Peter Löbbecke

Freie Messenger – Warum?

Eine (hoffentlich) verständliche, wenig technische Antwort,

verbunden mit einem Plädoyer.

Inhaltsverzeichnis

1. Hintergrund....2
2. Was ist die Freiheit der Freien Messenger?....4
3. Die Probleme Unfreier Messenger....5
   - 3.1. Beispiele Unfreier Messenger....6
   - 3.2. Problem: Nicht-offener (geheimer) Quellcode....6
   - 3.3. Problem: Zentralisierte Systeme....7
     - 3.3.1. Ende-zu-Ende-Verschlüsselung....8
     - 3.3.2. Daten vs. Metadaten....9
     - 3.3.3. Metadaten und zentrale Server....11
   - 3.4. Problem: „Geschlossene Systeme“ („Walled Gardens“)....11
   - 3.5. Problem: Eindeutige Nutzerkennung/-identifizierung....12
   - 3.6. Das besondere Facebook-WhatsApp-Problem....12
4. Die Vorteile Freier Messenger....14
   - 4.1. Der Freiheitsbegriff....14
   - 4.2. Gegenargumente....15
   - 4.3. Offener Quellcode....16
   - 4.4. Dezentrale („föderierte“) Systeme....17
   - 4.5. Offenheit....19
   - 4.6. Anonyme Nutzung ist möglich....20
5. Ein paar Grundlagen verschiedener *„wichtiger“* Systeme....20
   - 5.1. Freier Chat mit XMPP....21
   - 5.2. Matrix....23
   - 5.3. Peer-to-Peer und „Chatten via Email“....24
6. Ein Plädoyer....26
7. Anmerkungen siehe nächste Seite....27

Prof. Dr. phil. Peter Löbbecke („liberloebi“) ist Professor für Kommunikationswissenschaften an der Fachhochschule Polizei Sachsen-Anhalt in Aschersleben. Er kann über XMPP (S. 16) unter liberloebi@blabber.im erreicht werden.

1. Hintergrund

Die Covid-19-Pandemie hat eine Notwendigkeit zur Kommunikation „auf Abstand" geschaffen, die es vorher so noch nicht gab. Für viele Menschen bekam das Kommunizieren über das Internet auch im Privaten eine Qualität, die über den Austausch von Katzenbildern, Urlaubsfotos und privaten Grüßen deutlich hinausging – man konnte sich nicht persönlich treffen. Im Bildungsbereich gab es plötzlich – mit unterschiedlichem Erfolg und Qualität – Lernplattformen und Videounterricht sowie eine intensive Diskussion darüber, welche Systeme denn für Schüler[1.] geeignet seien (ich lasse die – wichtigen – Diskussionen über die Verfügbarkeit und den Zugang für finanziell schlechter Gestellte hier unbeachtet, sie gehören nicht zu meinem Thema). Eine große Rolle spielte und spielt die Frage nach der Sicherheit der persönlichen Daten der Schüler, der leider nicht überall die gebotene Aufmerksamkeit zukam.

Ein zentraler Bereich der Online-Kommunikation ist der Austausch über sogenannte Messenger. War lange Zeit der elektronische Brief, die Email, das herausragende Medium im Internet, so wurde sie schon vor einigen Jahren von „Instant Messengern" abgelöst (vgl. [2.]). Instant Messenger sind heute das mobile Kommunikationsmedium überhaupt, schnell, unkompliziert und relativ „locker" hinsichtlich der Umgangsformen. Dazu gibt es viele zusätzliche Funktionen, die die Kommunikation vereinfachen, komfortabler machen oder zusätzliche Möglichkeiten des Austauschs eröffnen, wie das Teilen von Fotos, Textnachrichten oder Dokumenten, das Senden von Sprachnachrichten, Videotelefonie und vieles andere. Messenger sind heute zu Allround-Kommunikationssystemen herangewachsen.

Der bekannteste und verbreitetste Messenger ist das zu Facebook gehörende WhatsApp[3.]. WhatsApp wurde im Jahr 2009 gegründet, im Jahr 2014 an Facebook verkauft und hat bis heute weltweit über 2 Milliarden Nutzer in über 180 Ländern[4.]. Seine größten scheinbaren Vorteile: Es ist kostenlos, und „jeder ist dabei". Allerdings stimmt das mit dem „kostenlos" nicht so ganz. Zur Zeit, als dieser Aufsatz geschrieben wird (Februar 2021), ist WhatsApp gerade (wieder einmal) in der öffentlichen Diskussion, da die Firma angekündigt hat, die Daten seiner Nutzer noch intensiver als bisher mit dem Mutterkonzern zwecks Auswertung und Kommerzialisierung zu teilen[5.]. Die Nutzer bezahlen also für die „kostenlose" Nutzung mit ihren persönlichen Daten. Dies ist jetzt schon so, auch wenn WhatsApp erklärt hat, den engeren Austausch mit Facebook (vorerst?) nicht auf den Bereich der DSGVO auszudehnen. Vielen, auch bisher enthusiastischen Nutzern, gefällt der Vorstoß überhaupt nicht; manche suchen nach Alternativen[6.]. Da WhatsApp so weit verbreitet ist, aus meiner Sicht aber auf keinen Fall empfohlen werden kann, habe ich mich mit ihm in einem eigenen Kapitel beschäftigt (Kapitel 3.6: Das besondere Facebook-WhatsApp-Problem).

Es kann kaum verwundern, dass Firmen wie WhatsApp oder Facebook Wege suchen und finden müssen, um Einnahmen zu erzielen; sie gehören zu den kommerziell wertvollsten Firmen der Welt, der Facebook-Gründer Mark Zuckerberg zu den reichsten Menschen[7.]. In der Tat sind sowohl WhatsApp als auch Facebook in der Vergangenheit immer wieder in

die Schlagzeilen geraten, weil sie sich in erster Linie über den Handel mit Nutzerdaten finanzieren[8]. Waren es zuerst kleinere Zirkel datenschutzbewusster Menschen, die sich über den Verbleib ihrer Daten und mögliche Folgen für sie selbst Sorgen machten, so wird spätestens seit Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) auch in der Öffentlichkeit intensiver über diese Tatsache diskutiert. Menschen suchen nach Möglichkeiten, von den großen kommerziellen Anbietern unabhängig zu werden, und werden auch fündig.

Bleiben wir im Bereich der Messenger. Einige der Alternativen haben bereits eine ansehnliche Verbreitung gefunden und werden auch von Laien als Ersatz für WhatsApp gerne genannt: Skype, Signal, Threema, Telegram und Wire dürften die bekanntesten sein; es gibt eine Vielzahl weiterer, meist weniger oder kaum bekannter Angebote wie etwa das inzwischen eingestellte Hoccer oder das sachsen-anhaltische Landesprodukt Chiffry. Alle Angebote besitzen die oben bereits erwähnten Funktionen und Zusatzeinrichtungen in unterschiedlichem Ausmaß, selbstverständlich haben auch alle – je nach Perspektive des Betrachters – ihre Vor- und Nachteile.

> Ich möchte an dieser Stelle ein Plädoyer für „Freie Messenger“ vorlegen, „frei“ nicht wie in „Frei***bier***“ als vielmehr wie in „Frei***heit***“. Da ich mit diesem Begriff etwas ganz Bestimmtes verbinde, verwende ich ***F***reie ***M***essenger (ebenso wie ***U***nfreie) hier als Eigennamen in Großschrift.

