

#PrismBreak

@calibanatspace
(Jochen Bachmann)

Wieso #PrismBreak?

Wieso #PrismBreak?

- Veröffentlichungen zu Prism und Tempora
- Kein Vertrauen mehr in Webdienste
- Weiter Kopf in Sand oder eine Lösung suchen?
- Lösungen die nicht zu sehr „schmerzen“

Wieso #PrismBreak?



Lavabit

My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund [here](#).

Screenshot lavabit.com, 08.08.2013

Was soll ausgetauscht werden?

- Windows
- Google (Search, Mail, Drive, Calender, Contacts)
- Dropbox

Was soll ausgetauscht werden?

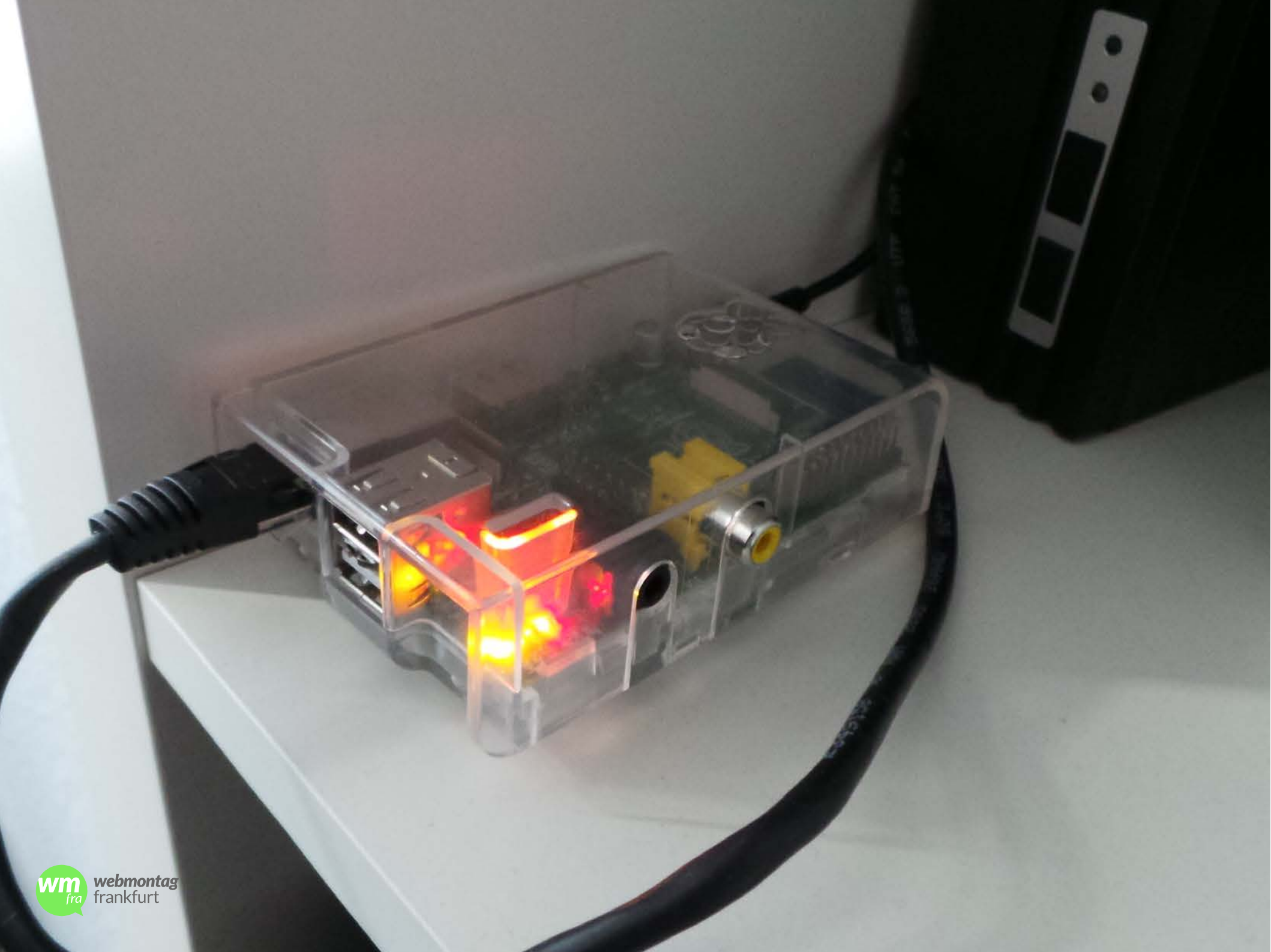
- Chrome
- Unverschlüsselte Mails
- Unverschlüsselte Chats (Skype, Hangouts,...)
- Stock Android / Hersteller Versionen
- Evernote
- Picasaweb

