

# Freenet / Hyphanet nutzen

## Technische Lösungen für freie Kommunikation im Internet

Dr. Arne Babenhauserheide

*<2015-02-10 Di>*

# Inhalt

Warum?

Technik

Lösungen

Eine Vision

*I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?' –Mike Godwin, Electronic Frontier Foundation, [“Fear of Freedom”](#) (1995)*

# Analoge Kommunikation

## Vertraulich



---

Im kleinen Rahmen  
Direkter Kontakt

# Analoge Kommunikation

## Vertraulich



---

Im kleinen Rahmen  
Direkter Kontakt

## Offiziell



---

Selbstzensur  
Fremdbestimmt

# Analoge Kommunikation

## Vertraulich



---

Im kleinen Rahmen  
Direkter Kontakt

## Offiziell



---

Selbstzensur  
Fremdbestimmt

## Pseudonym



---

Stetig auf der Hut  
Quellenschutz!

# Analoge Kommunikation

Im Überwachten  
Netz

Offiziell



---

Selbstzensur  
Fremdbestimmt

# Weckruf

*“There is now no shield from forced exposure. . . The foundation of Groklaw is over. . . the Internet is over” –Groklaw, Forced Exposure (2013-08-20)*

# Zusammenfassung

## Warum?

- Im Überwachten Netz wird Selbstzensur zur Pflicht.
- Zweite Chance dank Snowden.

## Lösungen



## Technik

## Eine Vision

# Vertrauliche Kommunikation in Hyphanet

## Vertraulich



# Vertrauliche Kommunikation in Hyphanet

## Vertraulich



## Darknet Nachrichten

- Infrastruktur
- Unsichtbar
- Mit Bekannten

# Vertrauliche Kommunikation in Hyphanet

## Vertraulich



## Darknet Nachrichten

- Infrastruktur
- Unsichtbar
- Mit Bekannten

## Freemail

- Perfect Forward Security
- Web of Trust

# Pseudonyme Kommunikation in Hyphanet



# Pseudonyme Kommunikation in Hyphanet

## Klassisch

- - Dateien/Ordner
- Webseiten
- E-Mail
- Blogs

## Pseudonym



# Pseudonyme Kommunikation in Hyphanet

## „Sozial“

- Foren
- Microblog
- Programmieren

## Klassisch

- Dateien/Ordner
- Webseiten
- E-Mail
- Blogs

## Pseudonym



# Kommunikation in Hyphanet

Vertraulich



Offiziell



Pseudonym



praktisch genutzt

# Darknet Nachrichten

## My Friends (trusted peers added by me)

Nickname for this node: ArneBab [\[Change\]](#)

	Status	Name	Trust level
<input type="checkbox"/>	CONNECTED	[REDACTED]	NORMAL
<input type="checkbox"/>	CONNECTED	[REDACTED]	NORMAL

<input type="checkbox"/>	NEVER CONNECTED*	[REDACTED]	NORMAL
--------------------------	------------------	------------	--------

Send N2NTM to selected peers

Change trust to

Change visibility to

## Send Node to Node Text Message

Composing N2NTM to send to the following peers:

[REDACTED]

## Node to Node Text Message 2 from

[REDACTED]

From: [REDACTED] (composed 18.09.14 23:05 | sent 18.09.14 23:05 | received 18.09.14 23:05)

I still hope [REDACTED]

[Reply](#)

## Node to Node Text Message 1 from

[REDACTED]

From: [REDACTED] (composed 18.09.14 18:29 | sent 18.09.14 18:29 | received 18.09.14 18:30)

[REDACTED]

[Reply](#)

## Freemail



## Freemail

**Browsing**

- Browse Freenet
- Upload a Freesite
- Search Freenet!