Die ganze Vielfalt Freier Messenger wird auf der Seite https://www.freie-messenger.de/ und ihren Unterseiten sehr übersichtlich, durchsuchbar und in verständlicher und möglichst wenig erklärungsbedürftiger Sprache dargestellt. Hier findet man auch u.a. eine „Schnellübersicht“ sowie einen Systemvergleich - nicht jedoch einen „Messenger“-Vergleich; dazu wird auf diverse externe Seiten verwiesen. Eine detaillierte tabellarische Übersicht, die aber keinesfalls vollständig ist, hält die Wikipedia bereit[9], eine weitere findet sich bei Mike Kuketz[10] bzw. mit zusätzlichen Erläuterungen hier[11]. In diesem Aufsatz versuche ich, aus Gründen der Lesbarkeit auch für nicht technisch interessierte Leser fortlaufend und lesbar zu schreiben; an vielen Stellen können Details, insbesondere solche technischer Art oder Quellenbelege, daher in den relativ umfangreichen Anmerkungen und beigefügten Links nachgelesen werden. Einige komplexe technisch interessante Details lasse ich einfach weg; wer sich dafür interessiert, findet wahrscheinlich in diesem Aufsatz sowieso wenig Neues.

2. Was ist die Freiheit der Freien Messenger?

Ich möchte mit ein paar grundlegenden Gedanken zu dem Begriff „Frei“ im Namen Freie Messenger beginnen.

Wenn heutzutage etwas „frei“ ist, dann assoziieren die meisten Menschen sicher ein kostenloses Angebot. Richtig ist, viele Freie Messenger sind (auch) „frei“ in dieser Hinsicht, sind aber, wie wir noch sehen werden, in vielfacher Hinsicht „freier“ als das scheinbar „nur *kosten*freie“ WhatsApp.

Frei kann in der deutschen (wie auch in der englischen) Sprache jedoch auch eine Bedeutung haben, die auf „Freiheit“ (Freedom) verweist. Freiheit bedeutet in diesem Sinne – bezogen auf Software und damit auch auf Messenger-Apps – vier „fundamentale Freiheiten“. Ein Programm ist gemäß der Definition der Free Software Foundation *dann* Freie Software, wenn die Nutzer die folgenden Freiheiten haben[12.] (wobei die ungewöhnliche Nummerierung von 0 bis 3 historische Gründe hat[13.]):

- **Die Freiheit, das Programm auszuführen wie man möchte, für jeden Zweck** *(Freiheit 0):*

  Damit sind die Bedürfnisse der Nutzer entscheidend für die Verwendung des Programms, nicht der Entwickler. Es darf keine Einschränkungen oder Vorgaben hinsichtlich des Einsatzes geben. Die Nutzer werden in keiner Weise bevormundet.

- **Die Freiheit, die Funktionsweise des Programms zu untersuchen und** eigenen Datenverarbeitungbedürfnissen **anzupassen** *(Freiheit 1)*. Der Zugang zum Quellcode[14.] ist dafür Voraussetzung.

  Das heißt, der eigentliche, menschenlesbare Programmcode muss öffentlich zugänglich sein. Auf diese Weise ist jeder Nutzer theoretisch in der Lage, eine eigene, auf die eigenen Bedürfnisse zugeschnittene Programmversion zu erstellen. Dies kann von ästhetischen (Farbe der Nutzeroberfläche) bis hin zu funktionellen (eigene Funktionen, Veränderung der Funktionsweise) Anpassungen gehen. Ganz entscheidend aber ist die Möglichkeit, den Quellcode zu *überprüfen*. Nur dann nämlich bin ich als Nutzer auch in der Lage, mich zu vergewissern, dass das Programm wirklich das tut, was es vorgibt, und nichts anderes (wie etwa meine Daten oder die Art meiner Nutzung des Programms an den Programmierer oder Anbieter weiterzuleiten). Nur Freie Software kann in letzter Konsequenz wirksam vor solchem Missbrauch schützen – nur Freie Software ist in letzter Konsequenz sicher!

  Natürlich sind die meisten Nutzer nicht in der Lage, solche Überprüfungen und Veränderungen selbst vorzunehmen; das machen häufig interessierte „Communities“[15.]. Darauf kommt es aber auch nicht an: Entscheidend für das Kriterium der „Freiheit“ ist die Möglichkeit dazu.

- **Die Freiheit, das Programm weiterzugeben und damit Mitmenschen zu helfen** *(Freiheit 2)*.

  Dies ist eine grundlegende Freiheit, denn wenn ich jemanden – etwa den ursprünglichen Programmierer – erst um Erlaubnis fragen muss, bevor ich Veränderungen vornehme und weitergebe – oder auch das ursprüngliche Programm –, verfüge ich nicht wirklich „frei" darüber.

- **Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben**, damit die gesamte Gesellschaft davon profitiert *(Freiheit 3)*. Der Zugang zum Quellcode ist dafür Voraussetzung.

  Hier wie auch in Freiheit 2 spielt der Community-Gedanke eine große Rolle: Software sollte nicht einem oder wenigen Menschen „gehören", sondern möglichst allen Menschen das Leben erleichtern. Freie Software „gehört" in diesem Sinne allen Menschen in gleichem Maße.

Bei genauerem Hinsehen fällt auf, dass die Freiheiten nicht davon sprechen, dass ein Programm kostenlos sein muss, um diese Kriterien zu erfüllen. Ein Entwickler kann durchaus etwa eine Gebühr verlangen, wenn jemand eine von ihm bereitgestellte Version erwirbt, es gibt Angebote für kostenpflichtigen Support und viele im weitesten Sinn „kommerzielle" Angebote mehr. Dann wird jedoch in der Regel eher eine Gebühr für eine Dienstleistung als für das Programm selbst fällig.

Wer sich mit der Materie noch nicht länger beschäftigt, mag in den oben genannten Freiheiten vielleicht eine eher idealistische, in der kommerziellen Welt wenig tragfähige Philosophie sehen; die Realität zeigt aber, dass es eine ganze Menge Freier und sehr erfolgreicher Software in diesem Sinne gibt. Außerdem implizieren die Freiheiten unterschiedliche Schutzfunktionen für die NutzerInnen Freier Software, auf die ich noch zurückkommen werde. Wichtig ist in diesem Zusammenhang vielleicht auch noch, dass die Datenschutzbeauftragten des Bundes und der Länder den Einsatz Freier Software ebenso befürworten[16] wie manche politischen Parteien[17].

Freie Messenger gehören zur Freien Software und sind ein wesentlicher Baustein für anbieterunabhängige und zukunftssichere Kommunikation; das Plädoyer für ihre Nutzung ist Thema dieses Aufsatzes. Doch schauen wir zunächst auf Unfreie Software und die Unfreien Messenger.

3. Die Probleme Unfreier Messenger

In der Einleitung habe ich auf die Datenschutzaspekte aufmerksam gemacht, die gerade im Schulbereich, bezüglich der persönlichen Daten von Schülern, eine große Rolle spielen und die Auswahl für den Lehrbereich geeigneter Software zu einem viel diskutierten Thema machen[18]. Konsequenterweise sollte dies auch für die Auswahl geeigneter Messenger gelten.

Nun gibt es keinen vernünftigen Grund, anzunehmen, dass die Daten von Schülern *stärker bedroht* wären, als die von Erwachsenen. Der Unterschied liegt vielmehr darin, dass Erwachsene für den Schutz ihrer Daten gegebenenfalls selbst verantwortlich sind und bei ihnen in den meisten Fällen auch eher ein informiertes Verständnis dessen vorausgesetzt werden darf, was mit ihren Daten passiert (ob das dann wirklich vorliegt, ist eine andere Frage). Die Gefahr der Nutzung, Verwertung, Kommerzialisierung, Verbreitung usw. der Daten durch Dritte ist dieselbe.

