digitalcourage
Hochschulgruppe
Bayreuth

Prof. Dr. P. Löbbecke

Freie Messenger – Sichere Kommunikation

Was, warum und wie

Verein und Hochschulgruppe stellen ihr Engagement und ihre Aktivitäten vor

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - „Für eine lebenswerte Welt im digitalen Zeitalter“
  - BigBrotherAwards
  - Aktionen zu aktuellen Themen

- Digitalcourage Hochschulgruppe (www.digitalcourage.de/hsg-bt)
  - Vorträge
  - Workshops
  - Lesungen gegen Überwachung
  - BigBrotherAwards Live Stream (in der Black Box am RW21)

Ausstehende Veranstaltungen finden im Sommersemester online statt

Wir freuen uns über Eure Teilnahme via BigBlueButton; abonniert unsere Mailing-Liste!

- 14. Juni: Digitale Selbstbestimmung und personale Identität
- 19. Juni: Theorie und Praxis von Festplatten-/Stick-Verschlüsselung
- 20. Juni: Passwortmanager/-safes verstehen und nutzen
- 26. Juni: Workshop Spurenarm surfen – Teil 1
- 18. September: Public Streaming der BigBrotherAwards

PETER LÖBBECKE

FH POLIZEI SACHSEN-ANHALT

- Soziologe und Erwachsenenpädagoge
- Interessen u.a.: Internet-Kommunikation und Social Media
- Bedürfnis nach Sicherheit und Schutz der Privatsphäre
- Mitglied bei digitalcourage

Was haben wir heute vor?

- Welche Messenger stehen heute im Mittelpunkt?
- Überblick über den „Status Quo“
- Warum sollte man Freie Messenger kennen und nutzen?

- Die Veranstaltung richtet sich ausdrücklich an Personen ohne Vorkenntnisse!

FRAGEN

Ein wichtiger Hinweis:

Verwendete Logos, Namen etc.

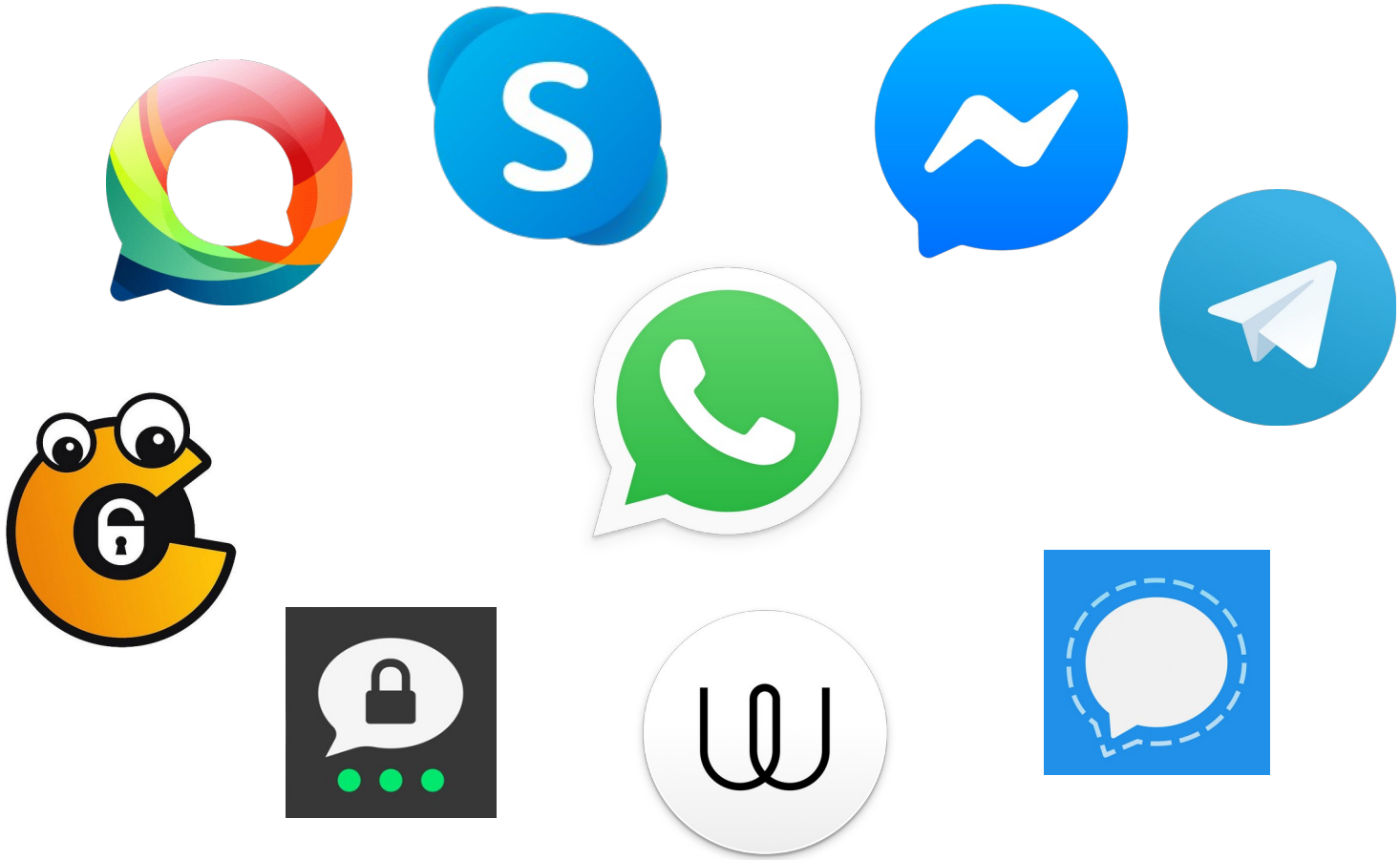
stehen entweder unter einer freien Lizenz

oder sind Eigentum der bezeichneten Firmen.

Ich beziehe außer meinem Gehalt

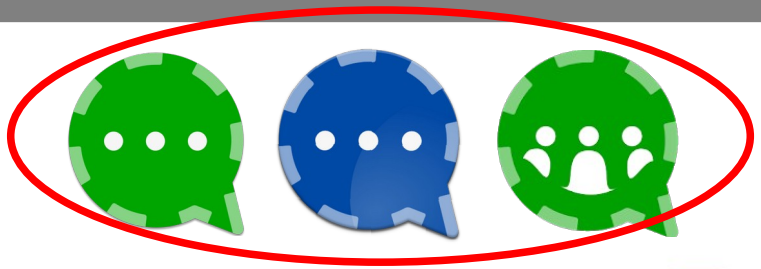
keine Zuwendungen von irgendwem!

Die wichtigsten (?) „Unfreien“ Messenger



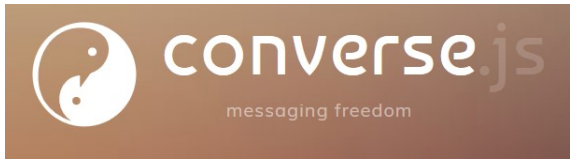
Die wichtigsten (?) „Freien“ Messenger…

- Android:
  - Conversations / Pix-Art / Quicksy



- iPhone / (Mac):
  - Monal / ChatSecure / Siskin

- Browser / Windows / Linux:
  - Gajim / Dino
    Conversejs.org

(

)

Freie Messenger: Die wichtigsten Protokolle

MS Skype

BRIAR

Peer-to Peer-Messaging)

DeltaChat (Email-Messaging)

Grundsätzlich: Zwei Kategorien von Messengern

- **„Proprietäre“** Messenger
  - Bilden eine „Marke“, „gehören“ jemandem, sind unkontrollierbar
  - Können nur untereinander kommunizieren (häufig eigenes „geschlossenes ***Protokoll***“, abgeschlossene „Server“, „***Zentralisierung***“)
  - Können jederzeit die Nutzungsregeln ändern
  - Brauchen das (blinde) Vertrauen der NutzerInnen
- **„Freie“** Messenger
  - Gehören der Allgemeinheit, nicht einem Einzelnen
  - Unterliegen auch sonst keinen Beschränkungen („*Freiheit*“)
  - Sind von jedermann/-frau kontrollierbar
  - Können auch meist fast beliebig mit anderen kommunizieren („öffentliches“ / „freies“ ***Protokoll***, „***Föderation***“)

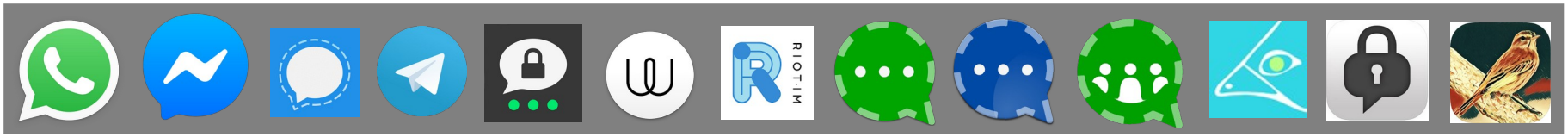
Was sind „Freie“ Messenger?

