# The world’s most secure text messaging app: surespot!


Ich habe heute Threema von meinem Smartphone geworfen und stattdessen Surespot installiert.
*surespot is a secure mobile messaging app that uses exceptional end-to-end encryption for every text, image and voice message returning your right to privacy*
*– surespot is not associated with your phone number or email*
*– you can delete your messages from the receiving device*
*– send voice messages when your hands or eyes are too busy to text*
*– multiple identities on a single device to keep matters separated*
*– free messenger with no advertising and totally open source*
*– your identity is portable so you can transfer your secure conversations to other devices*
*– uses 256 bit AES-GCM encryption using keys created with 521 bit ECDH**
** this means only you and the receiver can decrypt surespot messages*

Wer mit mir so Kontakt aufnehmen will: Mein Name ist Burks…

# Facebook kauft WhatsApp

Da wächst zusammen was zusammen gehört – die Datenkrake und das Scheunentor.

---

# Vorratsdatenspeicherung kommt, ganz gleich, was die Gerichte entscheiden

Heise (via Halina Wawzyniak): „Auch wenn der Europäische Gerichtshof (EuGH) im Frühjahr die EU-Richtlinie kippen sollte, will Bundesjustizminister Heiko Maas einen Gesetzentwurf zum verdachtsunabhängigen Sammeln von Verbindungs- und eventuell auch Standortdaten vorlegen."

Man könnte dazu ein Zitat abwandeln:
*Das genau ist es, was nicht nur zwei Richter in ihren abweichenden Voten, sondern auch ~~Ökonomen~~ Sicherheitspolitiker für gerichtliche Hybris halten: der Versuch, ~~das Krisenhandwerk~~ die anlasslose Totalüberwachung ~~von Notenbankern~~ des großen Bruders mit dem Mitteln des Rechts zu gängeln.*

---

# Verschlüsselung – nein danke!

Netzpolitik.org versucht, Abgeordneten oder einer Behörde eine verschlüsselte Mail zu senden. Man kann raten, was dabei

herauskommt.

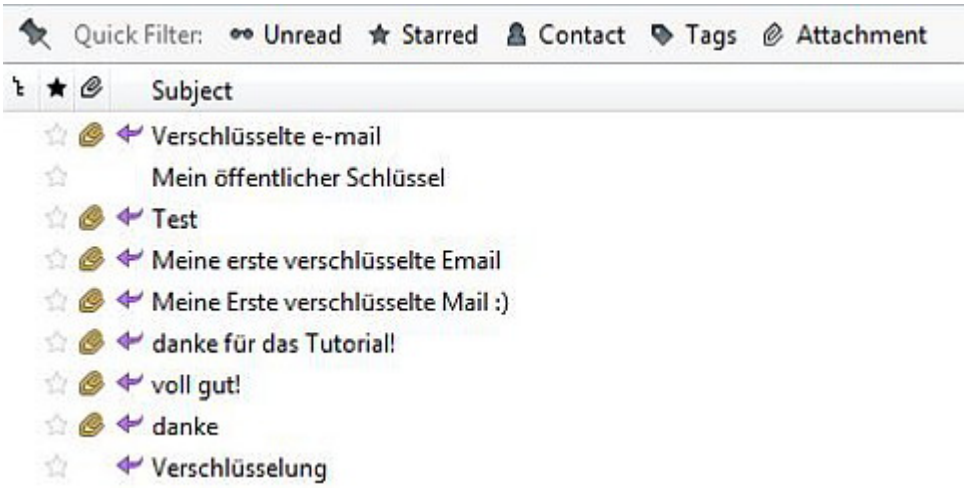
Ich hatte den Versuch schon vor sechs Jahren einmal gestartet, vgl. Telepolis vom 04.02.2008 „Security by obscurity im Bundestag“.

Wie man sieht, hat sich seitdem nichts geändert. Die wissen noch nicht mal, wovon die Rede ist.

Das bestätigte schon die FAZ am 10.08.2013. Kurz zuvor hatte ich in Telepolis (08.07.2013) das Thema wieder einmal angestoßen: „Verschlüsselung – nein danke!“. Die Medien sind eben auch nicht besser.