Die Frage, die an dieser Stelle immer wieder auftaucht, ist: Ist denn das wirklich so schlimm? Schließlich habe ich doch nichts zu verbergen, ich begehe keine Straftaten, und ob ein Algorithmus jetzt ein paar Daten von mir auswertet, spielt doch wirklich keine Rolle: „Die wissen doch eh' schon alles über mich". Diese Frage ist schon so oft beantwortet worden, dass ich an dieser Stelle darauf verzichten will und lieber auf andere verweise[19]; ich möchte nur darauf hinweisen, dass das, was jeder zu verbergen hat, die eigene *Privatsphäre* ist, die niemanden etwas angeht. Nicht umsonst steht die Unverletzlichkeit der Wohnung unter besonderem grundgesetzlichem Schutz; nicht umsonst schweigen wir über unsere Kontostände; niemand gibt Kreditkarten-PINs an Fremde heraus; und jeder macht hoffentlich die Klotür hinter sich zu.

Jeder Nutzer von Messengern (und anderer Software) sollte sich bewusst sein[20]: Digitale Kompetenz oder Internet-Kompetenz bedeutet nicht in erster Linie, Programme bedienen zu können. Sie bedeutet vor allem, sich darüber im Klaren zu sein, was für Spuren ich im Netz hinterlasse und wer diesen Spuren folgen könnte!

3.1. Beispiele Unfreier Messenger

Freie Messenger spielen beim Thema Daten- und Privatsphäreschutz aus meiner Sicht eine besondere Rolle. Doch wo liegt überhaupt das Problem mit den Unfreien Messengern? Es gibt ja nicht nur WhatsApp, über dessen Verbreitung ich oben schon geschrieben hatte. Immer wieder wird über eine Vielzahl von Alternativen zu WhatsApp geschrieben und gesprochen. Namen, die dabei fallen könnten, sind zum Beispiel *Skype, Signal, Threema, Telegram, Wire* und einige andere. Ein vollständiger Überblick ist nicht Gegenstand dieses Aufsatzes, und Vollständigkeit wird auch an keiner Stelle behauptet. Ich möchte aber diese Beispiele heranziehen, um deutlich zu machen, inwieweit die Gefahr besteht, die eigenen Daten (vielmehr sich selbst und andere) durch ihre Nutzung zu kompromittieren. Die nachfolgenden Aspekte, die ich als Probleme ansehe, treffen auf die genannten Beispiele in jeweils unterschiedlichem Ausmaß zu, und sicher auch auf viele andere Systeme, die nicht extra aufgeführt werden.

3.2. Problem: Nicht-offener (geheimer) Quellcode

Bei vielen Unfreien Systemen ist der Quellcode nicht offengelegt (vgl. unter Punkt 2 aufgeführte 4 Freiheiten). Die Nutzer können in solchen Fällen – selbst bei vorhandenem Fach-

wissen – nicht überprüfen, ob der Messenger wirklich das tut, was er verspricht, oder ob an irgendeiner Stelle Funktionen eingebaut wurden, die Daten oder andere Informationen (s.u.) für die Zwecke des Anbieters verwenden. Beispiele dafür gibt es genug[21.]; auch WhatsApp-Chats waren offenbar trotz der Ende-zu-Ende-Verschlüsselung nicht immer sicher vor dem Mitgelesen-Werden[22.], und sind es möglicherweise bis heute nicht[23.].

Lange Zeit war das seit 2011 der Firma Microsoft gehörende System Skype sehr beliebt für die spontane Kommunikation. Bereits sehr früh bot der „Urvater der Videochat-Funktion“[24.] die Möglichkeit zur Video-Telefonie. Das System war kostenfrei (außer für den kommerziellen Gebrauch), leicht zu installieren und zu bedienen. Es versprach immer schon Verschlüsselung der Nutzerinhalte und Schutz vor dem Zugriff böswilliger Nutzer.

Im Jahr 2013 fanden Sicherheitsforscher allerdings heraus, dass Microsoft sich selbst Zugriff auf Textnachrichten von Skype-NutzerInnen verschafft hatte und offenbar routinemäßig solche Nachrichten scannte[25.]. Möglicherweise waren solche Zugriffe Teil eines von Microsoft eingerichteten Sicherheitssystems[26.] und damit „gut gemeint“; die Möglichkeit, überhaupt die Kommunikation von Nutzern in dieser Weise auf bestimmte Inhalte hin scannen zu können, zeigt prinzipiell, dass die Verschlüsselung nicht undurchdringbar ist. Und eine Verschlüsselung, die von einer Instanz „geknackt“ werden kann, kann prinzipiell auch von anderen, außenstehenden Parteien gebrochen werden[27.].

Dieses für viele stehende Beispiel zeigt die Notwendigkeit, Programmcode – in diesem Fall insbesondere den für die Verschlüsselung zuständigen Teil – von unabhängiger Seite prüfen zu können. Nur dann kann nämlich sichergestellt werden, dass vollmundige Versprechungen eines Anbieters (hier Microsoft) über die Funktionsweise und Sicherheit eines Produkts auch wirklich den Tatsachen entsprechen. Das ausführbare Programm bietet keine Möglichkeiten zu so einer Überprüfung.

Außer Skype ist auch WhatsApp nicht quelloffen, bei anderen Beispielen sind unter Umständen nur die Anwender-Apps (Clients), nicht jedoch die Server-Systeme quelloffen.

3.3. Problem: Zentralisierte Systeme

Alle oben (S. 6) genannten Angebote lassen die Kommunikation der Nutzer über die firmeneigenen Server laufen. Sie machen damit ein Angebot, das schwerlich auszuschlagen ist: Es muss schließlich eine Stelle geben, an der die „Anschrift“ des Empfängers gelesen wird, damit die Nachricht zugestellt werden kann, und das ist der Server des Anbieters. Es entsteht ein Eindruck, wie er von der Post bekannt ist: Ich werfe meine Briefe in einen öffentlichen Briefkasten, jemand holt sie ab, stempelt die Briefmarke und schickt sie an die Adressen, die ich auf die Umschläge geschrieben habe. Für zentralisierte Messenger, deren Nutzer oft viele Kommunikationspartner haben, sieht das so aus (und ich danke Mike Kuketz für die Erlaubnis, dieses Bild und das auf S. 18 zu verwenden)[28.]. Jeder der kleinen blauen Punkte (Messenger) schickt seine Botschaften (Texte, Bilder, Dokumente, Sprach-

nachrichten, Anrufe,...) an den großen blauen Punkt (den Server des Anbieters); von dort wird sie an den richtigen kleinen blauen Punkt weitergeschickt:

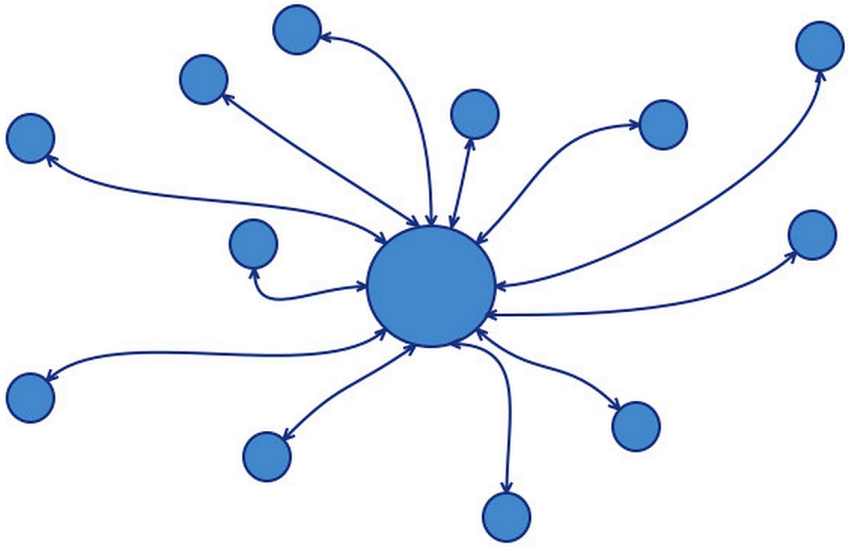

Abbildung 1: Schema der Funktionsweise zentralisierter Systeme

Damit kontrolliert der Anbieter den Datenfluss zwischen den kommunizierenden NutzerInnen. Aber ist denn das wirklich ein Problem? So gut wie alle Messenger verfügen doch heute über eine *Ende-zu-Ende-Verschlüsselung*, sie werben sogar damit und reklamieren besondere Datensicherheit für sich. Aber stimmt das wirklich?