- **„Freiheit“** in **„Freier Software“** (und **„Freien Messengern“**)
  - Sie können ohne Einschränkung verwendet werden
  - Man kann die Funktionsweise der Software untersuchen und für eigene Zwecke verändern (→ Zugang zum Quellcode)
  - Kopien der Software dürfen weitergegeben werden, um damit andere zu unterstützen
  - Eigene veränderte Versionen dürfen weitergegeben werden, damit die ganze Gesellschaft profitiert (→ Zugang zum Quellcode)

https://www.gnu.org/philosophy/free-sw.en.html, Übersetzung PL

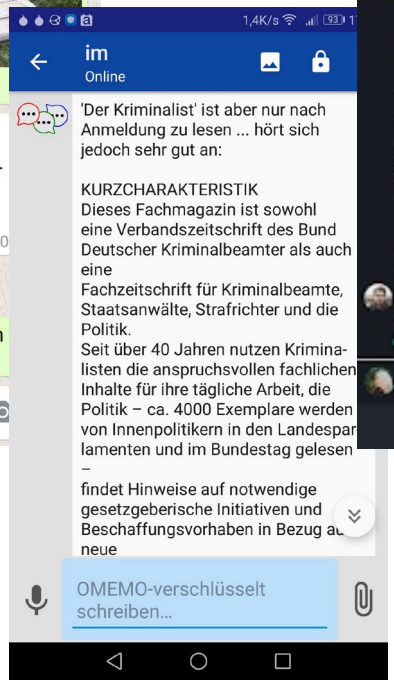
- **„Frei“ hat zunächst einmal nichts mit Geld zu tun!!**

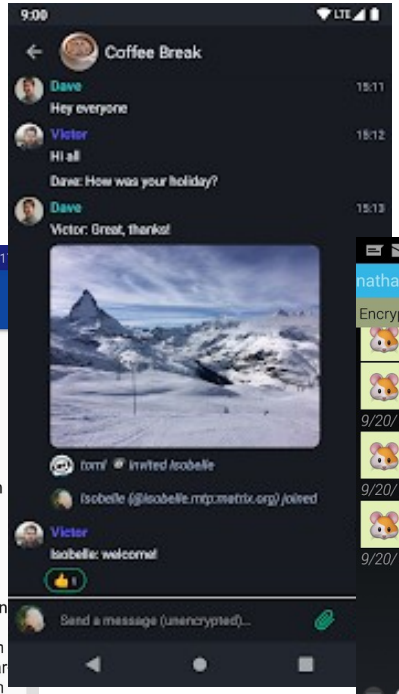
WARUM SOLLTE MICH DAS INTERESSIEREN ?

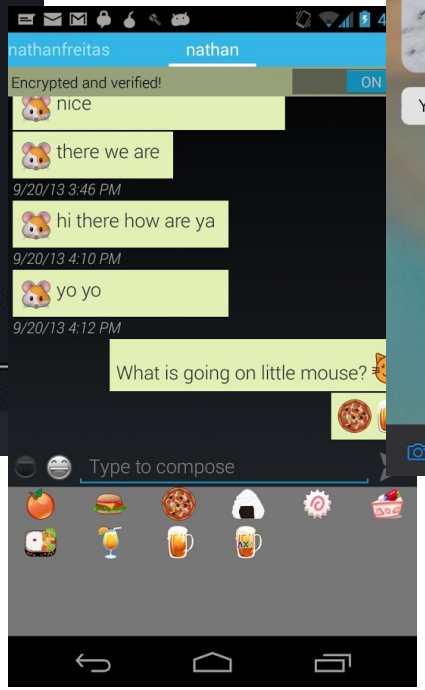


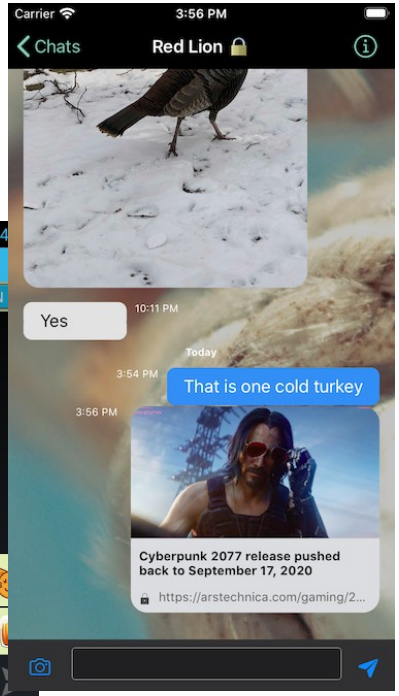
- Alle:
  - Versenden und Empfangen von Textnachrichten, zu zweit und/oder in Gruppen
  - Versenden und Empfangen von Dateien (Bildern, Videos, ...)
  - Verschlüsselung
- Viele:
  - Telefonieren
  - Video-Telefonie