---

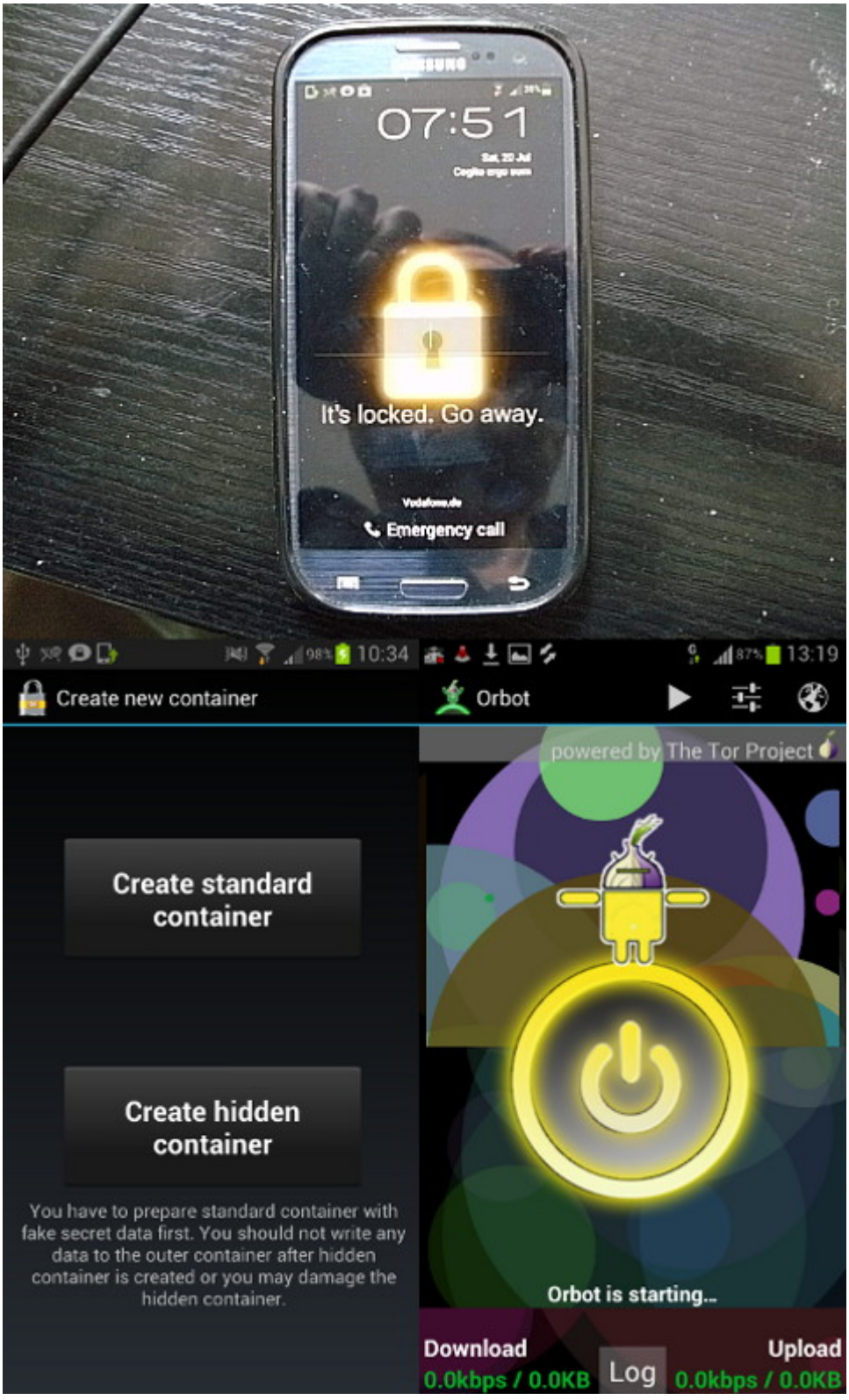
# Usability ist gefragt




Der Posteingang des Vereins *German Privacy Fund e.V.* wegen dieses Tutorials.

---

# Dem Redakteur ist Android-Verschlüsseln zu schwör?




„Den meisten dürfte der passwortgeschützte Sperrbildschirm reichen“, lese ich in den Mainstream-Medien über die Android-

Verschlüsselung.

Journalisten sollten nicht vermuten, ohne jedwede empirische Grundlage, und schon gar nicht suggestiv herumfabulieren. Dem Redakteur ist nichts zu schwör?

Mir reicht der passwortgeschützte Sperrbildschirm nicht! Das musste jetzt mal gesagt werden. Und ich bin ein normaler Bürger!