Ausgangsbasis

Ausgangsbasis

- Synology-NAS
- Raspberry Pi
- prism-break.org
















Opt out of global data surveillance programs like PRISM, XKeyscore and Tempora.

Stop governments from spying on you by encrypting your communications and ending your reliance on proprietary services.

Operating system

Proprietary	Free alternatives	Notes
 Apple OS X  Google Chrome OS  Microsoft Windows	<div style="text-align: right;"><input type="checkbox"/> show all</div> <p>GNU/LINUX</p> <div data-bbox="702 438 1330 510">  Debian Strictly free, ethical GNU/Linux distribution. most stable </div> <div data-bbox="702 550 1404 622">  Fedora Fast, stable and powerful GNU/Linux distribution. most popular </div> <div data-bbox="702 654 1564 726">  Gentoo GNU/Linux distribution about choice, control and security. most advanced features </div> <div data-bbox="702 758 1627 829">  Linux Mint Debian Edition Comfortable and easy-to-use GNU/Linux distribution based on Debian. easiest to use </div> <p>BSD</p> <div data-bbox="702 901 1255 973">  OpenBSD A secure BSD operating system. most paranoid </div>	<p>Apple, Google, and Microsoft to safeguard your personal information.</p> <p>Debian has a long tradition of an ethical manifesto. Strict inclusions in the main repositories.</p> <p>Gentoo describes itself as a machine allowing near-unlimited customization.</p> <p>Linux Mint Debian Edition is a Linux distribution based on Debian.</p> <p>Canonical's Ubuntu is not the default GNU/Linux distribution for several reasons.</p>

Live CDs & VM images

Free alternatives	Notes
 Liberté Linux Live CD/USB based on Hardened Gentoo designed as a communication aid in hostile environments.	<p>A live distribution like Tails have to do is create a bootable CD/USB preconfigured for you.</p>
 Tails Live CD/USB based on Debian and Tor aimed at preserving your privacy and anonymity.	<p>A virtual machine (VM) image of Tails can be installed in VirtualBox for whatever reason, including OS X.</p>
 Whonix VM-friendly OS based on Debian and Tor focused on anonymity, privacy and security.	

Umsetzung

Umsetzung

- Windows durch Linux ersetzen
 - Asus Zenbook
 - UEFI-Hölle
 - RAID „deinstallieren“
 - Gparted gutes Hilfsmittel

Umsetzung

- Windows durch Linux ersetzen
 - Linux Mint (Cinnamon)
 - Linux Mint (MATE)
 - Drucker, Scanner, Android ohne Probleme erkannt

Umsetzung

- Google Mail ersetzen
 - Mailadresse
 - Mailsammeldienst
 - Mail-Frontend

Umsetzung

- Google Mail ersetzen
 - Raspberry Pi mit Debian
 - Dovecot als IMAP-Server
 - Konfiguration von Dovecot einfach gehalten
 - getmail zum Einsammeln von Mails