Versenden und Empfangen von Textnachtrichten – zu zweit und in Gruppen

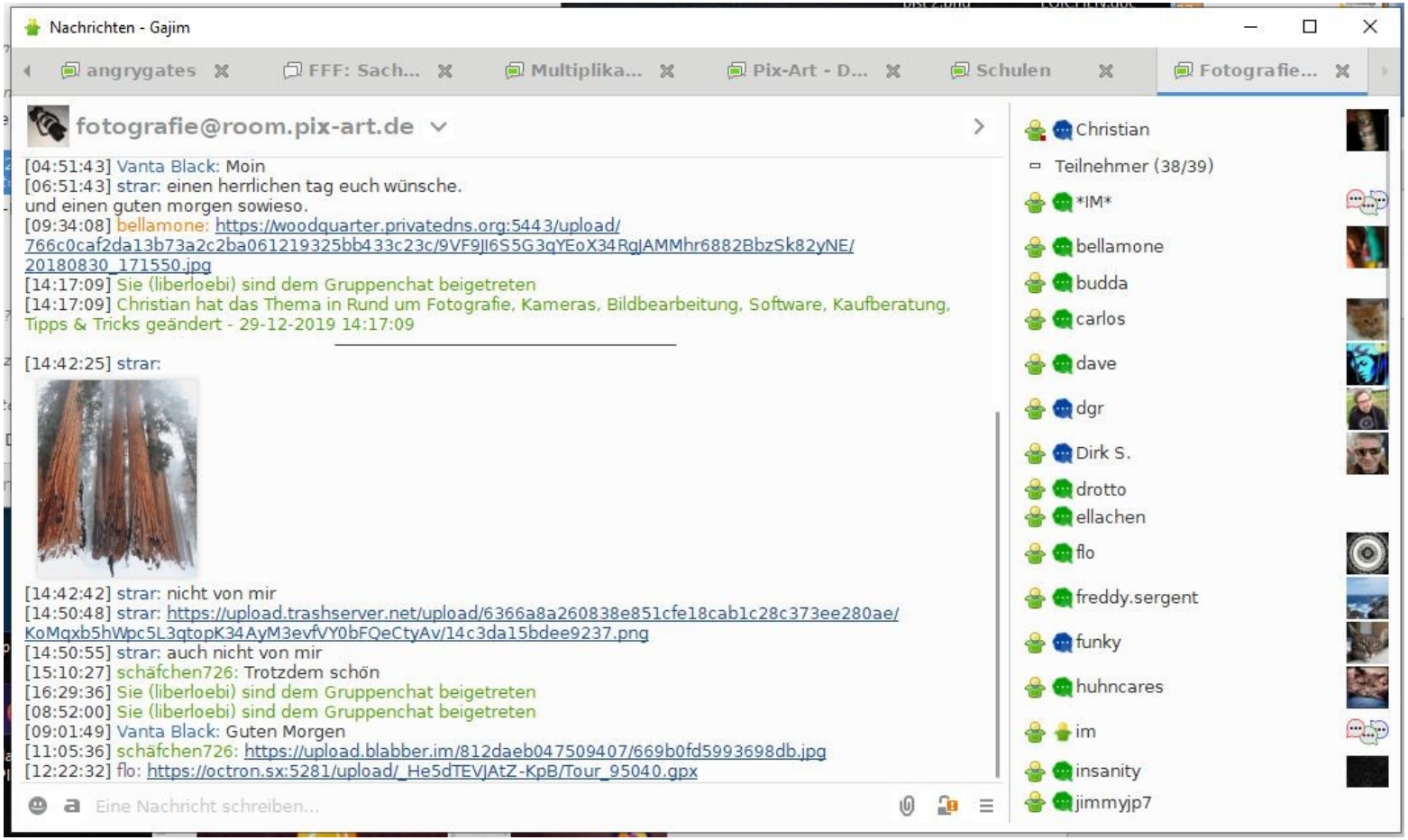




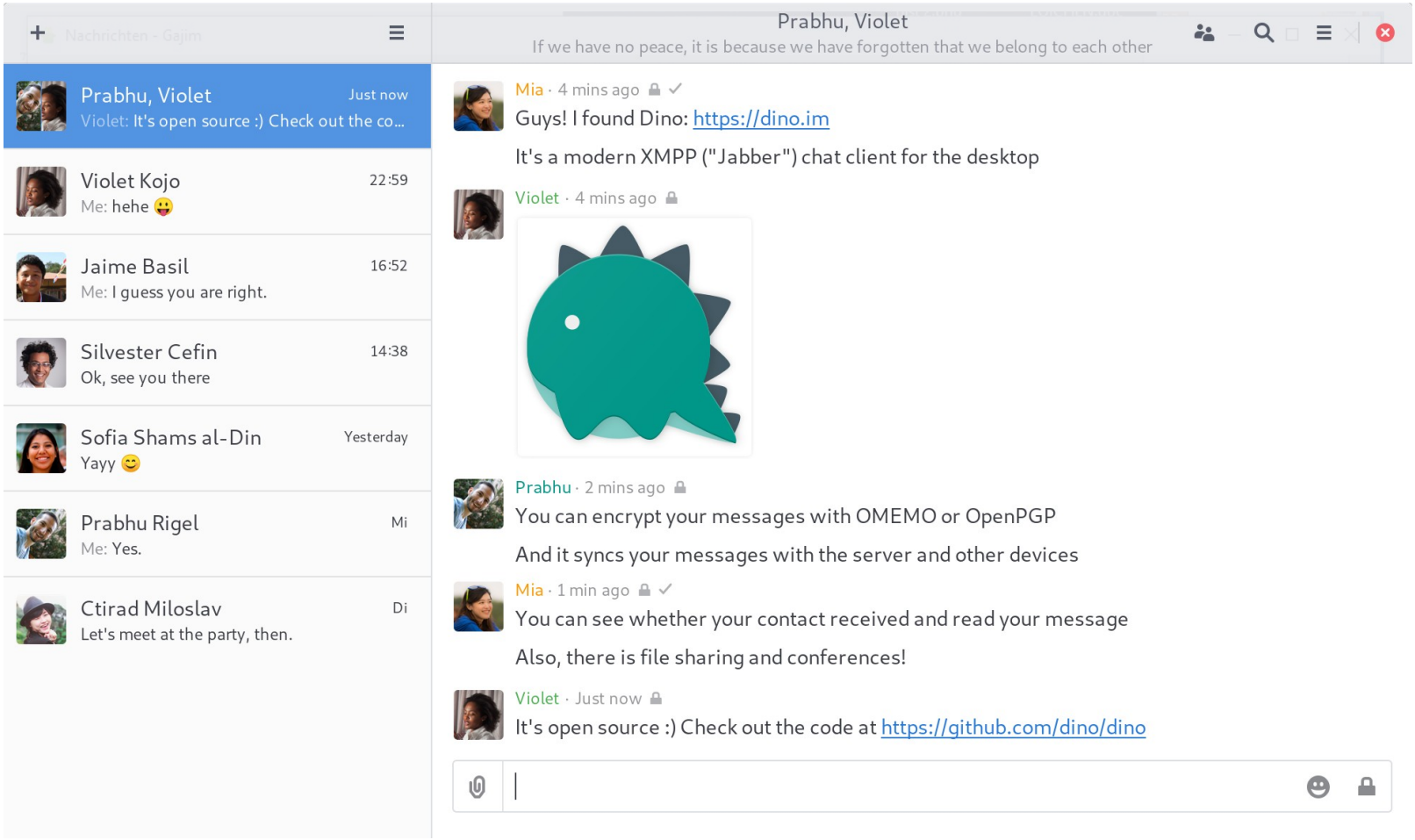




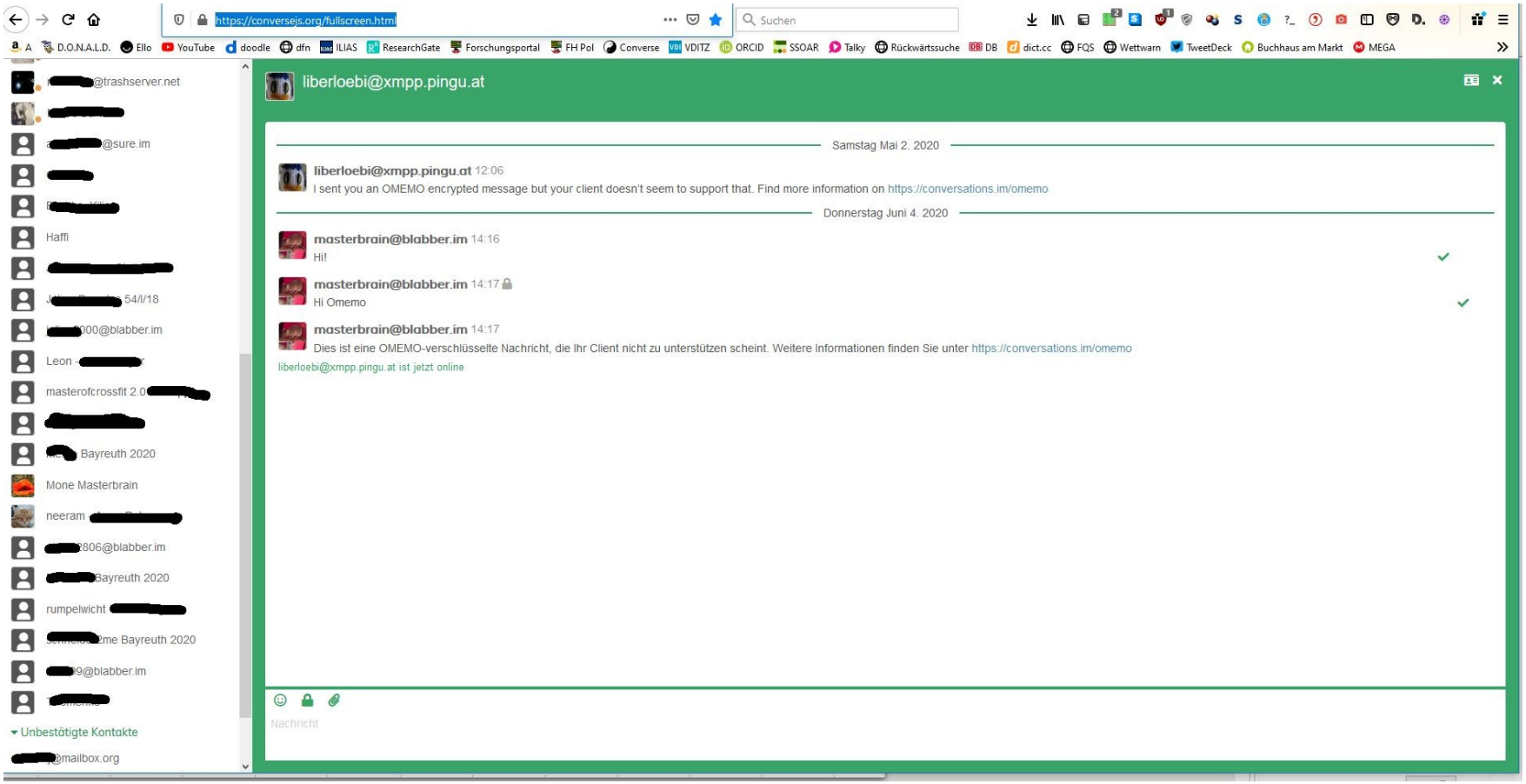
Versenden und Empfangen von Textnachtrichten – zu zweit und in Gruppen



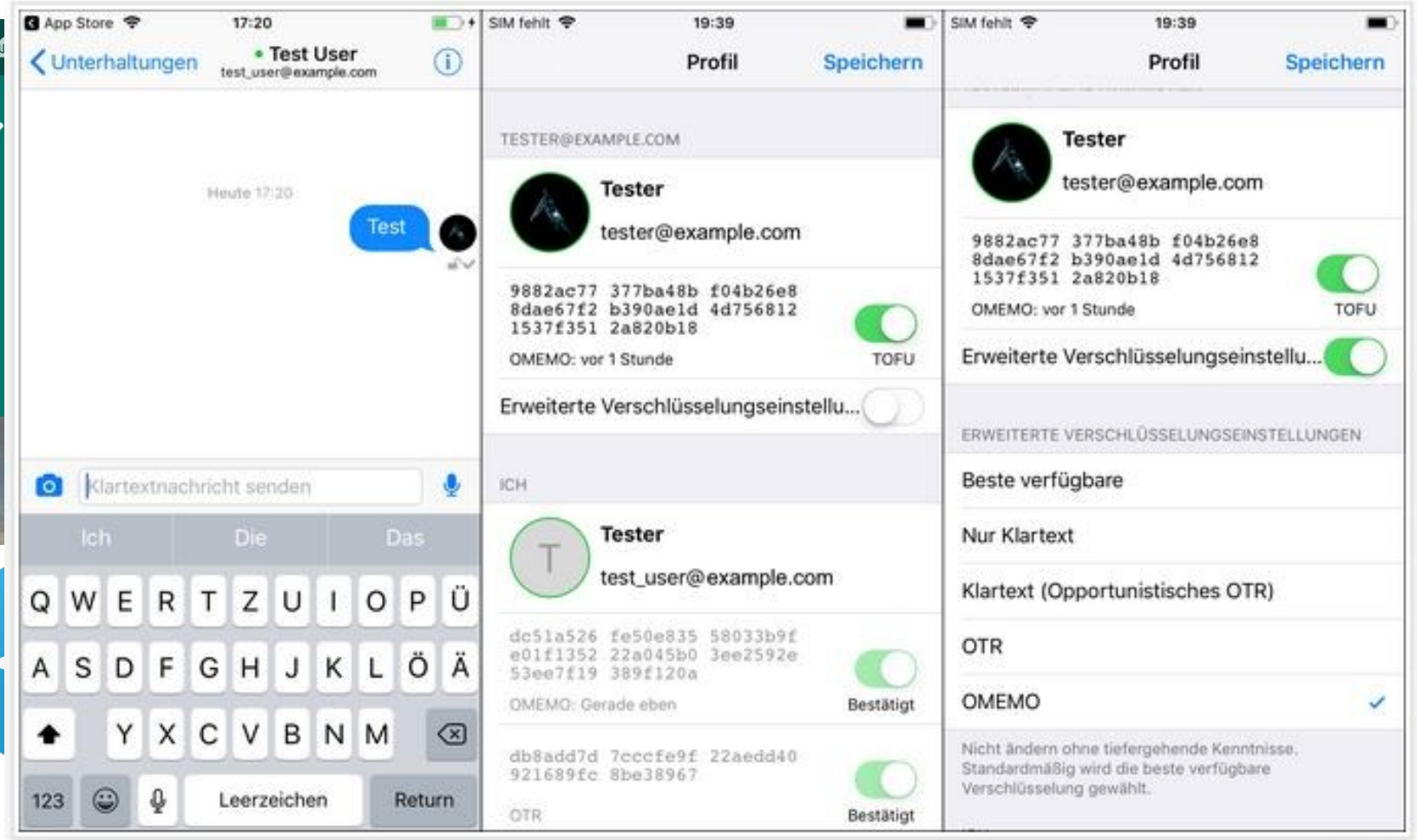
Versenden und Empfangen von Textnachtrichten – zu zweit und in Gruppen



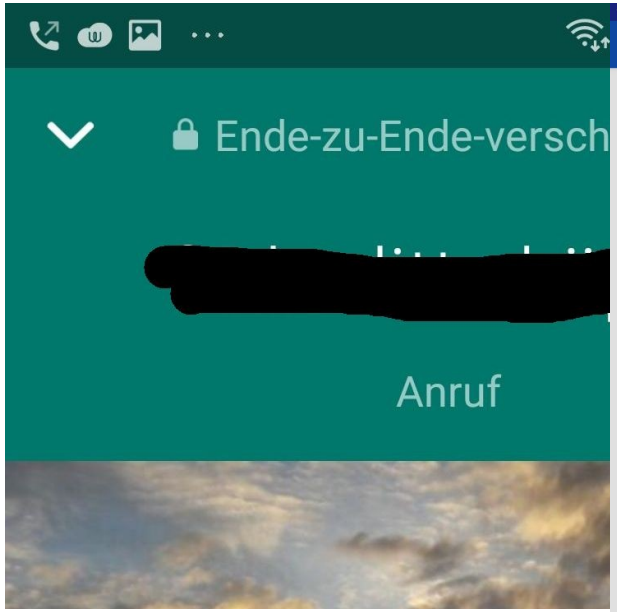
Versenden und Empfangen von Textnachtrichten – zu zweit und in Gruppen