3.3.1. Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung bedeutet genau das, was der Name besagt: Eine „Vorrichtung“, die die zu sendende Nachricht (Text, Bild, Video, ...) auf dem Gerät des Absenders (erstes „Ende“) so verschlüsselt, dass unterwegs niemand mehr Zugriff auf den *Inhalt* hat, bis er auf dem Gerät des Empfängers (zweites „Ende“) wieder entschlüsselt wird. Zu den technischen Grundlagen will ich hier keine Ausführungen machen, das würde im Kontext zu weit führen. Einige Verschlüsselungsverfahren gelten unter Fachleuten als besonders sicher, wie z.B. die von Signal verwendete Verschlüsselung[29], die auch von einigen anderen freien und unfreien Messengern verwendet wird. Andere Verschlüsselungen gelten als zweifelhaft, wie etwa die von Telegram[30]. Telegram fällt darüber hinaus durch eine ganze Reihe von Unsicherheitsfaktoren auf[31], etwa dadurch, dass hier die Verschlüsselung ausdrücklich eingeschaltet werden muss, was unter Umständen, etwa bei ungeübten Nutzern oder in Eile, auch vergessen werden kann, wodurch die eigentlich nicht einsehbare Kommunikation unter Umständen kompromittiert wird.

Auch für eine Verschlüsselung gilt übrigens, was ich bereits oben zur Offenlegung des Programmcodes geschrieben habe. Verschlüsselung beruht auf mathematischen Prinzipien. Sicherheit entsteht nicht dadurch, dass das Verfahren der Verschlüsselung geheim ist; werden an dieser Stelle schwache Verfahren eingesetzt, so kann durch entsprechenden technischen Aufwand die Verschlüsselung mehr oder weniger schnell (maschinell) gebrochen werden (Kerckhoffs Prinzip[32.]). Deshalb ist es wichtig, auch den Programmcode des Verschlüsselungssystems zur Überprüfung freizugeben, denn nur dann kann eingeschätzt werden, wie stark die Verschlüsselung wirklich ist. Das Verschlüsselungsverfahren von Signal erfüllt beispielsweise die Voraussetzung der Offenheit, was bei WhatsApp nicht gegeben ist.

In der Tat haben die meisten Messenger-Systeme Vorkehrungen getroffen, die die Daten ihrer Nutzer so verschlüsseln, dass die Anbieter selbst keinen Zugriff darauf haben (eben mit „Ende-zu-Ende-Verschlüsselung“). Wie ich im letzten Kapitel gezeigt habe, setzt das bei geheimem (unfreiem) Programmcode zunächst einmal ein Vertrauen darauf voraus, dass die Anbieter wirklich das umsetzen, was sie versprechen.

Nun legen manche Anbieter den Quellcode ihrer Clients und der Server-Software durchaus offen; von den Genannten können Signal und Wire, seit Ende 2020 auch Threema, als Beispiele dienen. Sie bieten darüber hinaus eine Ende-zu-Ende-Verschlüsselung; die von Signal gilt, wie gesagt, als besonders sicher und ist zum Standard auch für andere (auch Freie) Systeme geworden (vgl. hierzu auch die Schnellübersicht von Messengersystemen). Dennoch können auch solche Messenger nur mit Einschränkungen empfohlen werden. Offen bleibt nämlich immer noch die Frage nach den sogenannten *Metadaten*.

3.3.2. Daten vs. Metadaten

Den meisten Menschen ist aus der alltäglichen Unterhaltung, den Nachrichten und von vielen anderen Gelegenheiten der Begriff „*Daten*“ bekannt und vertraut. Was damit genau gemeint ist, fällt zu erklären schon schwerer. Dabei ist es eigentlich ganz einfach: *Jedwede* Information lässt sich als „Daten“ verstehen; kaum etwas kann *kein* „Datum“ sein. Dass dabei häufig an elektronische Kommunikation gedacht wird, ist eigentlich nicht richtig: Der Übertragungsweg von Daten spielt keine Rolle, im Gespräch werden ebenso Daten übermittelt wie beim Telefonieren, beim Chatten oder beim Schreiben von Aufsätzen. Daten können also die unterschiedlichsten Formen annehmen:

- als Aussagen über mich, über andere, über etwas;
- sie können Bilder und Fotos, Selfies, Videos, Musik, Playlisten und vieles mehr sein;
- Liebesbriefe und -schwüre, Erzählungen aus dem Urlaub und über die Kinder, den Chef, Ehefrau oder -mann;
- Namen, Telefonnummern, Adressen, Kontostand, Gehaltsbetrag, Schuldenstand,

- Passwörter und PINs, …
- … und vieles, vieles mehr.

Um solche Informationen sorgen wir uns in der Regel, wir möchten nicht, dass sie in falsche Hände geraten, sie sind privat und vertraulich.

„*Metadaten*“ hingegen sind vielen kaum ein oder gar kein Begriff; sie sind „Daten über Daten“, also Informationen, die über Aktionen anfallen, hier über Aktionen im Internet, wie etwa eine Suche, eine Mail oder einen Chat. Metadaten sind für verschiedene Zwecke wichtig (ich beschränke mich auf Beispiele aus der Kommunikation): Eine Adresse ist erforderlich für die Zustellung einer Nachricht, ein Absender ist erforderlich, um Antworten zu können (und um den Absender gegebenenfalls zuverlässig identifizieren zu können, ein Sicherheitsmerkmal), sie können unseren Standort enthalten, die Dauer der Kommunikation, zu ihnen gehört auch die Häufigkeit, mit der ich jemanden anschreibe, und vieles mehr[33]. Quasi: „Wer kommuniziert wann, wie oft, wie lange mit wem (oder auch nicht)“.

Diese scheinbar so harmlosen Informationen (schließlich stehen auch auf dem Briefumschlag Anschrift und Absender!) sind es, die auf den Servern immer anfallen. Sie sind für den technischen Betrieb erforderlich. Und beim Brief waren sie in der Tat auch relativ unerheblich, mit ein paar Ausnahmen: Wer wollte schon gern, dass der Absender des Erotik-Versenders auf dem Päckchen zu lesen war, das vom Nachbarn angenommen wurde?