**Community**

- Home
- Own anonymous identities
- Known anonymous identities
- Configuration

**Filesharing**

- Downloads
- Uploads
- Upload a file

**Friends**

- Connections to friends
- Add a Friend

**Discussion**

inbox
Sent

Delete
Inbox/Sent: c
Move

	<u>Subject</u>	<u>From</u>	<u>Date</u>
<input type="checkbox"/>	<a href="#">Re: Freenet Umzug</a>	ArneBab <ArneBab@5ptegyo3ycarnufd4n2gojbc5uscvsjp4bg4zblzung5j57xc33a.freemail>	19.07.2014 17:48:46
<input type="checkbox"/>	<a href="#">infocalypse-gvcs-over-freenet.R1/10</a>	HieronymusCH <hieronymusch@74avt2pm6bjxif4zvxp825cfw5whrjgk3nrxu7qq66ew6tv4aq.freemail>	18.07.2014 16:07:12
<input type="checkbox"/>	<a href="#">Freenet Umzug</a>	Vincenzo_Peacock <Vincenzo_Peacock@hgrnv7cbmdudp6ingje5edzqb7ndm6icx6b6dhx2aryeixwegwgsa.freemail>	16.07.2014 11:36:37
<input type="checkbox"/>	<a href="#">Freenet Umzug</a>	Vincenzo_Peacock <Vincenzo_Peacock@hgrnv7cbmdudp6ingje5edzqb7ndm6icx6b6dhx2aryeixwegwgsa.freemail>	15.07.2014 20:31:04
<input type="checkbox"/>	<a href="#">Hallo</a>	hisoka11 <hisoka11@mqapmmkikdtkh2fjcx46u2xtancxzizqwmwdw3wrfos4frpsa.freemail>	06.07.2014 22:23:58
<input type="checkbox"/>	<a href="#">Welcome to Freemail!</a>	Martin Nyhus <zidel@b5zswai7ybkmvcrfdlz5euw3ifzn5z5m3bzdgpucb26mzqvsfliq.freemail>	07.05.2014 09:33:34

# Web of Trust



## Web of Trust

**Browsing**

- Browse Freenet
- Upload a Freesite
- Search Freenet!

**Community**

- Home
- Own anonymous identities
- Known anonymous

**Summary**

Name	Last change	Last insert	Publishes Trustlist	Trusters	Trustees	Manage
ArneBab	2014-09-13 00:55:13	<u>2014-09-13</u> <u>00:55:13</u>	Yes	<u>494</u>	<u>514</u>	<input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Introduce"/>

Nickname:

---

**Restore an own identity from Freenet**

Use this if you lost your database for some reason but still have your identity's insert URI:

Insert URI:

**Summary**

Own Identities: 11  
 Known Identities: 10243  
 Trust relationships: 193658  
 Score relationships: 80853

# Webseiten lesen



## NERDAGEDDON

Generated: 2014-09-01



Welcome to Nerdageddon. Here we aim to bring you a list of all freesites, both old and new which could be interesting to political nerds. The links presented here exclude the sites which Linkageddon flags as porn or cp, and those which I perceive as normal. Sites are excluded via a blacklist, so new sites will appear here until I remove them to ensure that the index stays useful (though a bit messy) even if I do not get to check the sites.

If you feel the title and/or description for a particular freesite does not give sufficient warning about it's content then please feel free to comment to that effect on Some or to the relevant FMS board. If Linkageddon changes the description or title, this site will reflect that at the next update.

Use the KeyUtils plugin to extract all scripts which generate this site.

<p><b>xkcd - A webcomic of romance, sarcasm, math, and language - By Randall Munroe</b></p> <p>Freenet mirror of popular web comic.</p> <p>Updated: 2014-08-29</p>	<p><b>Mémoires</b></p> <p>French language freesite</p> <p>Updated: 2014-08-29</p>	<p><b>Freenet Statistics</b></p> <p>Updated: 2014-08-29</p>
<p><b>Index - Mis mierdas</b></p> <p>Hadie te obliga a leerme</p> <p>Updated: 2014-08-29</p>	<p><b>Enzo's Index</b></p> <p>Another Freenet Key index by Enzo.</p> <p>Updated: 2014-08-29</p>	<p><b>Korean Pop Music Girl Band Videos</b></p> <p>Updated: 2014-08-29</p>
<p><b>House of Cards</b></p> <p>Download episodes from the Netflix TV series House of Cards</p> <p>Updated: 2014-08-28</p>	<p><b>Freenet statistics</b></p> <p>Some data and graphs of the retrievability of Freenet data over time.</p> <p>Updated: 2014-08-28</p>	<p><b>Mitsu'liens</b></p> <p>Sharing interesting links and short posts (based on Shaarli)</p> <p>Updated: 2014-08-28</p>
<p><b>IRC Log</b></p> <p>Log of previous day's discussion on the official Freenet IRC development channel.</p> <p>Updated: 2014-08-28</p>	<p><b>Alejandro</b></p> <p>Updated: 2014-08-27</p>	<p><b>Index - Hieronymus' Flog</b></p> <p>my free digital home</p> <p>Updated: 2014-08-27</p>
	<p><b>Programming</b></p> <p>Programming</p> <p>Updated: 2014-08-26</p>	<p><b>Index - Something Satanic</b></p> <p>b4ph0m37's flog about Atheism, Satanism &amp; Satan.</p> <p>Updated: 2014-08-26</p>