---

# Tor, the bad guys and the good guys

Heise: „Forscher von der schwedischen Karlstad University sind bei einer systematischen Analyse des Tor-Netzwerks (PDF) auf 20 Exit-Nodes gestoßen, die verschlüsselte Verbindungen angreifen.“
*Several hundred Tor exit relays together push more than 1 GiB/s of network traffic. However, it is easy for exit relays to snoop and tamper with anonymised network traffic and as all relays are run by independent volunteers, not all of them are innocuous. (…) To reduce the attack surface users are exposed to, we further discuss the design and implementation of a browser extension patch which fetches and compares suspicious X.509 certificates over independent Tor circuits. Our work makes it possible to continuously monitor Tor exit relays.*

---

# The Day We Fight Back

---

# Kein Wegfall der Geschäftsgrundlage bei der Vorratsdatenspeicherung

Stefan Ansgar Strewe (SPD Sachsen) kommentiert bei Heise das Gutachten des Generalanwalts beim Europäischen Gerichtshof (EuGH) vom 12.12.2014: „Der Wegfall der Geschäftsgrundlage bei der Vorratsdatenspeicherung“.

Man denkt beim flüchtigen Lesen, es gäbe auch bei der SPD vereinzelt Leute, die denken können. Dann aber liest man die Leserkommentare:
*Der Gutachter hat gerade nicht empfohlen, die Vorratsdatenspeicherung zu kippen, sondern lediglich eine zeitnahe Überarbeitung der Richtlinie einzufordern, welche die bemängelten Punkte behebt. Dieser Gastkommentar trägt leider nur zur Verdummung der Leser bei, weil diese über wesentliche Tatsachen getäuscht werden.*

Man lehnt sich beruhigt zurück: Also doch die SPD, wie man sie kennt.

---

# Commercial Onion Routing Privacy Service

Eine interessante Frage aus der Tor-Mailingsliste: Offenbar gibt es einen „Anonymisierungs"-Dienst, der von (früheren?) NSA-Mitarbeitern betrieben wird. „It seems a Commercial Onion Routing Privacy Service for US enterprises and Government Agencies."

Der Dienst heisst NetAbstraction: „NetAbstraction is a Cloud-based service that obscures and varies your network pathways, while protecting your identity and your systems."

Hinter der Firma steckt eine andere – Cutting Edge CA (vgl. hier).

Nun schauen wir uns Barbara Hunt an, die bei beiden Firmen eine Chefin („Senior Leader") ist:
*My last position in the Intelligence Community (2008-2012) was as Director of Capabilities for Tailored Access Operations at the National Security Agency. As a member of NSA/TAO's senior leadership team, was responsible for end-to-end development and capabilities delivery for a large scale computer network exploitation effort.*

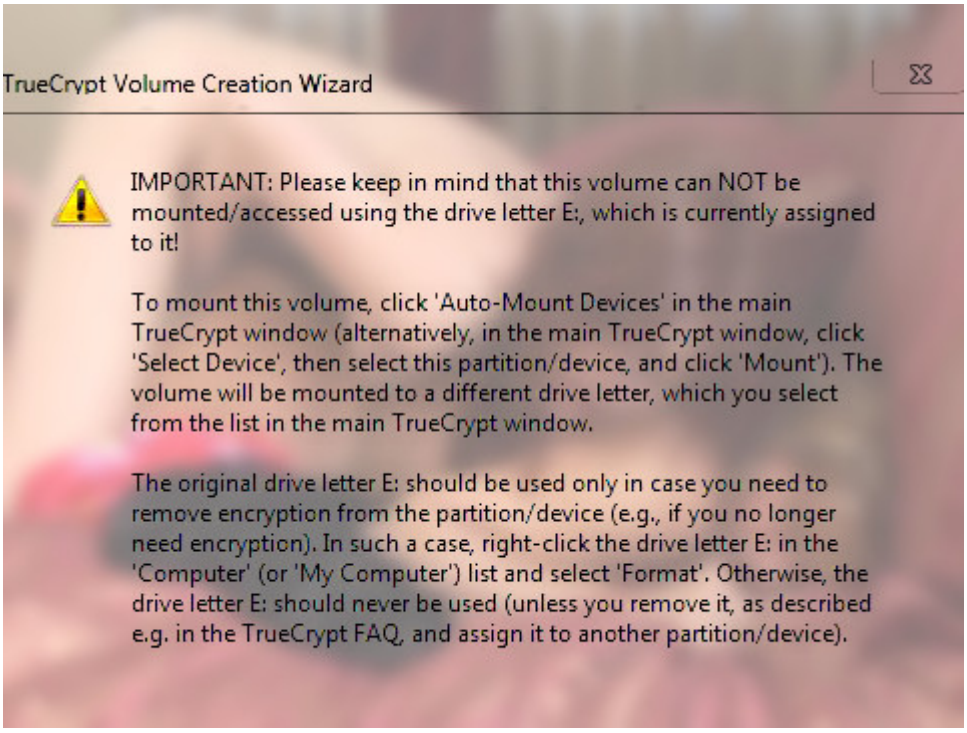
Und dann ist da noch Steven W. Bay, Chief Strategist:
*Mr. Bay is a retired CIA Senior Operations Officer with 24 years of experience conducting a full range of intelligence operations for the National Clandestine Service, including operational innovation and implementation of telecommunications and information technology programs. Mr. Bay also brings extensive experience in alternate persona research, planning, acquisition, and use."*