Im Zeitalter von „Big Data“[34] haben die Metadaten allerdings eine ganz andere Bedeutung bekommen. Sie lassen sich nämlich zu Nutzerprofilen verbinden, die eine Vielzahl von Rückschlüssen über die Person zulassen, die sie erzeugt. Insbesondere in Verbindung mit eindeutigen Kennzeichnungen (etwa Googles Advertising ID oder Apples Äquivalent, dem Identifier for Advertisers, IDFA) lassen Metadaten sehr schnell mit Hilfe geeigneter Algorithmen meine Vorlieben und Abneigungen erkennen: Sie fallen bei allen meinen Aktivitäten im Internet an. Erweitert werden sie um die Netze aus meinen Kontakten, die wiederum in andere Netze eingebunden sind, und so weiter. Mithilfe von „Tracking-Technologien“ ist es kein Problem, auch andere Aktivitäten im Internet in diese Netzwerke einzubinden, so dass sehr schnell große Datensätze entstehen, die Aufschluss über die NutzerInnen bis hin zu deren Religion, politischen und sexuellen Vorlieben, Unterhaltungsinteressen, detailliertem Beziehungsstatus und vielem mehr geben[35]. Metadaten können sogar tödlich sein – der ehemalige Direktor von CIA und NSA, Michael Hayden, sagte es freimütig: „We kill people based on metadata“[36] („Wir töten Leute auf Grund von Metadaten“). Es dürfte kaum ernsthafte Zweifel daran geben, dass solche Profile für eine Vielzahl von Interessenten von Bedeutung sind, wobei die Werbeindustrie noch die harmloseste, weil in der Regel[37] „nur nervig“, sein dürfte. Aber wenn mein Wählerverhalten auf dieser Basis manipuliert wird[38], wenn mein „sozialer Wert“ ermittelt und daraus Konsequenzen gezogen werden[39] oder wenn meine Krankenkasse meinen Lebenswandel analysiert, um meine Prämien zu berechnen, oder Schlimmeres[40], dann sieht die Sache anders aus.

3.3.3. Metadaten und zentrale Server

Und damit sind wir zurück beim Ausgangsproblem, dem der zentralisierten Systeme. Auf dem Server des Anbieters fallen Metadaten nämlich unweigerlich an, und als Nutzer muss ich sie dem Anbieter bedingungslos anvertrauen. Viele Anbieter legen offen, welche Metadaten für welche Zwecke erhoben und verwendet werden; eine Kontrolle ist nicht möglich. Selbst wenn Clients und Serversoftware quelloffen sind und von der Öffentlichkeit geprüft werden können, müssen die Nutzer sich immer noch darauf verlassen, dass genau diese Software auch wirklich in der Firmenzentrale läuft und dass die erhobenen Metadaten wirklich nur für die angegebenen Zwecke genutzt, nicht weitergegeben, nicht mit Nutzerprofilen verknüpft und nicht dauerhaft gespeichert oder verkauft werden. In der Regel sind das statistische Zwecke und das Bemühen um eine Verbesserung der Dienstleistungen, also durchaus ehrenwerte und nachvollziehbare Zwecke. Aber: Eine Kontrolle ist eben nicht möglich.

3.4. Problem: „Geschlossene Systeme“ („Walled Gardens“)

In vielen Ländern der Welt gibt es Gärten, die von Mauern umschlossen sind. Wahrscheinlich waren viele dieser Gärten ursprünglich einmal aus Sicherheitsgründen ummauert worden; heute dienen die Umfriedungen in der Regel eher gartentechnischen Zwecken wie der Erschaffung von Mikroklimata[41], etwa zur Erhöhung der Temperatur im Garten, um ansonsten ungeeignete Pflanzen anbauen zu können – und natürlich dazu, unerwünschte Pflanzen draußen halten zu können.

Auch die Angebote zentralisierter Messengerdienste ähneln einem umschlossenen Garten. In dieser Hinsicht ist ein „Walled Garden“ also ebenfalls ein umschlossenes Ökosystem mit allen Vor- und Nachteilen. Der Anbieter stellt sämtliche Regeln auf. Er schreibt vor, welche Werkzeuge zu benutzen sind – hier sind das die Messenger-Apps, von denen es je System in der Regel nur eine gibt, die dann eben verwendet werden muss. Es ist egal, ob man damit zurecht kommt oder nicht, bzw. ob sie die Funktionen bietet, die man möchte, oder auch nicht. Die „Pflanzen“, die wachsen dürfen, werden vom Anbieter ebenfalls reguliert, d.h. Vorschriften zu Inhalten müssen eingehalten werden. Das treibt manchmal die merkwürdigsten Blüten: Im Jahr 2016 entfernte Facebook das weltberühmte, mit dem Pulitzer Preis ausgezeichnete Foto der 9-jährigen Kim Phuc bei ihrer Flucht vor einem Napalm-Angriff während des Vietnamkrieges, weil es gegen seine Gemeinschaftsregeln über Nacktheit verstieß. Ein Sturm der Entrüstung ging durch die Weltpresse[42].

So, wie empfindliche Pflanzen nur innerhalb der Mauern wachsen können und andere meist zu Unkräutern erklärt werden, die „draußen“ bleiben müssen, so können auch bei geschlossenen Messengersystemen nur Angebote innerhalb des „Ökosystems“ genutzt werden: Man ist „bei“ WhatsApp, „bei“ Telegram, „bei“ Signal oder „bei“ Threema. Nutzergruppen müssen sich im eigenen Biotop ansiedeln (man muss „beitreten“), oder man hat keinen Zugriff. Kommunizieren kann ich nur mit Partnern, die auch „bei“ meinem Dienst

sind. Interoperabilität, also die Möglichkeit, mit Nutzern anderer Dienste in Kontakt zu treten, ist nicht vorgesehen, nicht möglich und üblicherweise von den Anbietern auch nicht gewünscht. Schließlich ist die Zahl der Nutzer, die dem eigenen Dienst vertrauen, immer auch ein – vermeintliches – Zeichen für Qualität und Zuverlässigkeit, vielleicht auch ein Identifikationsmerkmal. Nicht selten spielen auch kommerzielle Interessen eine Rolle, beispielsweise, wenn der Anbieter erweiterte Angebote für Firmenkunden gegen Entgelt zur Verfügung stellt. Beispiele, die hier schon genannt wurden, sind Skype, Threema und Wire. Aber auch der Gedanke und das Ziel, eigene Zahlungsplattformen mit anzubieten und damit Geld zu verdienen, so wie das bei einigen großen Konzernen geplant und in der Umsetzung ist, gehören hierhin. Produktbindung ist das Ziel. Forderungen nach einer Öffnung, wie sie im Jahr 2018 beispielsweise von Bundesjustizministerin Katarina Barley gegenüber WhatsApp erhoben wurden[43], laufen daher üblicherweise ins Leere. Walled Garden-Messenger errichten virtuelle Mauern um ihre Nutzer herum, in denen diese gefangen sind.

3.5. Problem: Eindeutige Nutzerkennung/-identifizierung

Manche Unfreie Messenger zwingen ihre Nutzer, ihre Telefonnummer oder E-Mailadresse zur Anmeldung und/oder Identifikation preiszugeben („*Identifier*“). Wieder mag mancher denken: Diese Daten haben doch viele Menschen, was soll’s, und wieder liegt die Antwort in den neuartigen, im Alltag oft kaum vorstellbaren Möglichkeiten zur Verarbeitung großer Datenmengen. Könnte man sich für eine Anmeldung per Email noch einer sogenannten Wegwerf-Email-Adresse[44] bedienen, die nach dem Anmeldevorgang ungültig wird und eine Identifikation somit unmöglich macht, so ist das bei einer Telefonnummer nicht möglich: Wenn man die Landesvorwahl einbezieht, dann ist die Nummer ein *weltweit einmaliges* Erkennungsmerkmal. So, wie ich es oben schon für Werbe-Kennungen von Mobiltelefonen beschrieben habe (S.10), kann auch die Telefonnummer zur Grundlage eines Nutzerprofils werden, in das beliebige Informationen problemlos und zu beliebigen Zwecken eingefügt werden können. Auch wenn es möglich ist, sich in innerhalb der App einen beliebigen Namen (Alias / Spitzname / „*nickname*“) zu geben, so ist letztlich in Bezug auf Privatsphäre und Datenschutz anonymes Chatten unmöglich. Der Anbieter kann jederzeit die bei ihm anfallenden Metadaten mit der Telefonnummer und damit mit einem eindeutigen „Identifier“, also einer ganz bestimmten Person, verbinden. **Damit werden Nachverfolgung, der Nachvollzug von Freundeskreisen und vieles mehr möglich, was ich oben schon beschrieben habe.**

3.6. Das besondere Facebook-WhatsApp-Problem

WhatsApp ist im Zusammenhang mit Daten- und Privatsphäreschutz in den letzten Jahren mehrfach negativ in die Schlagzeilen geraten; seine Nutzer sind in besonderem Maße Gegenstand der Nachverfolgung und der Kommerzialisierung ihrer Daten[45]. Die Suche nach Alternativen ist *ein* Auslöser für diesen Aufsatz, wie ich eingangs geschrieben habe. Da es einen großen, für den Geltungsbereich der DSGVO nicht ganz ersichtlichen Teil seiner ge-

sammelten Daten mit der aktuellen Mutterfirma Facebook teilt und Facebook vermutlich die größeren Datenverarbeitungskapazitäten besitzt, lohnt es sich, Facebook immer mit im Hinterkopf zu haben.