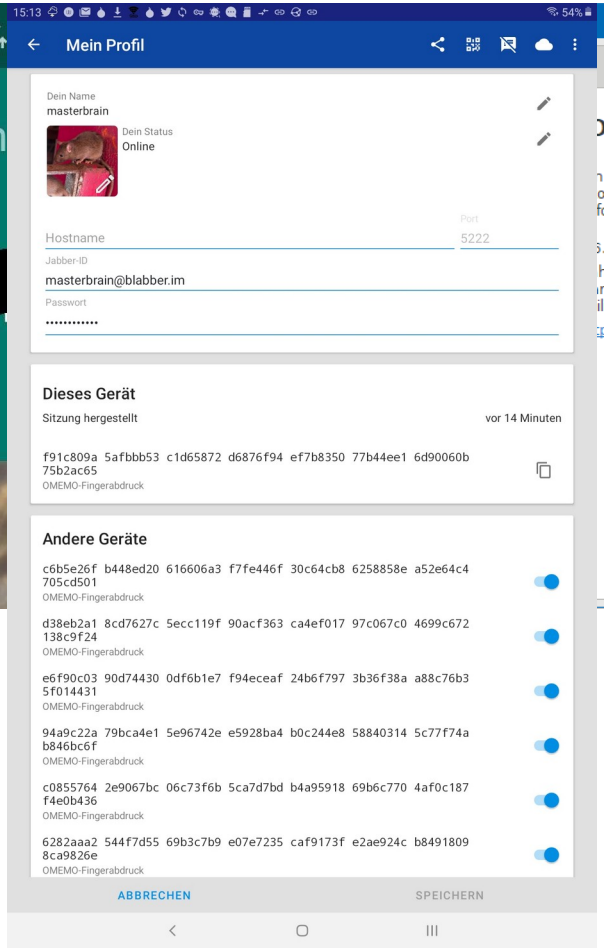


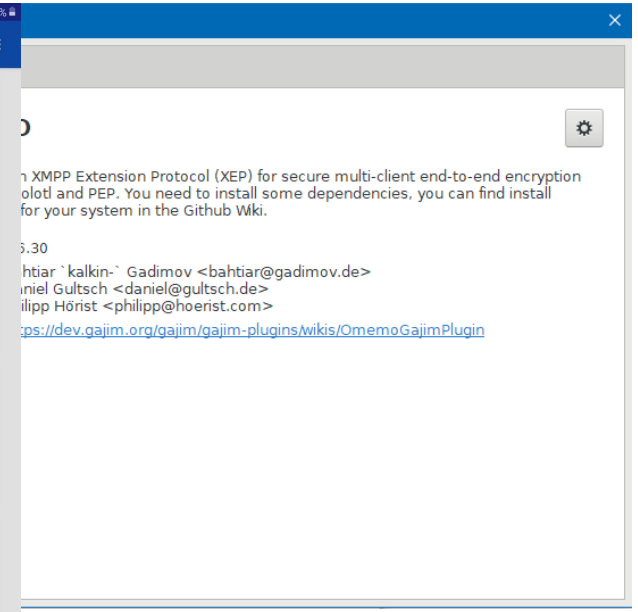
Verschlüsselung



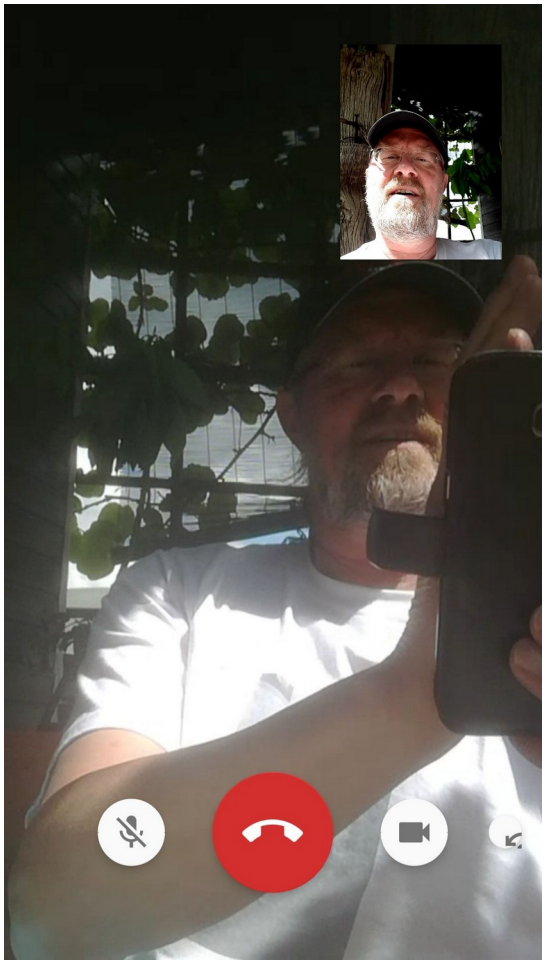
Verschlüsselung

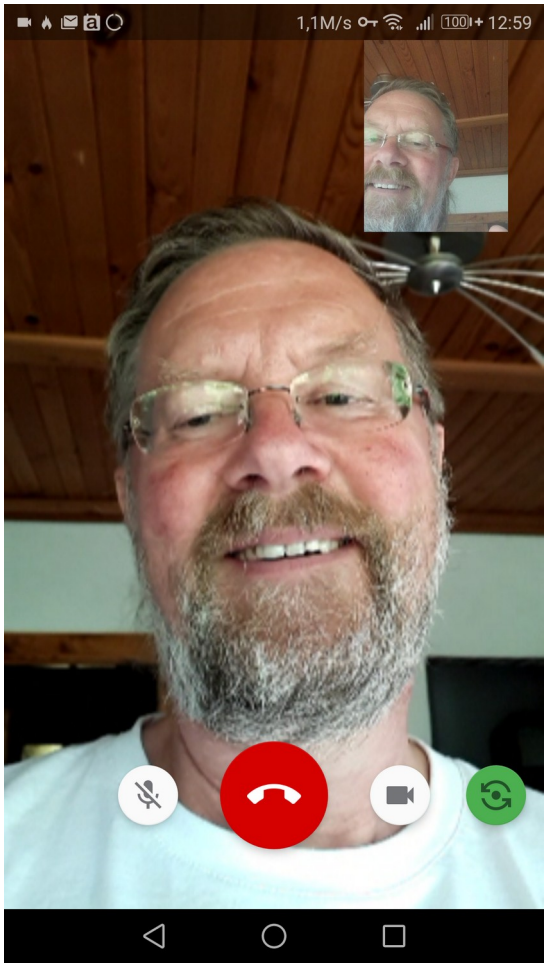


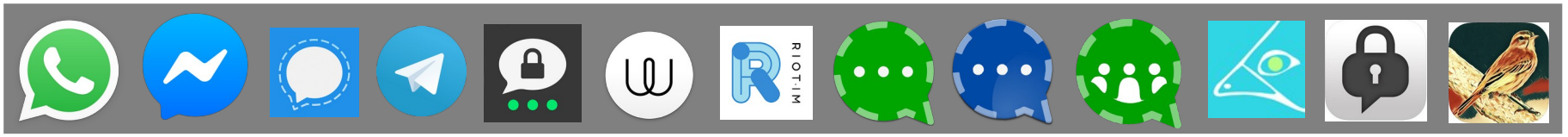




(Video-) Telefonie

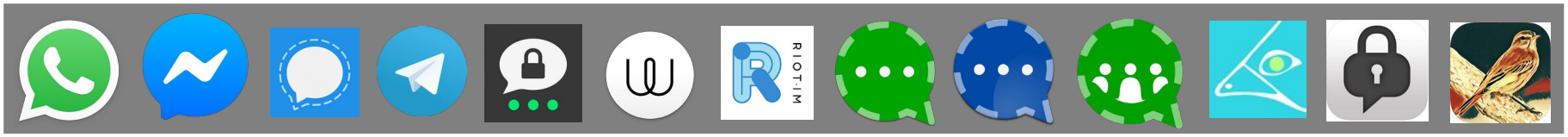




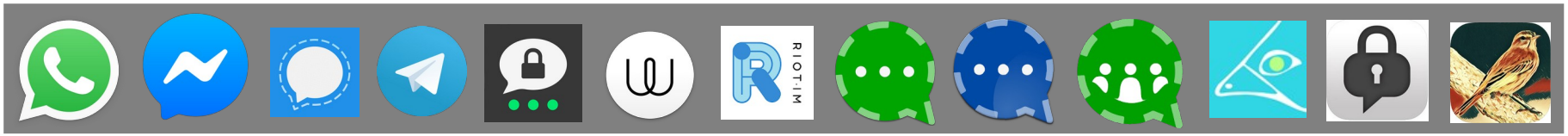


- Alle:
  - Versenden und Empfangen von Textnachrichten, zu zweit und/oder in Gruppen
  - Versenden und Empfangen von Dateien (Bildern, Videos, ...)
  - Verschlüsselung
- Viele (zum Teil in Vorbereitung):
  - Telefonieren
  - Video-Telefonie

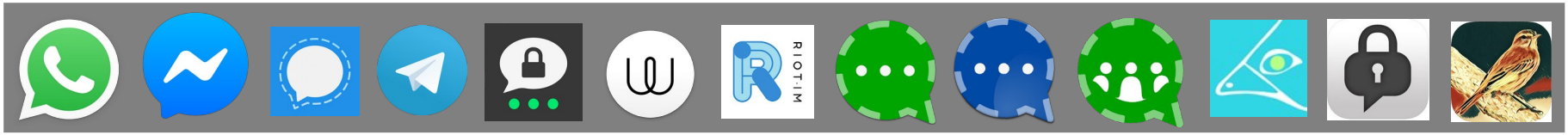
WARUM DANN WECHSELN??