Frage in der Mailingliste: „Former spy, experts on COMINT and SIGINT, running an online privacy service?"

Na klar. Denen würde ich sofort meinen Daten anvertrauen. Muahahahaha.

---

# Terroristisches Material und Pornografie in versteckten Containern glaubhaft abstreiten




Heise: „Die Regierung dürfe Laptops, Kameras und ähnliche Geräte von Reisenden durchsuchen. (…) Richter Korman begründete seine Entscheidung (PDF) damit, dass im 21. Jahrhundert die gefährlichste Schmuggelware oft in Laptops und anderen elektronischen Geräten enthalten sei – zum Beispiel terroristisches Material und Pornografie.“

Im Original: „“In the 21st century, the most dangerous

contraband is often contained in laptop computers or other electronic devices, not on paper. This includes terrorist materials and despicable images of child pornography.“

Ein Grund mehr, dass sich auch Nicht-Geeks und Nicht-Nerds mit dem Feature „Hidden Volume“ von Truecrypt beschäftigen.

Deutsche Anleitungen gibt es bei Christian Sickendieck, bei Wikipedia kann man etwas über das „Konzept der glaubhaften Abstreitbarkeit“ (der Begriff ist natürlich Deutsch des Grauens) lesen, und bei bei Truecrypt gibt es alles auch in Englisch. Über die Details hatten wir uns auch schon hier am 15.07.2013 (vgl. auch die Links in den Kommentaren) unterhalten.

---

# Fast ein Quantum Dingsbums

Wieder einmal wird die Panik-Sau durchs Mainstreammedien-Dorf getrieben. Wenn ich bei der NSA wäre, würde ich es auch so machen: So tun, als wäre ich überall schon „drin“, als könne man gar nichts mehr tun, als wären die Geheimdienste übermachtig und allwissen. Genauso kommen die aktuellen Artikel einher: Bürokraten neigen dazu, selbst dem kleinsten Furz eine geheimnisvolle Abkürzung zu geben,

die einschüchtern soll. Heute haben wir die „Quantumtheory“, „Quantumbot“, „Quantumcopper“ und die „NSA-Abteilung Tailored Access Operations (TAO)“. „The Asshole Open“ würde auch passen. Demnächst nennt die NSA *Remote-Access-Software*, die der Zielperson auf DVD per Fahrradkurier zugeschickt wird („Geile-Titten.exe – sofort installieren!) „einstein.exe“ oder so ähnlich.

Und natürlich geistern wieder die „Trojaner“ überall herum (nein, es waren die Griechen, die im Pferd saßen, *nicht* die Trojaner). Es ist alles wie schon bei der so genannten „Online-Durchsuchung“: Wer sich auskennt, lacht sich kaputt, und wer sich nicht auskennt, ist wie gelähmt und macht gar nichts mehr, weil es angesichts eines solchen übermachtigen Gegners keinen Zweck hat. Genau so ist das gewollt, und alle spielen mit.

Steht in den aktuellen „Enthüllungen“ (es ist alles noch viel schlimmer, als wir uns jemals vorgestellt haben, reloaded und revisited“) überhaupt etwas Neues?

Die TAO kann also angeblich „fast nach Belieben Rechner von Zielpersonen mit Schadsoftware verseuchen.“ Ach ja? Auch Linux? Und wie? Ach so – über das Wie schweigen wir schamhaft, auch wieder wie bei der „Online-Durchsuchung“. Das interessiert ja nicht wirklich. Und „fast“? Fast alle ausser

Burks‘ Rechner oder wie?