# Webseiten schreiben

### Edit ShareWiki freesite

[Go back to freesite menu](#)

Name / Title:

Short description of your freesite:

Full description, text and links:

## Foren: FMS

Home   Browse Freetnet   Browse Forums			
» Browse Forums		<input type="text"/> <input type="button" value="Sign In"/>	
		<input type="text"/> <input type="button" value="Search"/>	
Mark All Read			
New	Forum	Posts	Last Post
	<b>bitcoin</b> www.bitcoin.org	25 posts	Last post on 2014-04-30 21:28:23 in <a href="#">'Dark Wallet' Is About to M...</a> by MyID@PRJ1J82LylfZ3o-nd6221...
	<b>encrypted.messages</b> shared board for private messaging	0 posts	
	<b>flip</b> Freetnet Lightweight IRC Program	0 posts	
	<b>fms</b> Freetnet Message System	190 posts	Last post on 2014-06-12 18:49:32 in <a href="#">Re: How to autostart FMS on...</a> by Ada_Crandell@IDu3FJtpeFN1Xh...
	<b>freemail</b> Freemail	16 posts	Last post on 2014-06-07 12:38:32 in <a href="#">Re: How does it work?</a> by Groov@cNcXSeDF4A50Li-bkQ4fp...
	<b>freetnet</b> Discussion about Freetnet	680 posts	Last post on 2014-06-15 01:25:21 in <a href="#">Re: problem with freenet ve...</a> by operhlem1-notrust@LikDnTCJ3...
	<b>freetnet.0.7.bugs</b>	0 posts	
	<b>freetalk</b> freetalk	0 posts	
	<b>frost.freetnet</b>	455 posts	Last post on 2014-06-15 14:03:17 in <a href="#">Re: Patched 1462</a> by Anonymous
	<b>leak</b> Leaked documents	3 posts	Last post on 2014-06-06 23:04:44 in <a href="#">Re: [X-post from Frost] Lea...</a> by Yomper@t-R8mLbceLwMuRWdsd0Z...
	<b>news</b> News	241 posts	Last post on 2014-06-15 09:38:52 in <a href="#">CRYPTO-GRAM, June 15, 2014</a> by r_st@A4zx-

# Microblog: Sone



many identities.

about a week ago · [\[link author\]](#) · [Comment](#) · [Toggle Parser](#) · [Like](#) · ✓ · ✕



**Guoray\_Sigismund** I can put a piece of paper over my webcam, but what can I do about the microphone?

☆ · about a week ago · [\[link post\]](#) · [\[link author\]](#) · [Comment](#) · ↑1 · [Like](#) · ✓ · ✕



**Saul\_Particle** @Guoray\_Sigismund You could pull the tiny microphone plug from the board. On notebooks this is sometimes below the keyboard, so you won't have to disassemble too many parts. \*At your own risk\*

Maybe removing the sound driver (kernel modul) could be a first step without having to modify hardware (but you'll lose sound out that way)

about a week ago · [\[link author\]](#) · [Comment](#) · [Toggle Parser](#) · [Like](#) · ✓ · ✕



**NowWhat** @Guoray\_Sigismund Is the microphone really that big a deal though? I can't imagine most are good at picking up stuff that isn't close to the mic anyway. Also, anybody who could access your microphone is likely able t... » [show more](#)

about a week ago · [\[link author\]](#) · [Comment](#) · [Toggle Parser](#) · ↑1 · [Like](#) · ↻



**Guoray\_Sigismund** @Saul\_Particle It's one idea, but quite a bit of effort. Also I'd have to do it with phone, tablet, laptop etc :p

If a laptop is compromised, surely it could just modprobe the module itself?

5 days ago · [\[link author\]](#) · [Comment](#) · [Toggle Parser](#) · [Like](#) · ✓ · ✕



**Saul\_Particle** @Guoray\_Sigismund Indeed, quite a bit of effort. That's why the mainstream user will not do it.

You also cannot cut the wire on the phone you want to phone with... you'd need a second phone with working microphone (maybe be a €/5 20 'feature phone') you only switch on if you want to make a call.

