
- Vor allem aber braucht es dafür:

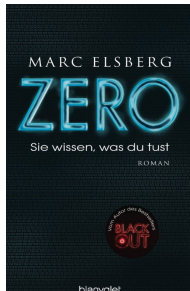
Das **Bewusstsein** dieser Sachverhalte und die daraus resultierenden Konsequenzen für unsere Gesellschaft

(Josef Pichlmeier, Security Day, FH St. Pölten 2014)



10 Schritte zur digitalen Selbstverteidigung

Marc Elsberg: Zero



<http://zero-das-buch.de/selbstverteidigungstipps.php>



Selbstverteidigungstipps Elsberg (1)

Surfen Sie wenn möglich nur auf gesicherten Seiten, deren Adresszeile mit „https“ anfangen.

- Vor allem, wenn es um kritische und persönliche Daten (Bankverbindung, Adresse, etc.) geht.
- „Https“ steht für sicheres Hypertext-Übertragungsprotokoll und dient dazu, Daten abhörsicher zu übertragen.



Selbstverteidigungstipps Elsberg (2)

Deaktivieren Sie Cookies.

- Cookies sind kurze Datenbank- oder Verzeichniseinträge zum Informationsaustausch zwischen Computerprogrammen. Viele Webseiten tauschen sich untereinander über ihre Besucher aus. Das passiert u.a. über die Cookies, die von Werbebannern auf Ihren Rechner gelegt werden.
- Richten Sie Ihren Browser so ein, dass er Cookies (http-Cookie, Flash-Cookie, Web-Storage etc.) nach jeder Sitzung löscht.



Selbstverteidigungstipps Elsberg (3)

Verwenden Sie keine Clouds.

- Speichern Sie Ihre Daten lieber auf Datenträgern, Ihrer Festplatte oder Ihrem Heimserver.
- Wenn Sie Ihre Daten in einer Cloud oder in einem Online-Backup speichern, sollten diese verschlüsselt sein.



Selbstverteidigungstipps Elsberg (4)

Denken Sie sich immer neue Passwörter aus.

- Und zwar solche, die Sie sich zwar merken können, aber nicht einfach zu erraten sind.
- Verwenden Sie dabei Zahlen, Groß/Kleinschreibung sowie Sonderzeichen (z.B. %, &, *, /).



Selbstverteidigungstipps Elsberg (5)

Installieren Sie ein E-Mail-Programm auf Ihrem Computer.

- Indem Sie Ihre E-Mails auf Ihrem Rechner schreiben, verhindern Sie, dass jedes Wort, das Sie schreiben, zeitgleich online ist.
- Erst wenn Sie Ihre Nachricht versenden und/oder zwischenspeichern, geht diese ins Internet.



Selbstverteidigungstipps Elsberg (6)

Verschlüsseln Sie Ihre E-Mails und Ihre SMS.

- Dafür gibt es heute einfache Programme. Nichtdestotrotz hilft es nicht viel weiter, wenn Sie Ihre E-Mail verschlüsseln und der E-Mail-Empfänger keine Verschlüsselung verwendet.
- Außerdem werden nur der Inhalt und die Anhänge codiert. d.h., dass ein potenzieller, unerwünschter Mitleser weiß, wem Sie wann eine E-Mail geschrieben haben.



Selbstverteidigungstipps Elsberg (7)

Chatten Sie nicht über zentrale Dienste,
sondern benutzen Sie freie Anbieter –
auf Ihrem PC und auch auf Ihrem Mobilgerät,
am besten mit OTR-Verschlüsselung.



Selbstverteidigungstipps Elsberg (8)

- **Schalten Sie auf Ihrem Smartphone die Ortungsfunktion aus** ebenso auf den verschiedenen Onlineplattformen, die sie besuchen.
- Dasselbe gilt für die Gesichtserkennungsfunktion.