*Früher war es für die NSA noch vergleichsweise mühsam, sich Vollzugriff auf den Computer einer Zielperson zu verschaffen. Sie griff dazu auf eine Methode zurück, die auch Cyberkriminelle und Staatshacker aus anderen Ländern einsetzen: Sie verschickten Spam-E-Mails mit Links, die auf virenverseuchte Webseiten führten.*

Normalerweise liest man bei einem derartigen Mupitz nicht weiter. Cookies, Viren, würmer, Trojaner – alles eine Soße.

Wer will da schon die Details wissen.
Vielleicht funktioniert die Methode aber bei Spiegel-Online-Redakteuren, sonst würde die das nicht schreiben. Das hatten wir doch schon: „Cipav.exe is an unknown application – install anyway?“

Lesen wir weiter, wie das Quantum Dingsbums des NSA „funktioniert“:
*Eine Quantum-Attacke funktioniert, grob erklärt, folgendermaßen: Zunächst wird der Internet-Traffic an den Punkten, an denen die NSA oder befreundete Dienste darauf Zugriff haben, nach digitalen Lebenszeichen der Zielperson durchkämmt. Das kann eine bestimmte E-Mail-Adresse sein oder etwa ein Webseiten-Cookie.*

Schon klar. Cookies. Wer erlaubt die denn, außer Spiegel-Online-Reakteuren? Mein digitales Lebenszeichen ist, wie

bekannt, burks@burks.de. Und jetzt?

*…kann sich der interessierte NSA-Analyst von dort aus weiterhangeln: Er kann weitere E-Mail-Adressen oder andere Cookies desselben Nutzers suchen, etwa den von Facebook oder Microsofts Hotmail-Dienst.*

Ach ja. Dann hangelt mal schön. Es geht munter weiter so:
*Statt der eigentlich angeforderten Yahoo-Seite ruft der Browser unbemerkt eine weitere Adresse auf, die von einem NSA-Server stammt.*

Also mein Browser macht „unbemerkt" gar nichts, und wenn doch, würde ich ihn zum Patent anmelden, wegen spontaner Evolution einer künstlichen Intelligenz, die bisher noch unbemerkt in meinen Computern schlummerte. Auch mit dem „Trojaner Olympus" (beim Zeus, was geben die für Namen?) schwurbeln sie einher, dass es nur so kracht: „Wer sich einmal derartigen Zugang zu einem Computer verschafft hat, kann mit dem infiltrierten Gerät nach Belieben verfahren." Wer hätte das gedacht. Aber wie kommt man rein? Spiegel online verweist auf sich selbst: „Die Spione nutzten dazu unter anderem manipulierte Kopien von LinkedIn-Seiten."

Ach. Das kommt von das. Wer die asozialen Netze, wie die Datenkraken heißen müssten, nutzt, der wird dazu erzogen, die Hosen permanent runterzulassen und alle aktive Inhalte zu erlauben. Ich hingegen erlaube gar nix. Viele Websites sind dann nur noch eingeschränkt lesbar. Quod erat demonstrandum. Webdesigner sind die natürlichen Feinde sicherheitsbewusster Surfer. Und das Geschäftsmodell der Mainstream-Medien, das gar

nicht funktionierten würde, verhielten sich die Nutzer so, wie es vernünftig wäre. Bei *Spiegel online* werden munter Cookies gesetzt, man kan sich sogar mit dem Fratzenbuch-Account einloggen, und ohne Javascript bleiben Teile der Website weiß. Das ist so, also würde ein Fleischerladen die Kunden auffordern, vegetarisch zu essen. Pappnasen.

Zu guter Letzt lesen wir ganz unten: „Mitarbeit: Andy Müller-Maguhn“. Dann kann ja nichts mehr schief gehen. Und Tron ist auch ermordet worden, vermutlich von der ~~NDS~~ NSA. Komisch, dass Snowden das nicht erwähnt hat.