I read Jacob Applebaum, while on stage at the Chaos Communication Congress, pulled out a cheap phone and a loose battery from his pocket, put the battery into the phone, sent an SMS, then removed the battery again. « [show less](#)

5 days ago · [\[link author\]](#) · [Comment](#) · [Toggle Parser](#) · [Like](#) · ✓ · ✕



**Saul\_Particle** @Guoray\_Sigismund \*pocket

5 days ago · [\[link author\]](#) · [Comment](#) · [Toggle Parser](#) · [Like](#) · ✓ · ✕

# Zusammenfassung

Warum?

Selbstzensur

Lösungen

Freie Kommunikation im Internet

Vertraulich



Offiziell



Pseudonym



Technik

Eine Vision

# Alleinstellungsmerkmale

- Freund-zu-Freund Darknet (plus Opennet)
- Hosting ohne Server (hochladen und verschwinden)
- Stabile Pseudonyme (privater Schlüssel)
- Dezentrale Spamresistenz (erprobt)
- Nutzungsabhängige Lebenszeit (anonym)

# Technik und Politik

## Tech alleine reicht nicht

Totale Überwachung und Kontrolle sind möglich.

## Politik alleine reicht nicht

Wenn Überwachung und Zensur trivial sind, werden sie genutzt.

## Tech und Politik

Technologie liefert die Grundlage, auf der Politik arbeiten kann: Überwachung und Zensur so aufwändig und teuer machen, dass wir den politischen Kampf gewinnen können.

*The NSA surveillance doesn't scale. \ – Constanze Kurz (EuroPython 2014)*

# Zusammenfassung

## Warum?

Selbstzensur im Netz

## Technik

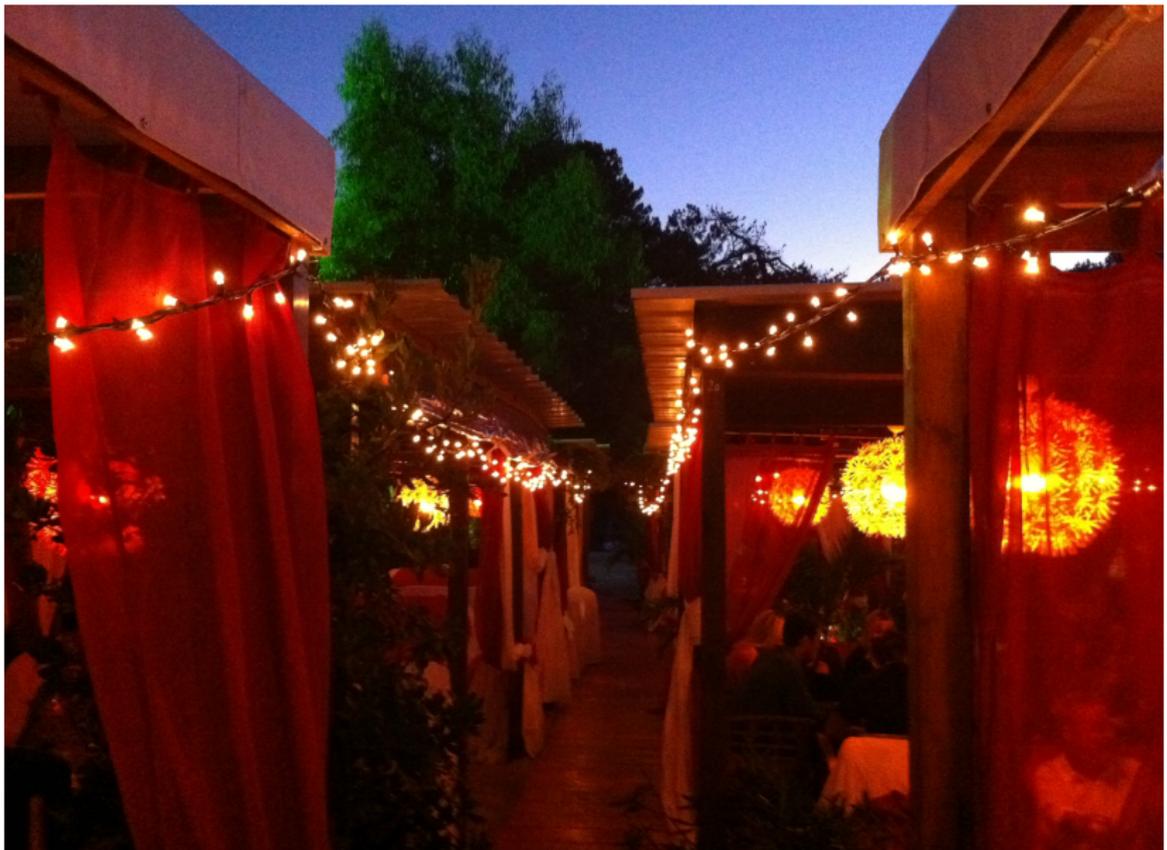
Stabile Grundlage:

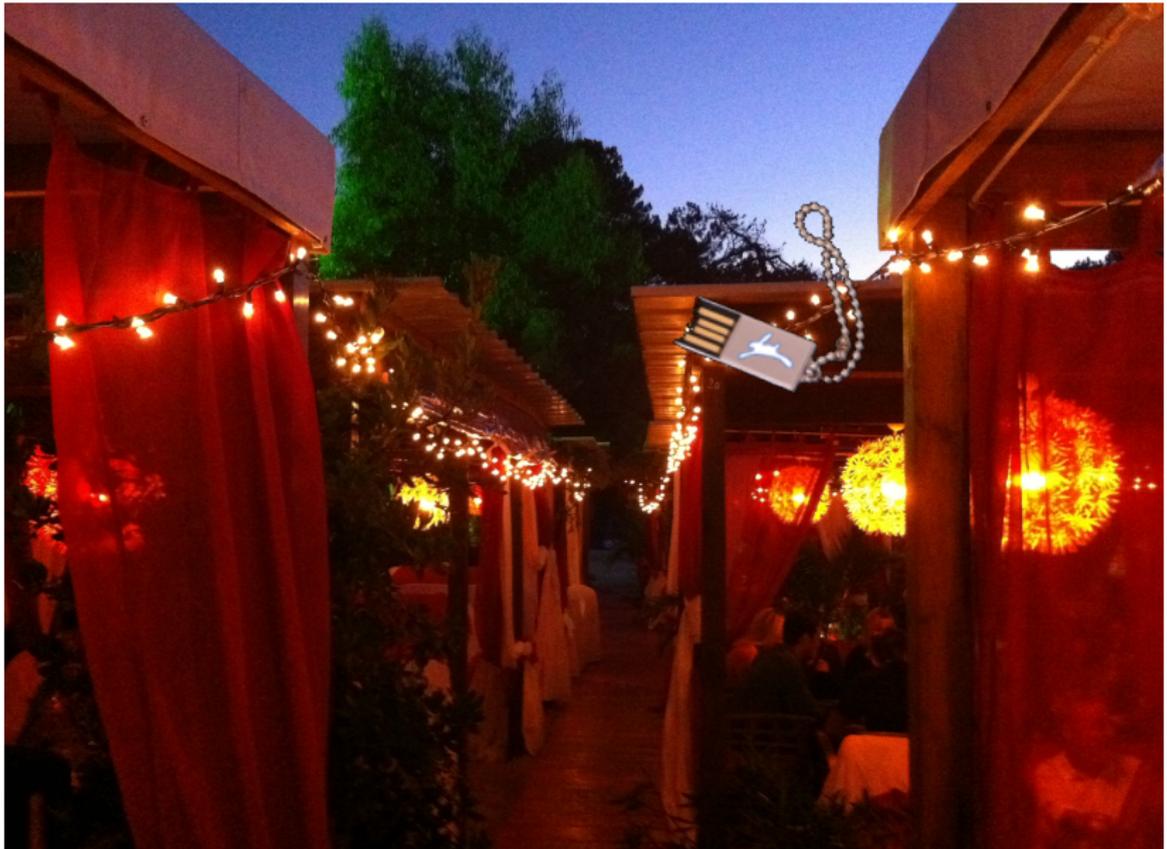
- Skaliert
- Pseudonyme
- Fokus auf wirklicher Pressefreiheit
- Grundlage für politisches Handeln