Die Firma WhatsApp Inc. bedient sich aber nicht nur großzügig an den Daten der WhatsApp-Nutzer, es zwingt diese auch, ihre Kontakte zu kompromittieren, indem es regelmäßig deren Telefonbücher von den Mobiltelefonen herunterlädt[46]. In einem Gerichtsurteil wurde bereits klargestellt, dass das ein Problem für die WhatsApp-Nutzer darstellen kann: Denn die Weitergabe der Daten all dieser Kontakte ist nur mit deren Zustimmung zulässig[47]. Doch seit der Veröffentlichung dieses Urteils gilt erst einmal weiter: Wo kein Kläger, da kein Richter …

Wehren kann man sich gegen diese Eingriffe nicht, wenn man den Dienst nutzen will, dann muss man die Bedingungen anerkennen[48]. WhatsApp hält mit der exzessiven Nutzung der Daten seiner Nutzer nicht hinter'm Berg; ein Blick in die AGB zeigt eindeutig, dass sowohl Daten erhoben[49] als auch ausgewertet[50] als auch an Dritte weitergegeben[51] werden.

Mit Hilfe der Kontaktdaten kann WhatsApp/Facebook weitere Verknüpfungen herstellen und nicht nur das Nutzerprofil des/der jeweiligen Nutzers/in immer weiter verdichten und um Bezüge zu anderen Profilen erweitern, sondern auch die Profile der so gewonnen Kontakte werden weiter ausgebaut, nämlich um die soziale Nähe zu allen, deren Angaben sich im gerade hochgeladenen Telefonbuch befinden. Interessen werden verknüpft, Bezüge zwischen den Inhalten der Telefonbücher aller anderen werden aufgebaut und analysiert …

Um die Bedeutung dieser Aussage klar zu machen, ist es nötig, auf einen Umstand hinzuweisen, der wenigen Internet-Nutzern bewusst ist. WhatsApp/Facebook (und auch andere) beziehen ihre Daten keineswegs nur aus dem, was die Nutzer in dem Sozialen Netzwerk eingeben und was an (Meta-) Daten beim Chatten anfällt. Viele Webseiten enthalten Facebook-Tracker, und viel mehr als die Hälfte der Apps im Google-Play Store sendet Daten über das Verhalten der Nutzer an Facebook[52]. Es dürfte kaum einen Internet-Nutzer geben, dessen Daten *nicht* von dieser Firma (und anderen, allen voran Google[53]) ausgewertet und zu Geld gemacht werden.

Das kann im Einzelfall schlimme Folgen haben. So wurden Fälle bekannt, in denen Sexarbeiterinnen über die Verbindung ihrer verschiedenen von Facebook erzeugten Nutzerprofile ihren privaten Bekannten und Familien gegenüber sozusagen „geoutet" wurden, obwohl sie für die Arbeit und das Privatleben zwei streng getrennte Facebook-Auftritte angelegt hatten. Dadurch können nicht nur Peinlichkeiten entstehen, sondern unter Umständen ganz konkrete Gefährdungen[54].

WhatsApp stellt trotz der Datenschutz- und Privatsphärebedenken eine hohe Hürde gegenüber einem möglichen Umstieg auf andere Systeme auf, denn: „Jeder ist bei WhatsApp". Und in der Tat sind fast ein Drittel aller Menschen auf der Welt Nutzer des Messengers[55]. Es fällt schwer, Freunde, Familie oder auch neue Bekanntschaften zu bitten, einen anderen

Dienst zu nutzen, wenn doch „alle“ WhatsApp haben. WhatsApp ist bequem, angeblich „sicher“, überall verbreitet, hat viele Funktionen, ist scheinbar kostenlos – eine „eierlegende Wollmilchsau“. *Ein Umstieg oder auch eine parallele Nutzung anderer Messenger erfordern einen Aufwand – und Einsicht in die Notwendigkeit.*

Andererseits: Es lohnt sich, einen Blick in die eigene Kontaktliste zu werfen und nachzuzählen, mit wie vielen Kontakten man wirklich regelmäßig wichtige persönliche Informationen austauscht. In den meisten Fällen dürften das sehr viel weniger Personen sein, als man zuerst meint. Aus meiner Sicht sollte einem die eigene Privatsphäre und der Schutz der Menschen, die einem nahestehen, die Mühe wert sein.

4. Die Vorteile Freier Messenger

Im Zusammenhang mit der Diskussion um Freie Messenger sind die obigen Punkte vielfach diskutiert worden. Nicht alle Punkte sind völlig unumstritten: So hält etwa der Entwickler des Messengers Signal, Matthew Rosenfeld (alias „Moxie Marlinspike“), Zentralisierung für ein Merkmal, das es durchaus zu verteidigen gilt[56]. Ob man solchen Argumenten folgen will, muss natürlich jeder Nutzer selbst entscheiden; dieser Aufsatz steht unter der Prämisse, dass vermeidbare Kompromisse vermieden werden sollten, da sie immer das Ziel des Schutzes persönlicher Daten und der Privatsphäre schwächen. Daher wird hier nachdrücklich für den Einsatz Freier Systeme plädiert. Freie Messenger sind zwar nicht in jedem Fall *kosten*frei, sie werden aber auf keinen Fall mit den Daten der Nutzer bezahlt. Ich möchte daher im Folgenden die oben skizzierten Nachteile Unfreier Messenger jetzt mit ihren Gegenstücken aus der Welt der Freien Messenger kontrastieren. Zunächst jedoch ein paar Gedanken zum Freiheitsbegriff, wie er m.E. durch Freie Software im Allgemeinen, also auch und besonders durch Freie Messenger im Speziellen verwirklicht wird.

Im Kapitel 5 werde ich auf einzelne Systeme etwas genauer eingehen, die m.E. von einiger Bedeutung sind.

4.1. Der Freiheitsbegriff

In einer Gesellschaft wie der unsrigen, die sich grundsätzlich auf die Freiheit des Individuums aufbaut, soweit das gegenüber der Gesellschaft möglich ist (wobei Einschränkungen unserer Freiheiten durch das Grundgesetz prinzipiell unter Gesetzesvorbehalt und in enge Grenzen gestellt sind), sind Einflussnahmen auf die Kommunikation eigentlich nicht hinnehmbar. Es gibt ein Telefon- und Briefgeheimnis (Art. 10 GG), und sehr schnell würde ein Anbieter dieser Dienste vom Markt verschwinden oder vom Staat in seine Schranken gewiesen, der etwa vorschreiben wollte, dass bestimmte Inhalte *nicht* in Briefe oder Telefonate gehören. Nicht einmal der Staat selbst darf ohne nachgewiesene triftige Gründe in den Austausch auf diesen Wegen eingreifen (jedenfalls, wenn es nach Recht und Gesetz geht).