---

# How nerdy

Feynsinn sagt das Nötige über den aktuellen CCC-Kongress: „Totale Überwachung also. Ist noch Kuchen da? Und was kommt heute Abend im Fernsehen? So viel zu Gravitation. Relevanz. Relationen. In dieser Parallelwelt gibt man sich also entsetzt über Zustände, die in der wirklich wahren Wirklichkeit gar keine Rolle spielen. How nerdy! Schatz, ich will auch sowas haben!“

---

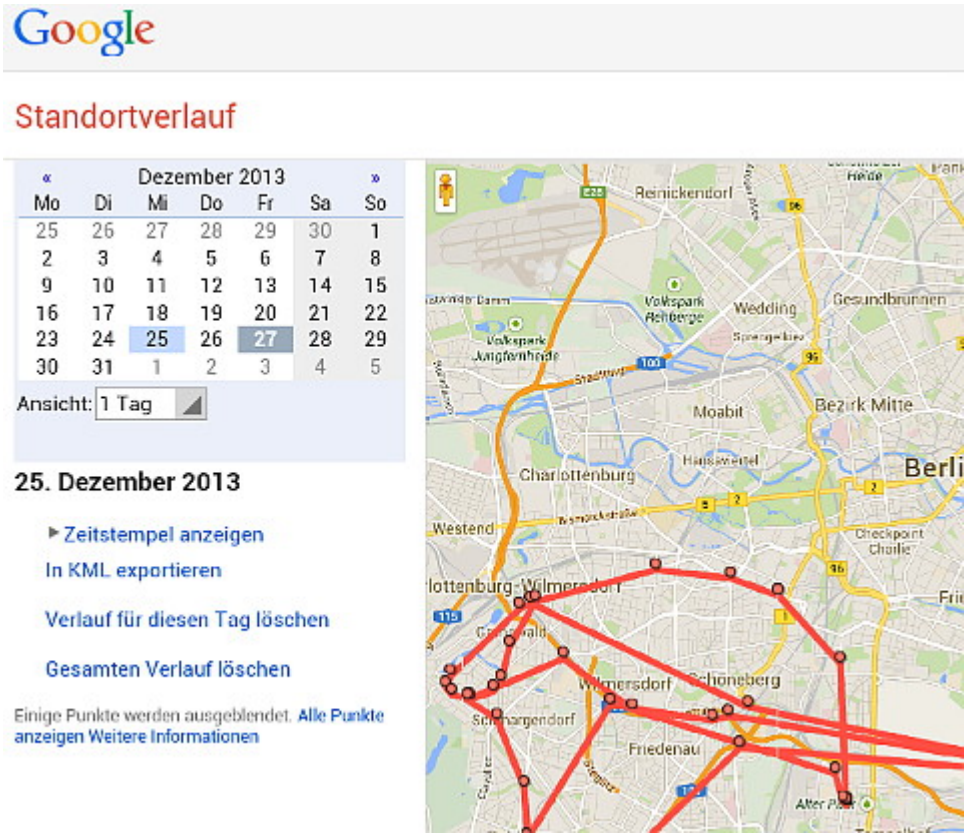
# No backdoors, never ever

Heise berichtet ausführlich über den Vortrag Roger Dingledines (obwohl von Krempl geschrieben: lesenswert wegen vieler interessanter Details): „Eine Vertreterin des Justizministeriums sei auf die Kernentwickler zugekommen und habe davon gesprochen, dass der US-Kongress Washington das

Recht gegeben habe, ‚alles mit Hintertüren zu versehen'. (…) Der nach Berlin ausgewanderte US-Netzaktivist freute sich besonders, dass Tor insgesamt den ‚Snowden-Sommer' überlebt habe. Er spielte damit auf Enthüllungen des NSA-Whistleblowers an, wonach sich der technische US-Geheimdienst an dem Anonymisierungsnetz bislang mehr oder weniger die Zähne ausgebissen habe."