## Lösungen

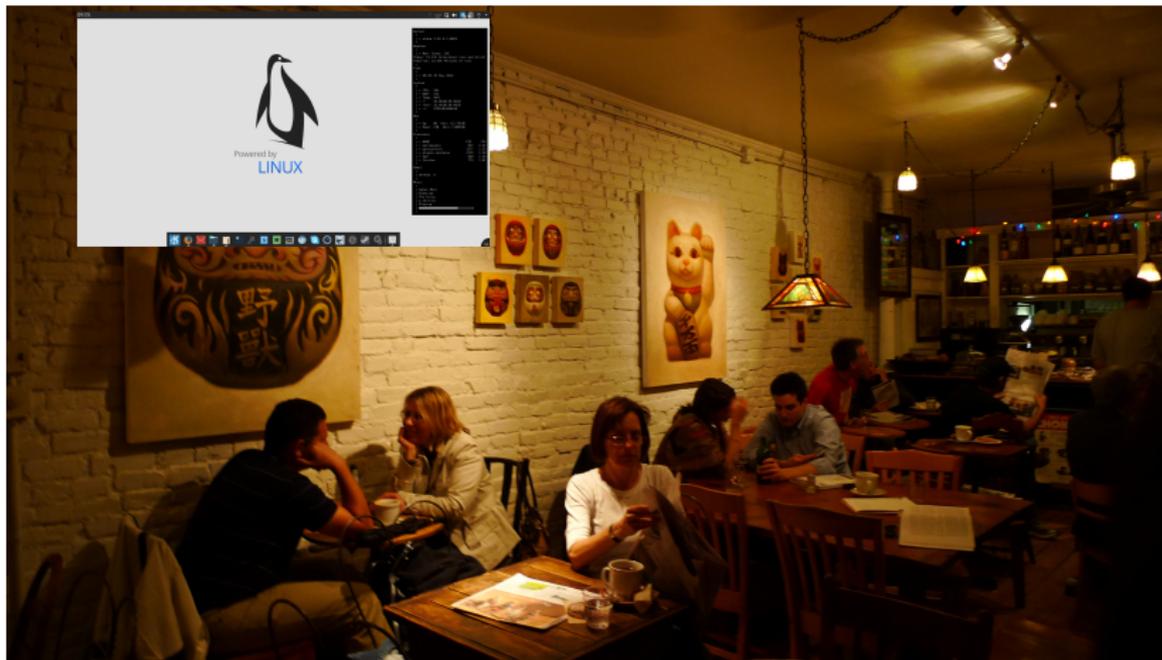
Freie Kommunikation

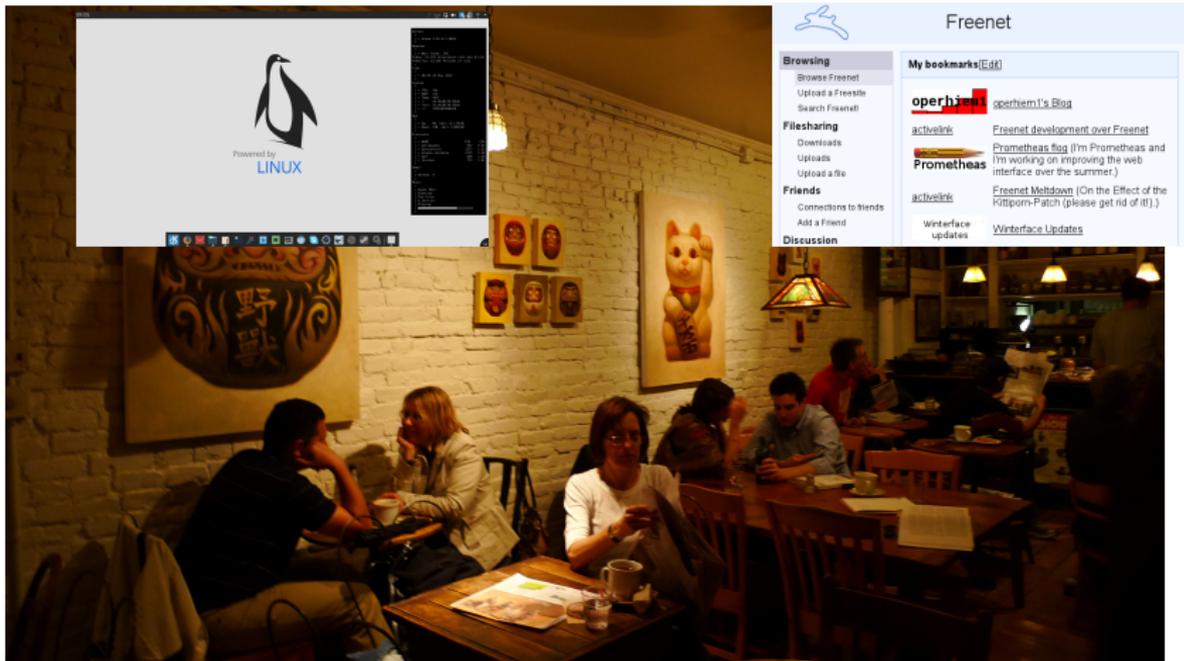
## Eine Vision

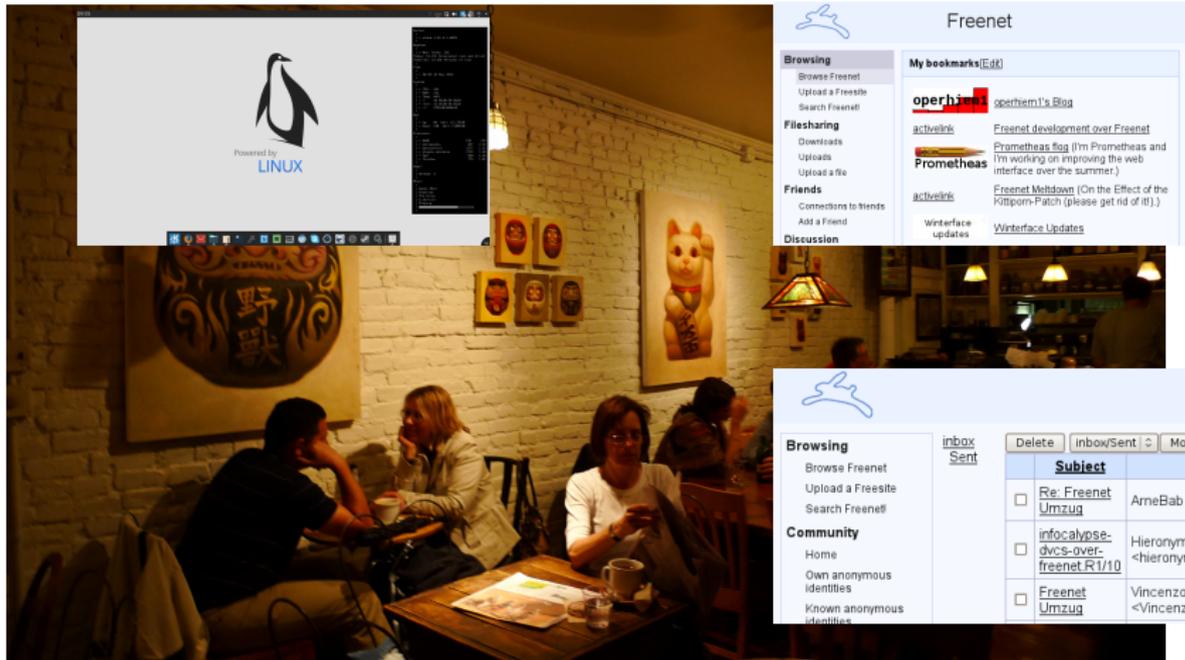






















**Browsing**

- Browse Freenet
- Upload a Freesite
- Search Freeneff

**Community**

- Home
- Own anonymous identities
- Known anonymous identities

inbox  
Sent

Delete	Inbox/Sent	Mo	Subject	
<input type="checkbox"/>			Re: Freenet Umzug	ArneBab
<input type="checkbox"/>			infocapypse-gycs-over-freenet R1/10	Hieronym<hieronym
<input type="checkbox"/>			Freenet Umzug	Vincenzo<Vincenz



in  
Sent

	Subject	
<input type="checkbox"/>	Re: Freenet Umzug	ArneBab
<input type="checkbox"/>	infocalyptse-dyds-over-freenet R1/10	Hieronym<hieronym
<input type="checkbox"/>	Freenet Umzug	Vincenzo<Vincenz





**Browsing**

- Browse Freenet
- Upload a Freesite
- Search Freenet

**Community**

- Home
- Own anonymous identities
- Known anonymous identities

inbox Sent

Delete	Inbox/Sent	Subject
<input type="checkbox"/>		Re: Freenet Umzug ArneBab
<input type="checkbox"/>		infocalyse-gyvs-over-freenet R1/10 Hieronym <hieronym@freenet.de>
<input type="checkbox"/>		Freenet Umzug Vincenzo <Vincenzo@freenet.de>

# Zusammenfassung

## Warum?

Selbstzensur im Netz

## Technik

Stabile Grundlage

## Lösungen

Freie Kommunikation

## Eine Vision

- Nicht nachweisbare Pseudonyme
- Whistleblower und Journalisten
- Normale Menschen
- Technisch mit Hyphanet möglich – wir wollen es einfach machen

# Nutzt Hyphanet!



hyphanet.org



Abbildung: ArneBab, toad, leuchtkaefer, digger3.