Selbstverteidigungstipps Elsberg (9)

- **Nutzen Sie möglichst wenige kostenfreie Dienste.**
- Machen Sie sich stets bewusst, dass Sie hier in einer anderen Währung bezahlen: Mit Ihren Daten und Ihrer Freiheit.



Selbstverteidigungstipps Elsberg (10)

- **Vermeiden Sie, wenn möglich, regelmäßige Zahlungen** mittels Bankkarten, Bahncard oder sogenannter Rabattkarten, um zu verhindern, dass Ihre Konsum- und Reisegewohnheiten gespeichert werden.



STOA Study on "Mass surveillance of IT Users"

Studie für das EU Parlament

- **STOA: Science and Technology Options Assessment**



- verfasst von Experten der Beraterfirmen Tecnia und Cap Gemini
- <http://www.europarl.europa.eu/stoa/>
- The first part of the study concludes with a list of security solutions to help citizens protect themselves from illicit mass surveillance activities. It emphasizes that the use of end to end encryption over the internet is a good solution if the two communication 'end-points' are secured, if there are no flaws or backdoor in the software and protocols used, and finally, if the configuration parameters are set correctly.
- The second part of the study concludes with the proposal of several policy options with different levels of public intervention and technological disruption.
- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



STOA Study on "Mass surveillance of IT Users" - Links

STOA Study on "Mass surveillance of IT Users" - Part 1

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409_REV1_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409_REV1_EN.pdf)

STOA Study on "Mass surveillance of IT Users" - Part 2

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU\(2015\)527410_REV1_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf)

Short video-clip on Part 1

- <https://www.youtube.com/watch?v=i3-ftrJFuc4>

Short video-clip on Part 2

- <https://www.youtube.com/watch?v=cl5UyUnTck0>

STOA options brief

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU\(2015\)527410\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410(ANN2)_EN.pdf)

How to Protect your Privacy on the Internet

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



Software-Empfehlungen (STOA Studie 2015)

Disk Encryption

- DiskCryptor
- tcNext
- CipherShed
- FileVault
- BitLocker
- GnuPG

Encryption of Communication Channel

- HTTPS Everywhere

How to Protect your Privacy on the Internet

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



Software-Empfehlungen (STOA Studie 2015)

Email

- Prism
- BitMessage
- Sendinc
- Enigmail
- Mailvelope
- GnuPG
- Startmail
- GPG Tools
- iPGmail
- And You And I
- oPenGP

Voice (and Video) Communication

- Cellcrypt
- Celltrust
- OSTN
- Omnisec
- Seecrypt
- SilentPhone
- Redphone
- Jitsi
- Tox

How to Protect your Privacy on the Internet

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



Software-Empfehlungen (STOA Studie 2015)

Web Browsing

- TOR
- I2P
- Blur
- Disconnect
- NoScript
- Orweb
- Onion Browser

Chat / IM

- TorChat
- Pidgin
- Adium
- MiOTR
- Cryptocat
- Jitsi
- ChatSecure

How to Protect your Privacy on the Internet

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



Software-Empfehlungen (STOA Studie 2015)

Search Engines

- DuckDuckGo
- Ixquick
- StartPage

Operating Systems

- Qube OS
- OpenBSD
- TAILS

How to Protect your Privacy on the Internet

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



Software-Empfehlungen (STOA Studie 2015)

- Install perimeter security – firewalls and antivirus
- Apply software and security updates regularly – setup automatic updates if possible
- Use strong passwords – more than 8 chars using a mix of alphanumeric and special symbols
- Do not open unknown mail attachments and do not follow suspicious web links
- NEVER reveal your passwords or bank details to third parties

How to Protect your Privacy on the Internet

- [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU\(2015\)527409\(ANN2\)_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN2)_EN.pdf)



PRISM BREAK

Sehr ausführliche Liste an empfohlener Software
gegen Massenüberwachung:

<https://prism-break.org/de/>



50 Tipps in 5 Stufen



<http://www.digital-selfdefense.com/>

1.10.2015

URANIA 2015

CryptoParty.at/Graz



Verteidigungsstufe I :