---

# Guerilla, aufgemerkt!

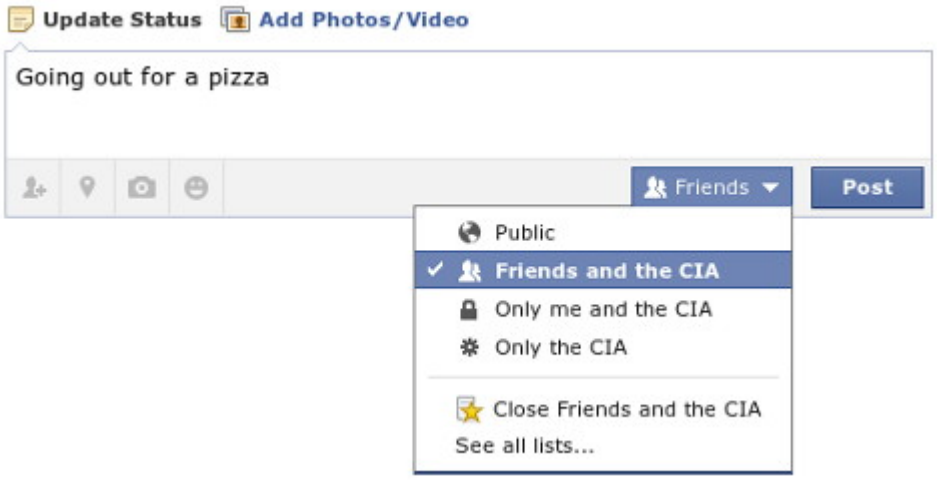



Ich habe neulich, wie schon erwähnt, „Hostages" von Stefan Heym gelesen. Man stelle sich nur vor, wie heute der Widerstand gegen einen faschistischen Staat, eine Militärdiktatur oder nur gegen ein unterdrückerisches Regime aussehen würde, trügen die Guten Smartphones. Die Bösen würden jederzeit wissen, wo sie sind und wer mit wem Kontakt hat. Wer

also eine Revolution plant, sollte darauf verzichten. (Ja, man kann das Feature auch ausstellen – in Maßen.)

---

# Das klingt betrüblich




„Mit dem jüngsten Update verlangt die Facebook-App für Android, dass der Anwender ihr weitreichende Rechte einräumt. So will die App nun auch ‚SMS und MMS lesen' und darüber hinaus ‚Kalendertermine sowie vertrauliche Informationen lesen' und ‚ohne das Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden'". (Heise)

Nutzt Facebook! Eine Milliarde ~~ScheißhausFliegen~~ können nicht irren!

---

# Donate to Support Encryption

# Tools for Journalists


Ich bin erst einmmal skeptisch, wenn ich das lese: *Protecting the digital communications of journalists is now one of the biggest press freedom challenges in the 21st Century.(…) To that end, we're providing you with an easy way to donate to support open-source encryption tools that can better protect the communications of journalists and sources.*

Wer steckt dahinter? Es kann ja jeder so eine Website aufziehen. Empfohlen wurde sie in der Tor-Mailingliste.

*The Freedom of the Press Foundation is dedicated to helping support and defend public-interest journalism focused on exposing mismanagement, corruption, and law-breaking in government. (…) You can go here to see a description of the organizations we are currently crowd-funding donations for.*

Auch das hier klingt gut: „How to Protect Your Privacy in the Age of NSA Surveillance„.

Das deutsche Wikipedia hat gar keinen Eintrag über die *Freedom of the Press Foundation*. Wenn aber die EFF unterstützt, kann man der Sache vertrauen.

In Deutschland müsste man so etwas vereinsmeierisch aufziehen. Unser Verein German Privacy Fund ist ja so gedacht, da die alte *German Privacy Foundation sich aufgelöst hat.*

---

# Protocols and procedures

„If one believes Snowden, our algorithms are OK, but our protocols and procedures are questionable.“ (Bill Frantz, cryptography – The Cryptography and Cryptography Policy Mailing List)

---

# Interview mit Snodwden: „They will make mistakes“

…in der Washington Post.
*His colleagues were often „astonished to learn we are collecting more in the United States on Americans than we are on Russians in Russia,“ he said. Many of them were troubled, he said, and several said they did not want to know any more.*

Das ist bei deutschen Geheimdiensten (außer dem Inlandsgeheimdienst) natürlich gaaaaaaanz anders.

Hier noch ein Kommentar aus dem Heise-Forum:
*‚Er habe der Gesellschaft eine Chance geben wollen, selbst herauszufinden, ob sie sich ändern wolle, sagte Snowden weiter.‘*
*Die Gesellschaft will sich nicht ändern, wie das Desinteresse*

*der Massen sowie die Bundestagswahl gezeigt hat.“*

---

# Secret contract tied NSA and security industry pioneer

Reuters, Techcrunch.com, Arstechnica u.a.: Die NSA hat dem IT Security Branchenprimus RSA $10 Millionen bezahlt, um schwache Verschlüsselung zu promoten.
*Reuters later reported that RSA became the most important distributor of that formula by rolling it into a software tool called Bsafe that is used to enhance security in personal computers and many other products. (…) The RSA deal shows one way the NSA carried out what Snowden’s documents describe as a key strategy for enhancing surveillance: the systematic erosion of security tools.*