Genau das tun aber manche Anbieter, oder sie haben wenigstens die Möglichkeit dazu, wie ich oben beschrieben habe. Skype scannt Nachrichten, Facebook zensiert Inhalte – vielleicht tun das auch andere? Allein die Möglichkeit dazu ist ein Verstoß gegen die „Freiheit 0“ (S. 4) und, wie ich meine, auch gegen die grundsätzliche und grundgesetzliche Ordnung unserer Gesellschaft.

4.2. Gegenargumente

Nun werden, soweit ich sehen kann, vor allem zwei Gegenargumente vorgebracht, auf die ich hier kurz eingehen will: Es steht jedem frei, einen **Vertrag** einzugehen, in dem sich der Betroffene entsprechenden Regelungen unterwirft. Nichts anderes ist die Nutzung eines Unfreien Messengers in letzter Konsequenz, wenn ich die Nutzungsregeln akzeptiere[57].

Dagegen ist nicht viel zu sagen, selbstverständlich steht das jedem frei. Nur: Warum sollte ich freiwillig meine Möglichkeiten einschränken lassen, wenn es gleichwertige Alternativen gibt, die das nicht erfordern? Warum sollte ich meine grundgesetzlich verbriefte Freiheit zur Kommunikation ohne Not und ohne eine höherwertige Notwendigkeit als dem Interesse eines Messengeranbieters einschränken lassen? Da ich nicht weiß, über welche Themen ich zukünftig einmal kommunizieren will oder muss, gehe ich mit so einem Vertrag ein großes, vielleicht *zu* großes Risiko ein.

Zum anderen könnte man einwenden, dass die Einschränkungen auf hochwertige moralische Ziele und die Verhinderung von ***Straftaten*** zielen. Auch dieses Argument für eine Einschränkung von Freiheit in der Kommunikation zieht m.E. nicht. Moral ist ein System aus Normen, Werten, Handlungsvorschriften u.ä., die sich in einer pluralen Gesellschaft gerade *nicht* verallgemeinern und damit für alle verbindlich setzen lassen. Moral an sich ist normativ (Regeln setzend), aber eine einheitliche, verbindliche Moral für alle Mitglieder unserer *pluralistischen* Gesellschaft gibt es nicht – sonst gäbe es z.B. keine Kirch*en* (Plural), keine konkurrierenden Parteien auf der Basis jeweils verschiedener Werte und vieles mehr. An die Stelle einer solchen Einheitsmoral ist in einer pluralen Gesellschaft das *Recht* getreten, das sozusagen den Minimalkonsens einer Gesellschaft mit Platz für unterschiedliche Moralvorstellungen festlegt, um sicherzustellen, dass deren Träger sich nicht gegenseitig an die Gurgel gehen.

Auf politischer Ebene wird sehr häufig nach einer Einschränkung der Kommunikationsfreiheit zur Verhinderung von Straftaten gerufen. So steht gerade aktuell die starke Verschlüsselung von Messengerdiensten in der Diskussion. Vordergründig ist das Bedürfnis der Sicherheitsbehörden durchaus nachvollziehbar: Kann ich auf die Chats von Straftätern zugreifen, dann habe ich vielleicht alle Fakten, um ihre Taten zu vereiteln und sie zu festzunehmen. Doch dieser Gedanke hat einen Haken: Um Straftaten *zu verhindern*, muss man bereits im Vorfeld wissen, wer sie begehen wird[58] – nur dann kann man *überhaupt* mithilfe der Gesprächsinhalte oder Texte präventiv tätig werden. Anderenfalls muss man *alle* Gespräche und Chats *aller* erreichbaren Menschen mitschneiden und speichern, um *im*

Nachhinein Straftaten *aufklären* zu können[59]. Eine solche Vorratsdatenspeicherung ist aber kaum verfassungsgemäß[60] und damit unzulässig. Will man die Gespräche/Texte lediglich zur Nachweisführung aufbewahren, so sind sie in der Regel nicht mehr besonders hilfreich, weil es bereits genug andere Beweise aus der Straftat gibt. Will man anhand von Kommunikationsvorgängen Täter suchen, so impliziert das wieder, dass man ständig und für unabsehbare Zeit *jeden* Austausch zwischen Menschen mitschneidet und speichert, weil man ja nicht weiß, wann eine Straftat begangen wird – ein terroristischer Anschlag wie der auf das World Trade Center braucht vielleicht ein paar Jahre Vorbereitungszeit! Damit wären wir wieder bei der unzulässigen Vorratsdatenspeicherung – die im Übrigen den Anschlag auf das World Trade Center nicht verhindert hätte.

Aus meiner Sicht sind also beide Argumente nicht wirklich stichhaltig. Schauen wir uns daher an, welche Antwort Freie Messenger auf die oben dargelegten „Probleme" der Unfreien Systeme geben.

4.3. Offener Quellcode

Freie Messenger sind zwangsläufig solche, deren Programm- bzw. Quellcode öffentlich einseh- und veränderbar ist. Dies ergibt sich ursächlich aus den Anforderungen an Freie Software (nicht nur Messenger), die ich oben beschrieben habe (S. 4, die *4 Freiheiten*). Damit stehen sie der Überprüfung ihrer Funktionsweise durch Menschen mit entsprechender Sachkenntnis offen. Es kann sichergestellt werden, dass die Messenger auch wirklich das – und nur das! - tun, was sie vorgeben. So weit, so gut.

Nun haben auch einige Anbieter Unfreier Systeme den Quellcode Ihrer Apps, und manchmal auch der Server-Software, offengelegt und zur Überprüfung freigegeben. Bekannte Beispiele sind Signal, Wire und – seit kurzem – Threema. Dennoch sind diese Systeme nicht frei, denn 2 der o.g. Freiheiten sind nicht erfüllt: Die Möglichkeit zur Anpassung an eigene Bedürfnisse und die Freiheit zur Verbesserung. Dass diese Freiheiten durchaus eine Rolle im Alltag spielen, zeigt sich in der Freie-Messenger-Welt am Beispiel des Messengers Conversations.

Conversations ist ein Messenger, der für seine Funktion den XMPP-Standard nutzt, ein international standardisiertes „Protokoll", das Funktionen zur Datenübermittlung im Internet festlegt; ich komme darauf später noch zurück. Er hat sich seit seiner ersten Veröffentlichung 2014 eine recht solide Nutzerbasis erworben: Allein im Google Play Store wurde die App zwischen 100.000 und 500.000 Mal abgerufen[61], dazu kommt eine Vielzahl von Installationen über den alternativen Store F-Droid. Der Quellcode von Conversations wurde von seinem Entwickler unter einer Freien Lizenz veröffentlicht.

Da der Quellcode Frei ist, besteht die Möglichkeit, auf seiner Basis eine eigene Variante / Abspaltung – einen sogenannten „Fork" – herzustellen, also das ursprüngliche Programm weiterzuentwickeln und mit neuen oder veränderten Funktionen neu zu veröffentlichen. Genau dies geschah ebenfalls schon im Jahr 2014, in dem der Conversations-Abkömmling

„Pix-Art“ (heute „blabber.im“) veröffentlicht wurde. Das geschah, um verschiedene Vereinfachungen und – aus Sicht des Pix-Art-Entwicklers – Optimierungen vor allem in der Benutzerführung in das Programm einzubauen[62]. Im Austausch mit vielen Nutzern wurde zum Beispiel die Nutzeroberfläche des Programms anders gestaltet, einige Funktionen wurden verändert oder neu hinzu entwickelt. Beide Apps koexistieren heute und bedienen Nutzergruppen mit unterschiedlichen Anforderungen an das System. Darüber hinaus gibt es weitere Projekte, die auf der Codebasis von Conversations basieren oder sie integrieren. Ein sehr bekanntes Beispiel hierfür ist Snikket.