Die 10 grundlegenden Dinge, die Sie tun sollten

- 1) Löschen Sie Cookies und das Webprotokoll
- 2) Verwenden Sie Google-Datenschutz-Werkzeuge,
aber vermeiden Sie es zu häufig Google zu benutzen
- 3) Diese Informationen gehören nicht in Soziale Netze
- 4) Verwenden Sie mehrere Web-Browser
- 5) Verwenden Sie Pseudonyme für Ihr privates Ich
- 6) Grundlegende Sicherheit bei facebook
- 7) Grundlegende mobile Sicherheit
- 8) Schützen Sie Ihre Emails
- 9) Verwenden und merken Sie sich sichere Passwörter
- 10) Kaufen Sie sicher mit Ihrer Kreditkarte ein



Verteidigungsstufe II :

Die nächsten 10 Dinge, die Sie tun sollten

- 11) Verwenden Sie Blocking-Werkzeuge in Ihrem Web-Browser
- 12) Verwenden Sie privates Surfen
- 13) Verwenden Sie Firefox zum Porno-Surfen
- 14) Sperren Sie Social Widgets
- 15) Fortgeschrittene Sicherheit bei facebook
- 16) Sicherheit bei mobilen Apps
- 17) Verbergen Sie Ihre IP-Adresse mit einem VPN
- 18) Säubern Sie Ihre Online-Reputation
- 19) Beugen Sie Identitätsdiebstahl vor
- 20) Säubern Sie Ihren Rechner



Verteidigungsstufe III :

Die nächsten 10 Dinge, die Sie tun sollten

- 21) Sichern Sie Ihre Fotos
- 22) Verschlüsseln Sie Ihre Korrespondenz – die Grundlagen
- 23) Surfen Sie mit Verschlüsselung
- 24) Verschlüsseln Sie Ihre Chats
- 25) Verschlüsseln Sie Ihre Beiträge auf Sozialen Netzwerken
- 26) Mobile Sicherheit für Fortgeschrittene
- 27) Verschlüsseln Sie Ihre Festplatten
- 28) Entfernen Sie Ihren digitalen Spuren
- 29) Manchmal hilft nur der Hammer
- 30) Löschen Sie Ihr facebook-Profil



Verteidigungsstufe IV :

Zehn Dinge, um Spionen das Leben schwer zu machen

- 31) Meiden Sie US-Dienstleister und US-Software
- 32) Verschlüsseln Sie Ihre Daten im Ruhezustand
- 33) Verschlüsseln Sie Ihre Kommunikation von A bis Z
- 34) Nichtamerikanische Email-Dienste
- 35) Nichtamerikanische Suchmaschinen
- 36) Nichtamerikanische Hosting-Anbieter und Cloud-Dienste
- 37) Das Trio: Verwenden Sie VPNs und Anonymisierung plus Verschlüsselung
- 38) Vergängliche Alternativen zu E-Mail
- 39) Verzichten Sie auf Ihr Smartphone
- 40) Verzichten Sie auf Kreditkarten



Verteidigungsstufe V :

Der Rest

- 41) Entfernen Sie die Kennung Ihres Handys
- 42) Verwenden Sie Einwegtelefonnummern
- 43) Verwenden Sie Fingerabdruck-Authentifizierung und Passwörter vom USB-Stick
- 44) Überprüfen Sie Ihren Browser-Fingerabdruck
- 45) So begehen Sie Selbstmord auf Twitter
- 46) Säubern Sie Ihr YouTube-Konto
- 47) Das ist nicht cool – Medienkompetenz für Kinder
- 48) Sollte man Passwörter wiederverwenden?
- 49) Gönnen Sie sich eine Pause von der digitalen Welt
- 50) Bereiten Sie Ihr digitales Erbe vor



Danke fürs Zuhören !

Gibt es Fragen ?

www.cryptoparty.at/graz