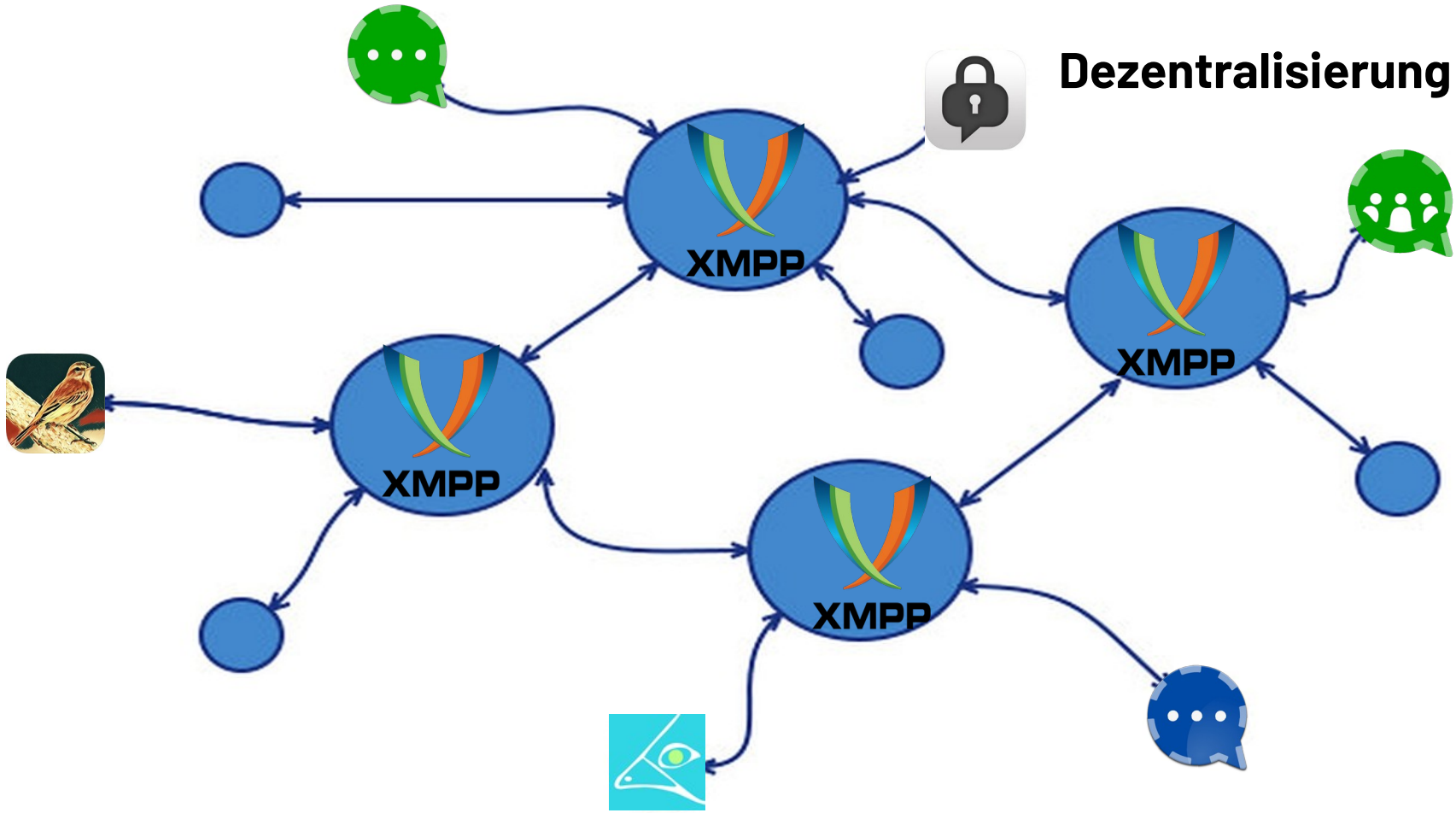


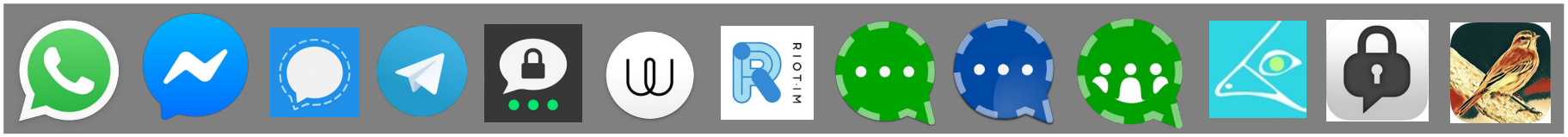
- Interessante Features: Zentralisierung vs. Dezentralisierung
  - Wer kommuniziert mit wem?