Außerdem:

- operhiem1
- xor: WoT
- nextgens: Sicherheit
- Bombe: Sone
- TheSeeker
- SomeDude: FMS
- Eleriseth: Kern
- ... (ein Dutzend mehr)

# Quellen

Diese Präsentation: [github.com/ArneBab/freenet-fundraising/](https://github.com/ArneBab/freenet-fundraising/)  
Bilder: Hase unter GPL, alle weiteren cc by.

- <https://www.flickr.com/photos/anonymous-munich/3282278914>
- <https://www.flickr.com/photos/okubax/15814107199>
- <https://www.flickr.com/photos/okubax/14248440483>
- <https://www.flickr.com/photos/okubax/15812839470>
- <https://www.flickr.com/photos/gruenejugendffm/6272541036>
- <https://www.flickr.com/photos/okubax/15812839470>
- <https://www.flickr.com/photos/eppofficial/13564824463>
- <https://www.flickr.com/photos/digitpedia/4709307610>
- <https://www.flickr.com/photos/maguide/6092244239>

## Quellen2

- <https://www.flickr.com/photos/focusc/4758319160>
- <https://www.flickr.com/photos/amitd/4693814169>
- [http://commons.wikimedia.org/wiki/File:International\\_newspaper,\\_Rome\\_May\\_2005.jpg#metadata](http://commons.wikimedia.org/wiki/File:International_newspaper,_Rome_May_2005.jpg#metadata)
- [http://commons.wikimedia.org/wiki/File:Edward\\_Snowden\\_2013-10-9\\_%281%29\\_%28cropped%29.jpg](http://commons.wikimedia.org/wiki/File:Edward_Snowden_2013-10-9_%281%29_%28cropped%29.jpg)

# Eine alte Hoffnung

- 1995: Scheideweg: **Überwachung oder Freiheit.**
- 1999: **Freenet** gestartet.
- 2001: **9/11**. War on Terror.
- 2013: Snowden. Kostbare Zeit, um **das Rad zurück zu drehen.**

# Programmieren: Infocalypse

```
$ hg clone freenet://USK@j2Mfv0b81MNSslh3Qg9gs1vgQj36whsuosP8ydZq158,\
Xb~vh8XEXmdwGFca4HAX-ILOZD6AWPVuRzIuLerl4PU,AQACAAE/infocalypse-repo.R1/17
```

...

As basic protection, infocalypse automatically set the username  
'anonymous' for commits in this repo...

```
$ hg fn-pull-request
```

...

```
$ hg fn-check-notifications
```

...

- clone / fork
- pull
- pull-request

# Weitere Technische Grundlagen

- Unveränderlicher Datenspeicher
- Aktualisierbar durch Versionierung
- Hochladen mit
  - Passwort (KSK — CAPTCHAs)
  - Pseudonym (SSK/USK — Webseiten)
  - Inhalt (CHK — erneut hochladen)

# Nutzermeinungen

*The practical cool result now, is that the Mempo repository can not be censored, DDoSed or taken offline, despite having just 1 tiny server (or no server at all) \ — rfreeman im Artikel „apt-get over Freenet“.*

*“After running the Tor services for years it was a big relief to just shut down the services for good and say ‘fuck it’. I never again had to worry no more about security. With Freenet I am Free, it suites the name pretty well if you ask me.” \ — Unkwon*

# Skaliert schon?

*Was steht noch, wenn morgen 10 mio Menschen Hyphanet installieren?*

- Darknet Nachrichten
- Dateien/Ordner
- Webseiten
- Programmieren

*Mit Darknet Routing.*

- Opennet (mehr seednodes)
- Foren (fragmentiert)
- Index-Seiten (aufteilen)
- Spam-Schutz mit Web of Trust
  - E-Mail
  - Blogs
  - Microblogs

*Fix WoT: kein globales Wissen: \*  
*bug #6228 und bug 5524.*