Umsetzung

- Mails verschlüsseln
 - Thunderbird mit Enigmail
 - Public/Private Key für jeden Mailaccount
 - Public-Keys veröffentlicht
 - K-9 Mail mit AGP für Android

Umsetzung

- Chat verschlüsseln
 - Pidgin mit OTR (Off the record)
 - Jabber-Account bei jabber.de angelegt

Umsetzung

- Google Calendar/Contacts ersetzen
 - Owncloud auf Synology
 - Sync-Apps für Android benötigt
 - CalDav-Sync
 - CardDav-Sync
 - Thunderbirds mit Add-Ons
 - Google Contacts
 - Lightning

Umsetzung

- Google Drive/Dropbox ersetzen
 - Synology CloudStation
 - BitTorrent Sync auf Raspberry Pi

Umsetzung

- Chrome durch Firefox ersetzt
 - Passwörter-Sync deaktiviert
 - Sync per 1Password über CloudStation
- Evernote
 - Einfach Lösung per Texteditor und CloudStation
- Picasaweb
 - Synology Photo Station

Umsetzung

- Websuche
 - startpage.com
 - duckduckgo.com

Umsetzung

- Stock-/Hersteller Android austauschen
 - Cyanogenmod
 - Privacy Guard
 - Getestet mit
 - Nexus 4
 - Nexus 7
 - Samsung S3
 - Geräte verschlüsseln

Umsetzung

- Foursquare deinstalliert

Umsetzung

- Windows durch Linux ersetzen ✓
- Google Mail ersetzen ✓
- Mails verschlüsseln ✓
- Chat verschlüsseln ✓
- Google Calendar/
Contacts ersetzen ✓
- Google Drive/
Dropbox ersetzen ✓
- Chrome durch Firefox ersetzt ✓
- Evernote und Picasaweb ✓
- Websuche ✓
- Stock-/Hersteller
Android austauschen ✓
- Foursquare deinstalliert ✓

Was fehlt noch?

Was fehlt noch?

- Zweites Notebook auf Linux umstellen
- Richtigen Mailserver aufsetzen?
- Mehr Leute aus meinem Umfeld zur Verschlüsselung überreden
- RSS Reader selbst hosten?
- Sourcecode Repositories selbst hosten?

Was fehlt noch?

- Eigener Jabber-Server?
- Überprüfen, mit wem Apps „kommunizieren“
- Video-Chat (Skype, Hangout)

Was fehlt nicht!

Was fehlt nicht!

- Twitter
- Facebook
- Google+
- App.net

Und jetzt?

Und jetzt?

- Fühle ich mich besser?
- Sehr zeitaufwändig
- Man lernt einiges dabei
- Es sollte out-of-the-box angeboten werden
- Es fehlt bestimmt noch einiges...

Was könnt Ihr tun?

Was könnt Ihr tun?

- Krypto-Parties
 - www.cryptoparty.in/frankfurt

Danke

Präsentation und Links:
wmfra.de/prisymbreak

Links (1/4)

- <https://prism-break.org/>
- <https://eschnou.com/entry/implementing-prism-break-62-25013.html>
- <http://yellowshoes.de/tag/prismbreak/>
- <http://gparted.sourceforge.net/>
- <http://www.linuxmint.com/>

Links (2/4)

- <http://dovecot.org/>
- <http://pyropus.ca/software/getmail/>
- <http://www.enigmail.net/>
- <http://hogi.sakura.ne.jp/en/gmcont/gmcont.rhtml>
- <https://www.mozilla.org/projects/calendar/lightning/>

Links (3/4)

- <http://owncloud.org/>
- <http://labs.bittorrent.com/experiments/sync.html>
- <https://play.google.com/store/apps/details?id=com.fsck.k9>
- <https://play.google.com/store/apps/details?id=org.thialfihar.android.apg>

Links (4/4)

- <http://pidgin.im/>
- <http://www.cypherpunks.ca/otr/>
- <http://www.cyanogenmod.org/>