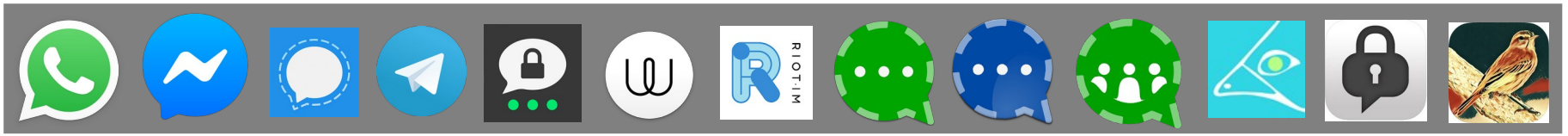
Zentralisierung

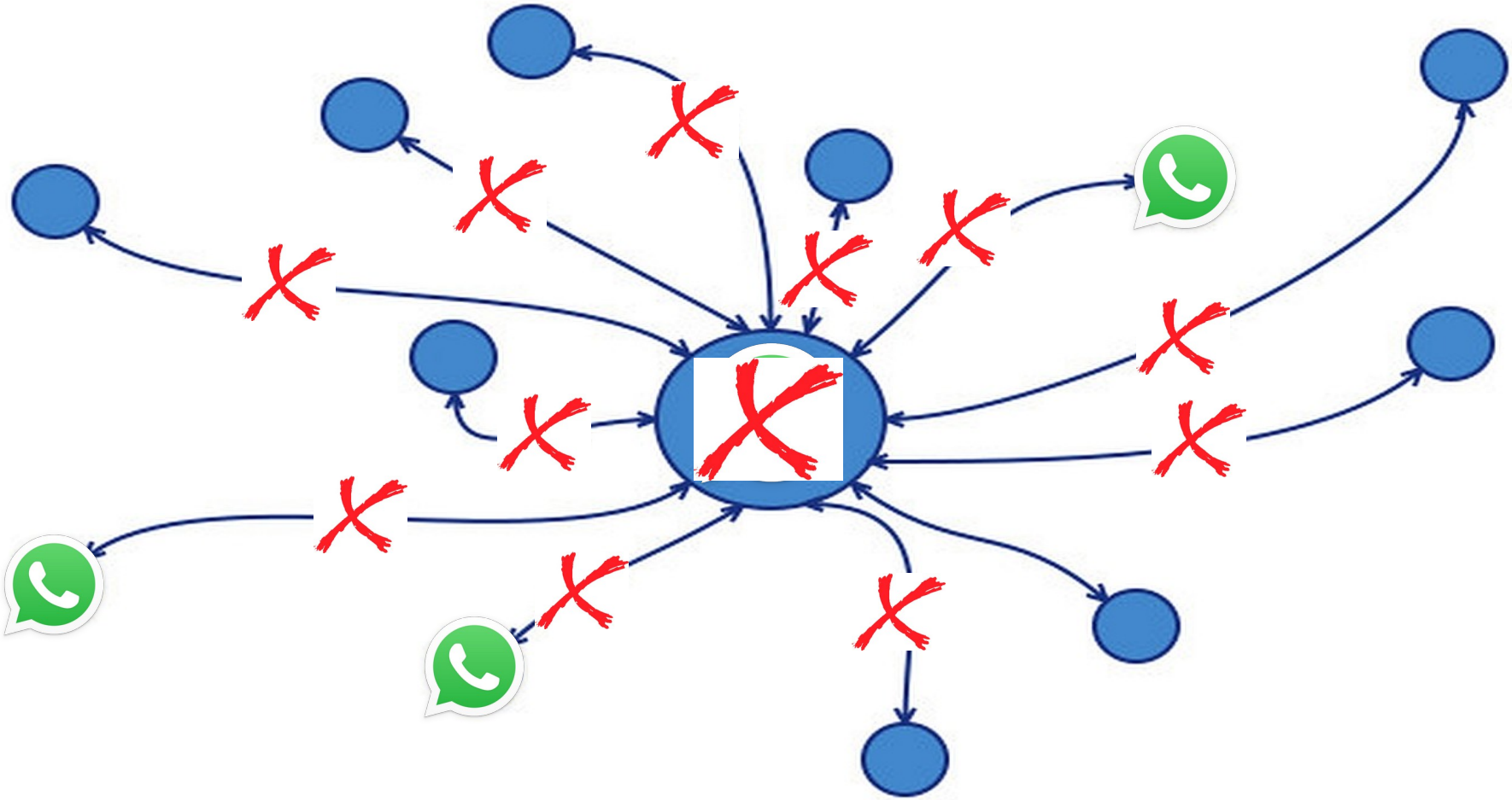


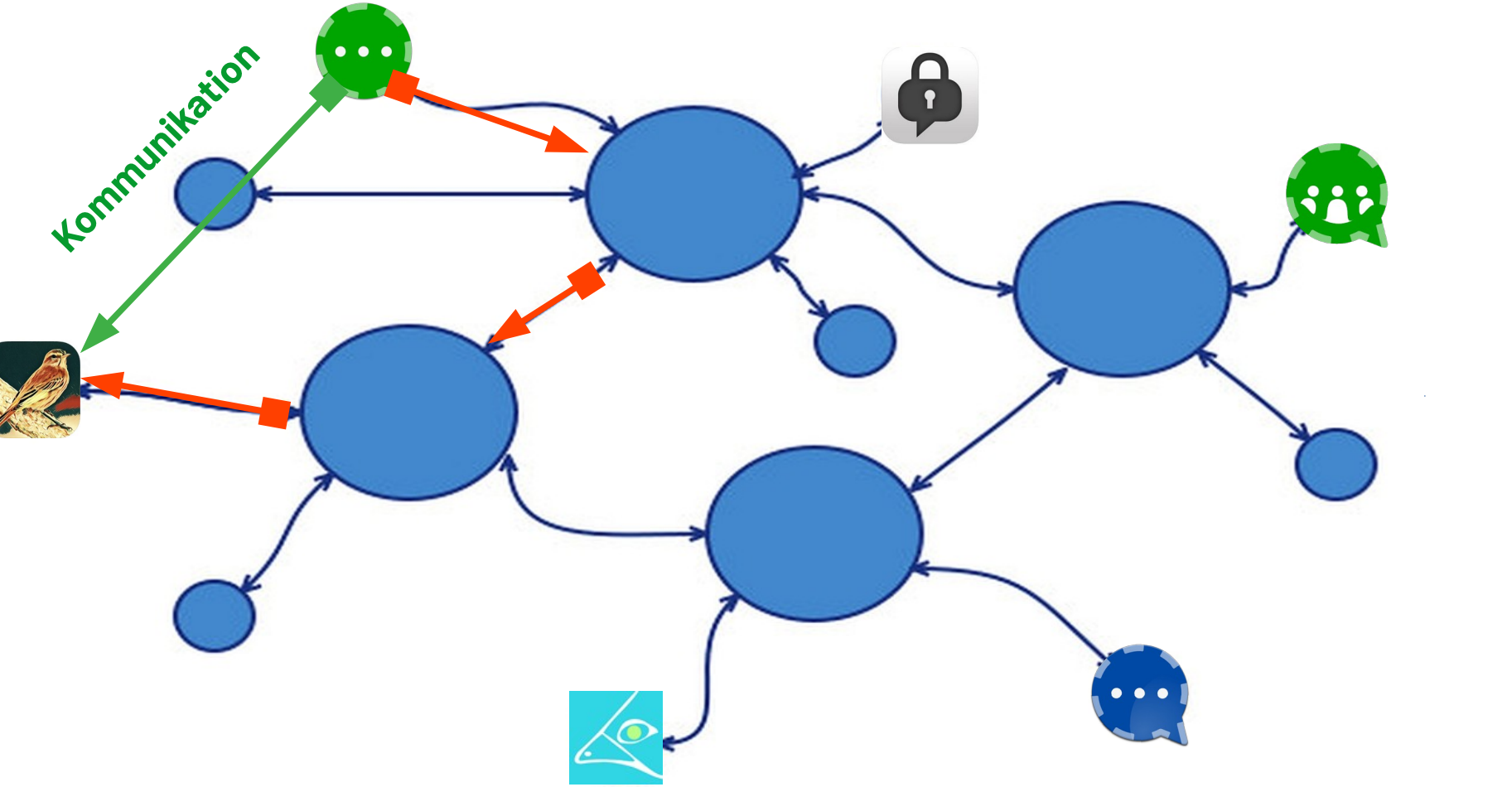

Dezentralisierung
XMPP
XMPP
XMPP

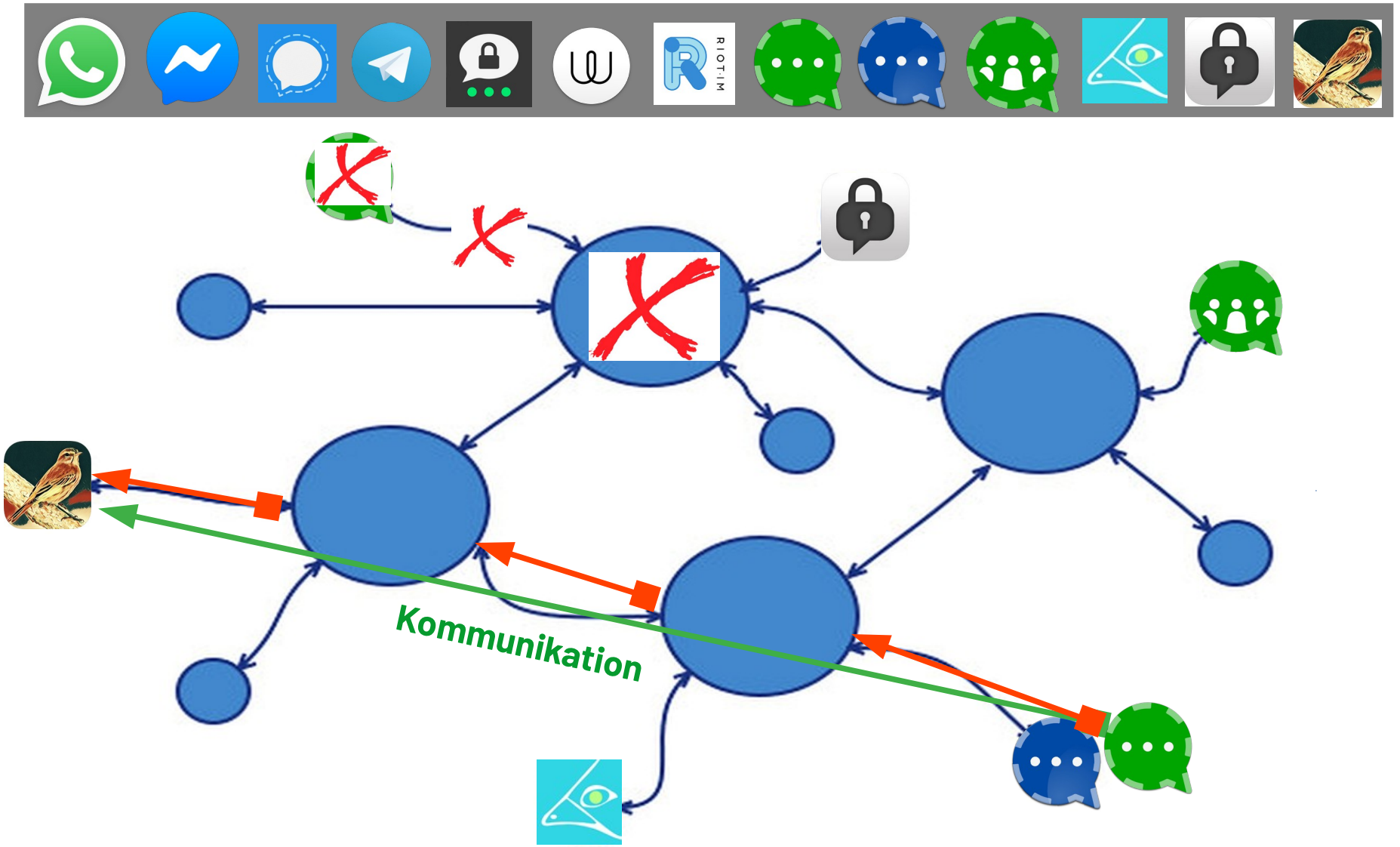


- Interessante Features: Zentralisierung vs. Dezentralisierung
  - Wer kommuniziert mit wem?
  - Was passiert beim Serverausfall?
    - Dann nutze ich einfach ein anderes Konto!



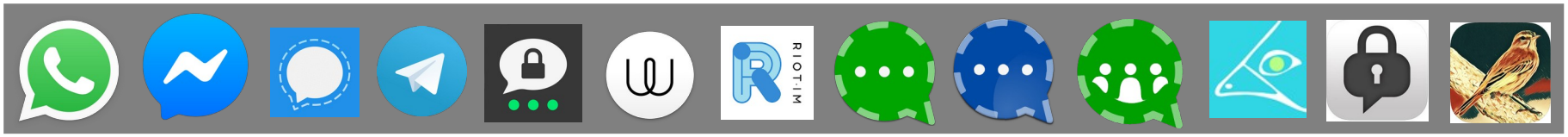



Kommunikation

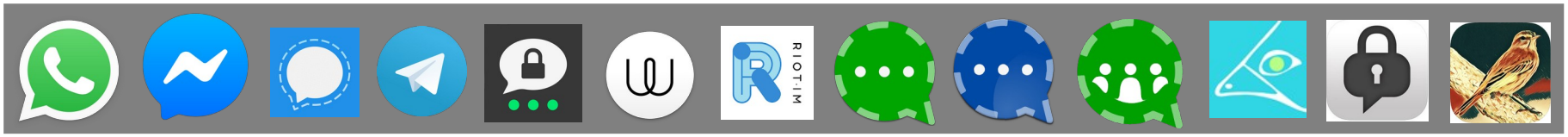

Kommunikation

- Interessante Features: Zentralisierung vs. Dezentralisierung
- **Das heißt:**
  - Proprietäre Messenger:
    - Bilden Insellösungen sog. „*Walled Gardens*“
  - Freie Messenger:
    - Können mit jedem kommunizieren, der ihre „Sprache“ (Protokoll) spricht
    - Fällt ein Server aus, nutze ich ein Konto auf einem anderen
  - Vereinzelt gibt es bereits sogar „Brücken“ zwischen den Protokollen

Was bleibt:



- Interessante Features: Geschäftsmodell der Anbieter
  - Was machen die Anbieterfirmen wirklich?
    - Zum Beispiel Whatsapp:
    - Beliebtester Messenger weltweit
    - Ende-zu-Ende-Verschlüsselung (??)
    - Eigene Auswertung von Nutzerdaten, auch mit Dritten
    - Lädt Adressbuch zur Mutterfirma hoch und unterstellt Zustimmung (auch aller Kontakte)
    - Telefonnummer als Identifier – Klarnamenpflicht

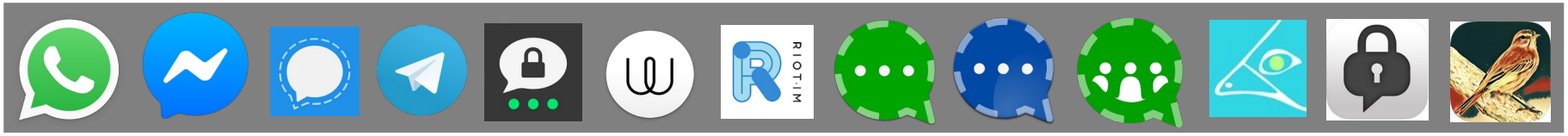


- Interessante Features: Geschäftsmodell der Anbieter
  - Was machen die Anbieterfirmen wirklich?
    - WhatsApp ist Teil der Facebook-Gruppe (USA; seit 2014)
    - Die Mutterfirma lebt vom Handel mit Nutzerdaten und -metadaten
    - z.T. auch ohne deren Wissen: wirbt z.B. auch im Namen von Nutzern („Peter gefällt…“)

- Möglichkeiten zur Verbesserung unserer Dienste. Wir analysieren, wie du WhatsApp nutzt, um sämtliche Aspekte unserer hier beschriebenen Dienste zu verbessern, u. a. indem wir Unternehmen, die WhatsApp nutzen, helfen, die Effektivität und Verbreitung ihrer Dienste und Nachrichten zu messen. Zu diesem Zweck verwendet WhatsApp die ihm zur Verfügung stehenden Informationen und arbeitet auch mit Partnern, Dienstleistern und

Adressbuch. Im Einklang mit geltenden Gesetzen stellst du uns regelmäßig die Telefonnummern von WhatsApp Nutzern und anderen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten.

Zustimmung zu unseren Nutzungsbedingungen („Bedingungen"). Du stimmst unseren Bedingungen zu, indem du dich registrierst oder unsere Apps, Dienste, Funktionen, Software oder Webseite installierst, nutzt oder auf diese zugreifst.



- Interessante Features: Fehlende Quelloffenheit
  - Was machen die Programme wirklich?
  - Was geschieht eigentlich mit den ***„Daten“***?

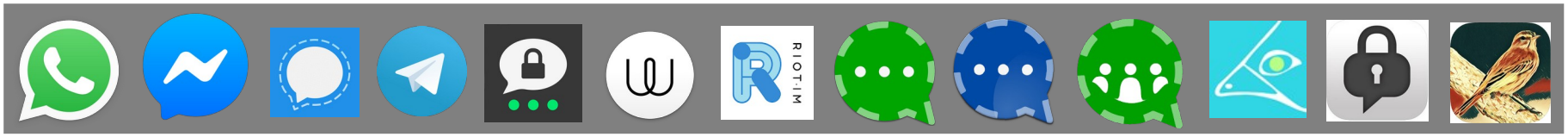
- We found that at least **61 percent of apps we tested automatically transfer data to Facebook the moment a user opens the app.** This happens whether people have a Facebook account or not, or whether they are logged into Facebook or not.

Was *sind* Daten?

- Daten sind Informationen in jeder Form:
  - Aussagen und Infos aller Art, über mich, andere oder anderes
  - Bilder / Selfies / Videos / Musik / Playlisten
  - Suchanfragen
  - Was ich in der Cloud speichere
  - Meine Telefonnummer und mein Name
  - …

Was *sind* Daten?

In our analysis, apps that automatically transmit data to Facebook share this data together with a unique identifier, the Google advertising ID (AAID). The primary purpose of advertising IDs, such as the Google advertising ID (or Apple's equivalent, the IDFA) is to allow advertisers to link data about user behavior from different apps and web browsing into a comprehensive profile. **If combined, data from different apps can paint a fine-grained and intimate picture of people's activities, interests, behaviors and routines, some of which can reveal special category data, including information about people's health or religion.** For example, an individual who has installed the following apps that we have tested, "Qibla Connect" (a Muslim prayer app), "Period Tracker Clue" (a period tracker), "Indeed" (a job search app), "My Talking Tom" (a children's' app), could be potentially profiled as likely female, likely Muslim, likely job seeker, likely parent.



- Interessante Features: Fehlende Quelloffenheit
  - Was machen die Programme wirklich?
  - Was geschieht eigentlich mit den ***„Daten“***?
  - … und was geschieht mit den ***„Metadaten“***?

Was *sind* Metadaten?

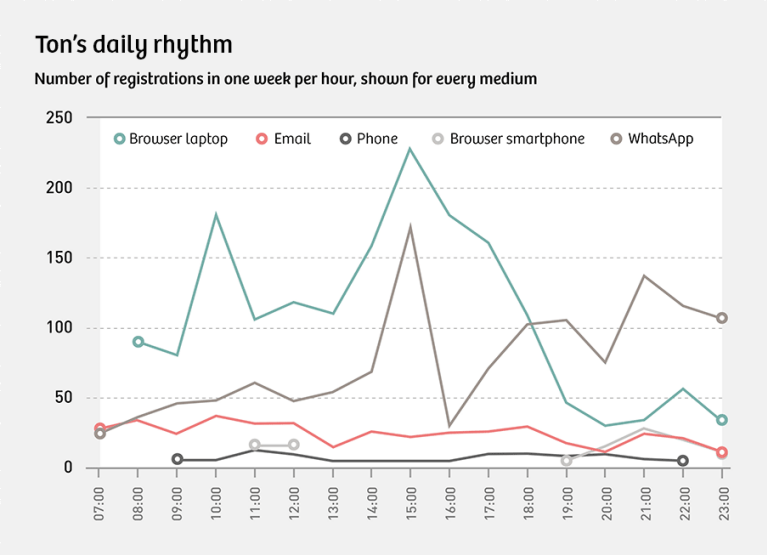
- ***Meta***daten: Daten, die ***über die Kommunikation*** anfallen, z.B.
  - Wer sendet / empfängt, mit wem?
  - Wo befinden sich beide?
  - Welche Webseiten suche ich von wo aus wann und wie lange auf, was mach‘ ich da, wohin surfe ich dann?
  - Wonach suche ich, einmal, öfters, immer wieder…
- Metadaten fallen ***immer*** auf den Servern an -

Kann ich denen immer vertrauen??

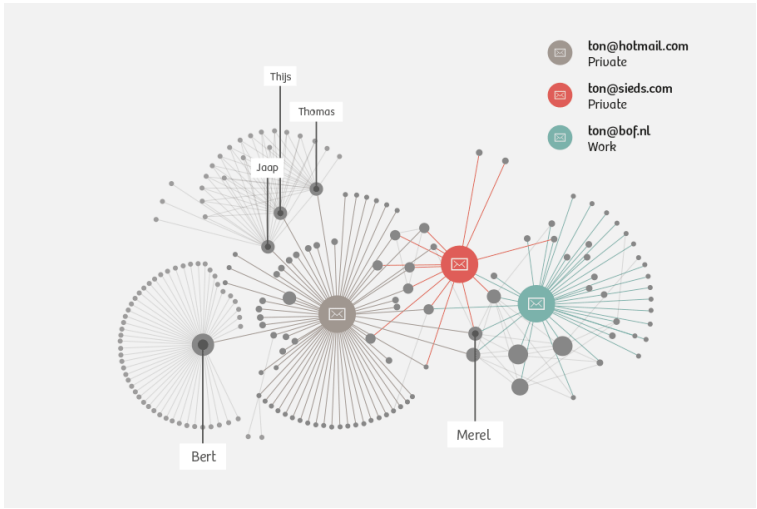
Metadaten

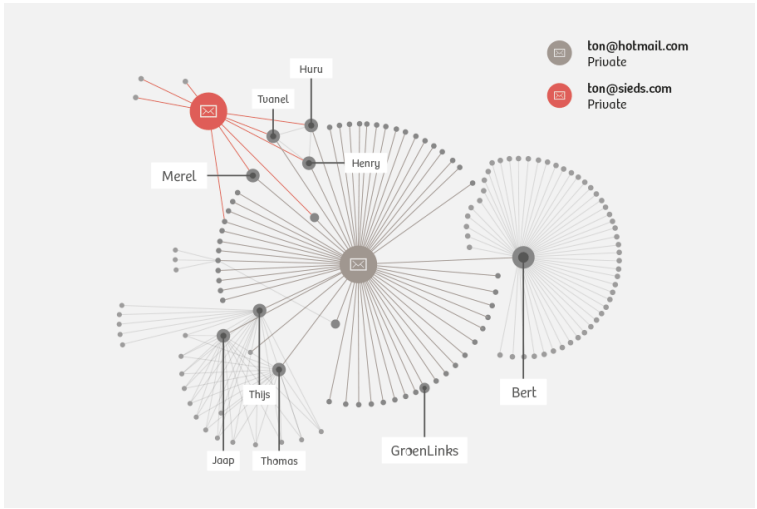
- Das Experiment von Ton Siedsma:
  - 15.000 Datensätze innerhalb nur einer Woche
  - Ton Siedmas Gerätenutzung
  - Ein Tag von Ton Siedsma:
  - Tons Freunde und Kollegen
- **Metadaten sind tödlich:**

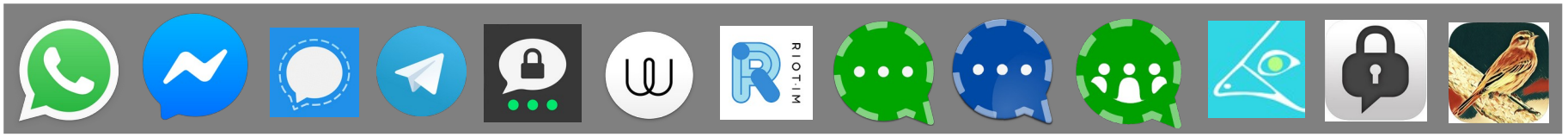
„We kill people based on Metadata!“


Ton's daily rhythm
Number of registrations in one week per hour, shown for every medium
Browser laptop
Email
Phone
Browser smartphone
WhatsApp
250
200
150
100
50
0
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00

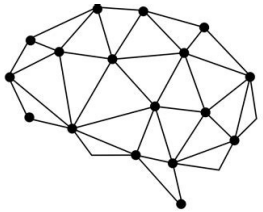

11:47
Looks online for a snuggle
14:53 - 16:15
64 Whatsapp messages to Merel and an unknown number
15:38
Phonecall from Hilversum Media Park 035-6775422
19:12
Leaves Hilversum and looks up an address on 9292.nu
10:06
Makes an appointment via email with the personal assistent of liberal MP Foort van Oosten.
20:46
Calls girlfriend Merel
21:04
Emails regarding the intern
22:21
Mails about a thesis on stealth sms technology
09:17
Reads The Guardian: US trade deal full frontal assault on democracy
08:00
Whatsapp to girlfriend Merel
01:06
Receives an email from his boss Ot van Daalen. Message: [Internal] Van Delden must go.
22:44
Reads an article about Anne Frank on news site nu.nl


ton@hotmail.com
Private
ton@sieds.com
Private
ton@bof.nl
Work
Thijs
Thomas
Joop
Bert
Merel


ton@hotmail.com
Private
ton@sieds.com
Private
Huru
Tuanel
Merel
Henry
Bert
Thijs
GroenLinks
Joop
Thomas

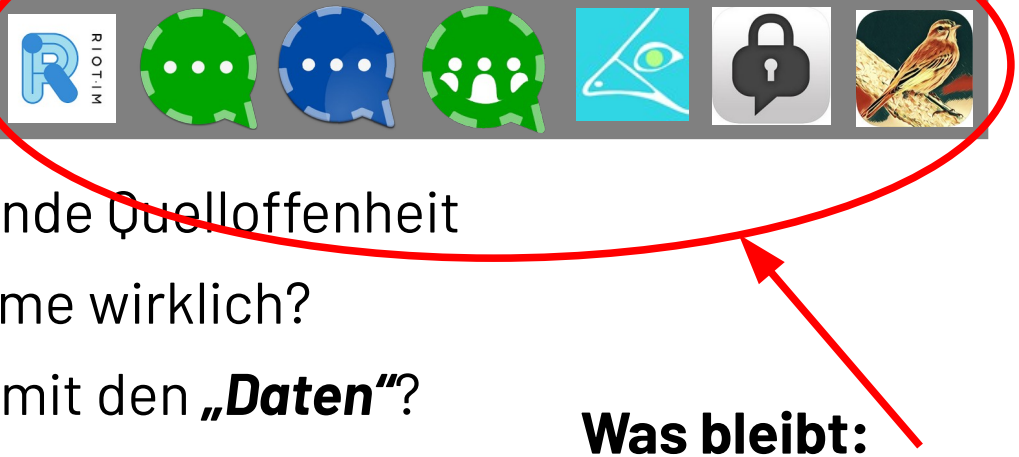


- Interessante Features: Fehlende Quelloffenheit
- **Fazit: Daten machen uns durchschaubar, Metadaten noch mehr!**
- Es gibt viele (Kauf-)Interessenten:



Cambridge
Analytica


Daten sind das Wasser
des 21. Jahrhunderts
(M. Kuketz)



- Interessante Features: Fehlende Quelloffenheit
  - Was machen die Programme wirklich?
  - Was geschieht eigentlich mit den ***„Daten“***?
  - … und was geschieht mit den ***„Metadaten“***?

Was bleibt:

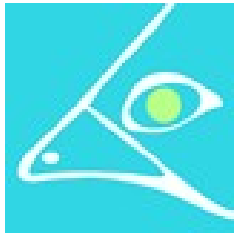
- **Fazit: Anonymität ist Persönlichkeitsschutz**
  - **Manche verhindern sie durch Identifizierung von Anfang an: Über die Telefonnummer oder den Klarnamen!**
  - **Manche brauchen zu viel Vertrauen (unfreie Software)**
  - **Manche brauchen zu viel Vertrauen (keine freie Serverwahl)**

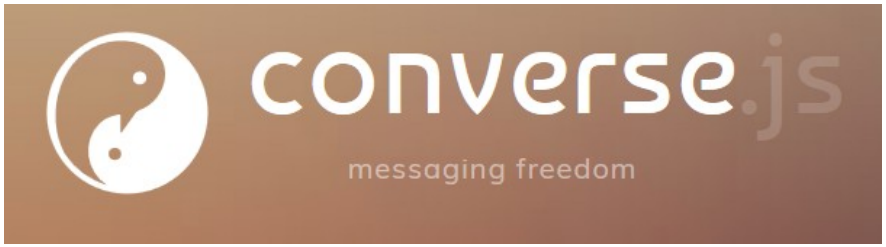
„Ich habe doch nichts zu verbergen“

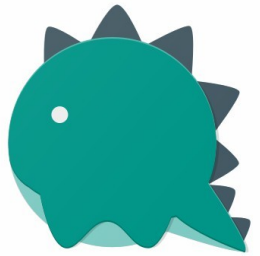
WIRKLICH NICHT?

- Machen Sie die Klotür hinter sich zu?
- Ist Ihr Privatleben ein Verbrechen?
- Wollen Sie erpressbar sein?
- Wollen Sie sich für die Zukunft gefährden?
- Wollen Sie, dass jemand alles über Ihre Kinder weiß?

Es bleiben für (halbwegs) sichere / privatsphärefreundliche Kommunikation im Alltag:







Ausgewählte Literatur und Webseiten

Verwendete und empfohlene Dokumente und Webseiten (Anmerkung: Dies ist keine wissenschaftliche Veröffentlichung. Die angegebenen Texte lassen sich leicht mit Hilfe einer Suchmaschine finden ;-)

- AppStore— und PlayStore-Abbildungen (diverse)
- Bitkom e.V.: Neun von zehn Internetnutzern verwenden Messenger
- Bitkom e.V.: Zahl der verschickten SMS sinkt um 40 Prozent
- BKA: Internetkriminalität/Cybercrime / Lagebild/Cybercrime
- Böse Überraschung: WhatsApp-Nutzerin findet fremde Chats auf neuem Handy, https://www.giga.de/apps/whatsapp-fuer-android/news/boese-ueberraschung-whatsapp-nutzerin-findet-fremde-chats-auf-neuem-handy/
- Dokumentation: Nackt im Netz https://www.youtube.com/watch?v=yGXb-ChrSFA
- How to track President Trump: https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html und verlinkte Webseiten
- Ingenieur.de: Trotz Verschlüsselung: Bei WhatsApp können Hacker kinderleicht mitlesen
- Kosner, Anthony Wing: Facebook Is Recycling Your Likes To Promote Stories You've Never Seen To All Your Friends
- Kuketz, Mike: Google scant bzw. analysiert E-Mails
- Kuketz-Blog: Abbildungen „Federation“ und „Zentralisation“
- Libert, Timothy: Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites, International Journal of Communication 9(2015), 3544–3561
- Löbbecke, Peter: Sichere Messenger für Polizisten, in: Deutsche Polizei 8/2019, S. 14-16
- Mehner, Matthias: Nutzerzahlen Messenger Apps Deutschland und Weltweit
- Netzpolitik.org: Tracking durch Drittanbieter auf einer Million Webseiten
- Netzpolitik.org: Metadaten: Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt
- Netzpolitik.org: Den Trackern auf der Spur: Forscher geben Einblick in die kommerzielle Überwachungsindustrie
- n-tv.de: Ortung im Supermarkt: Händler spüren ihren Kunden hinterher
- Privacy International: How Apps on Android Share Data with Facebook (even if you don’t have a Facebook account)
- Screenshots der jeweils erkennbaren Programme / Apps
- Temperton, James: tried to keep my unborn child secret from Facebook and Google | W... https://www.wired.co.uk/article/the-internet-hates-secrets?utm_mediu...
- We kill people: https://www.youtube.com/watch?v=3gJvABEi3wQ (Ausschnitt)
- WhatsApp Rechtliche Hinweise - https://www.whatsapp.com/legal/?l=de
- Zeyn, Martin: Niemand hat nichts zu verbergen
- diverse veröffentlichte Fotos ohne Quellenangabe/m.W. ohne Copyright

Ausgewählte Literatur und Webseiten

Wichtige Internet-Links:

- https://digitalcourage.de/
- https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-whatsapp-und-threema-instant-messenger
- https://www.freie-messenger.de/
- https://netzpolitik.org/
- https://www.fsf.org/de
- https://www.gesetze-im-internet.de/gg/BJNR000010949.html
- https://www.gnu.org/philosophy/free-sw.de.html
- https://www.researchgate.net/publication/332950252_Sichere_Messenger_fur_die_Polizei
- Nackt im Netz Intime Details von Politikern im Handel Panora.mp4 <project://163FE0CD116AAU9V5CKCK6DJ7DPDHF2LXX08/../../../dwhelper/Nackt%20im%20Netz%20Intime%20Details%20von%20Politikern%20im%20Handel%20Panora.mp4
- https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern
- https://www.orcas.de/whatsapp-facebook-skype-telegram-signal-threema-wire-viber-hangouts-icq-jabber-simsme-hoccer-yooyuu-discord-vergleich/ <https://www.orcas.de/whatsapp-facebook-skype-telegram-signal-threema-wire-viber-hangouts-icq-jabber-simsme-hoccer-yooyuu-discord-vergleich/#Signal
- https://matrix.orgbloghome.URL <project://163FE0CD116AAU9V5CKCK6DJ7DPDHF2LXX08/../../../../ALVISM~1/AppData/Local/Temp/httpsmatrix.orgbloghome.URL
- https://github.com/iNPUTmice/talks/blob/master/2019_08_10_-_state_of_the_xmpp_community.md
- https://www.orcas.de/whatsapp-facebook-skype-telegram-signal-threema-wire-viber-hangouts-icq-jabber-simsme-hoccer-yooyuu-discord-vergleich/
- https://netzpolitik.org/2018/die-ultimative-liste-so-viele-datenskandale-gab-es-2018-bei-facebook/
- https://f-droid.org/
- https://www.isode.com/markets/military-xmpp.html
- https://www.nato.int/docu/update/2007/pdf/majic.pdf

Herzlichen Dank!!!