Alles das wäre mit proprietären Messengern nicht zulässig und wahrscheinlich auch nicht möglich gewesen, prüft doch die Server-Software unter Umständen, ob es sich bei der Anwendungssoftware um das firmeneigene Original handelt[63]. Ich werde später nochmals auf das Beispiel Conversations noch zurückkommen.

4.4. Dezentrale („föderierte“) Systeme

Echte Freie Systeme schreiben ihren Nutzern nicht vor, bei welchem Anbieter sie ihre „Basis“, ihr „Konto“ haben müssen. Habe ich bei WhatsApp und den anderen geschlossenen Systemen keine andere Wahl, als meine Nachrichten über den einen Firmenserver zu leiten, so ist das bei Freien Messengern nicht der Fall. Technisch interessierte können sogar mit geringem Aufwand ihren eigenen Chatserver betreiben und trotzdem mit allen anderen plaudern.

Wir kennen das dahinterliegende Prinzip vom Telefon und der E-Mail: Dort kann sich jeder Kunde den Anbieter aussuchen, der ihm am besten gefällt, die besten Zusatzangebote macht oder den besten Preis bietet – oder den für den Kunden besten Kompromiss aus diesen. Rufe ich jedoch einen Teilnehmer eines anderen Anbieters an, so ist das für mich völlig transparent, in der Regel weiß ich nicht einmal, wo mein Gesprächspartner Kunde ist. Bei der E-Mail ist der Anbieter normalerweise über die E-Mailadresse erkennbar, aber ansonsten ist das Prinzip dasselbe. Wir alle würden sehr erstaunt aus der Wäsche schauen, wenn man uns – analog zu den firmeneigenen Messengern – auffordern würde, den Telefonanbieter zu wechseln, um mit der Oma oder dem Chef telefonieren zu können.

Bei Freien Messengern kann sich jeder Nutzer einen Dienste-Anbieter (= Serverbetreiber) aussuchen und sein Konto dort anlegen. Der Austausch mit anderen TeilnehmerInnen ist völlig problemlos, solange ich deren Adresse besitze – wie bei der E-Mail. Die Struktur ist sogar dieselbe: name@server.xyz.(also .de, .org, .net. com, usw.). Die Server kommunizieren in der Regel transparent miteinander, so dass die Nutzer von der automatischen Weiterleitung ihrer Nachrichten nichts mitbekommen. Die einzige Voraussetzung ist: Die Server müssen die selbe Sprache (dasselbe Protokoll) benutzen, also beispielsweise XMPP (s.o.)– Briefe muss ich der Post oder einem ihrer Konkurrenten übergeben. In der Übersicht sieht das so aus:

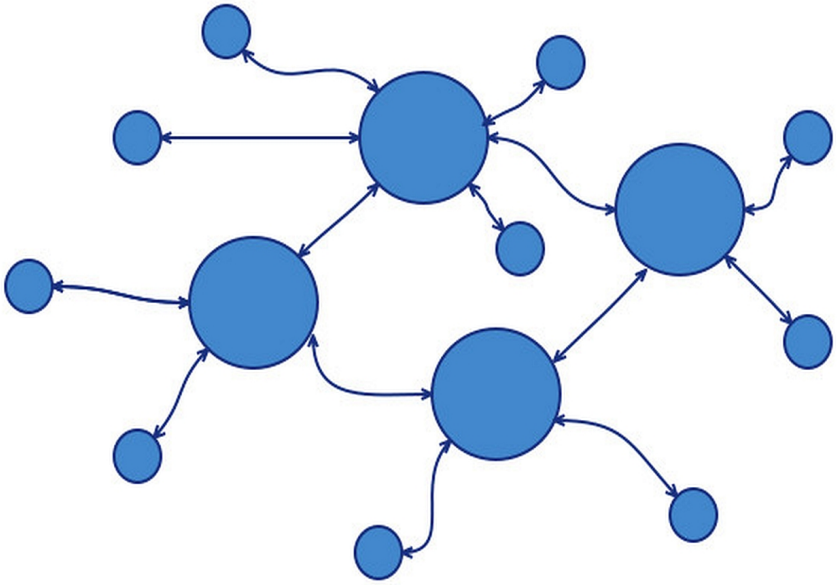

*Abbildung 2: Schema der Funktionsweise **de**zentraler Systeme*

Ein Nutzer sendet mit seiner Chat-App oder Messengerprogramm (einer der kleinen blauen Punkte) schickt seine Botschaften (Texte, Bilder, Dokumente, Sprachnachrichten,…) an *seinen* Diensteanbieter / den Server, dem er/sie hinsichtlich der Metadaten vertraut (großer blauer Punkt; siehe auch den nächsten Absatz!); von dort wird die Nachricht an den Anbieter (Server) des Empfängers (ebenfalls als großer blauer Punkt dargestellt) weitergeschickt. Dieser leitet die Nachricht dann letztendlich an den „richtigen" Empfänger (wieder ein kleiner blauer Punkt) weiter.

Es ist sogar möglich (wenn auch technisch nicht Versierten nicht unbedingt zu empfehlen), sich einen eigenen Server in die Wohnung zu holen oder als Firma oder Organisation einen eigenen Chatserver im IT-Bereich zu betreiben. Muss man bei einem externen Anbieter noch dem Serverbetreiber hinsichtlich der Metadaten vertrauen, so ist man bei einem eigenen Server vollständig Herr darüber, was aufgezeichnet, gespeichert und so weiter wird - also genauso wie bei E-Mail. Dem Austausch mit anderen Servern mit demselben Protokoll sind prinzipiell keine Grenzen gesetzt. Metadaten fallen immer an, da sonst eine „Zustellung" der Nachrichten nicht möglich wäre; sie zu kontrollieren oder sich einen vertrauenswürdigen Serverbetreiber statt eines anonymen Großbetriebes aussuchen zu können – z .B. einen, der Metadaten regelmäßig und häufig löscht – bedeutet aber einen großen Schritt in Richtung Privatsphäre- und Datenschutz. Eine starke, geprüfte Ende-zu-Ende-Verschlüsselung wie das schon erwähnte Signal-Protokoll oder das beim eben erwähnten Conversations und blabber.im verwendete OMEMO[64] (das ebenfalls diese Verschlüsselung verwendet) sorgt dafür, dass die Inhalte auch auf dem Empfänger-Server nicht gelesen werden können, sondern ausschließlich vom Empfänger.

4.5. Offenheit

Freie Messengersysteme sind keine abgeschottete Gärten, sondern lassen frischen Wind durch ihr Ökosystem pfeifen. Ähnlich wie bei der E-Mail gibt es keine Vorschriften, was oder wie kommuniziert werden darf. Dass möglicherweise auch sittenwidrige oder gar kriminelle Inhalte dabei sein können, ist ein Risiko, das im selben Maße auch bei anderen Kommunikationsformen wie der Briefpost und beim Telefon auftritt. Niemand kontrolliert irgendwelche Inhalte oder stellt Regeln auf (oder liest gar die Inhalte während der Übertragung mit, was durch eine grundsätzliche Transportverschlüsselung und den Einsatz der empfohlenen Ende-zu-Ende-Verschlüsselung gewährleistet wird). Für die öffentliche Kommunikation, etwa in Nutzergruppen, gelten selbstverständlich die allgemeinen Rechtsvorschriften/Gesetze, ebenso wie überhaupt alle anderen Gesetze gelten. Das Urheberrecht etwa ist sowenig aufgehoben wie bei der Kommunikation per Brief. Auch wenn ich selbst Dienstleistungen, Informationen, Diskussionsforen oder anderes in die Öffentlichkeit bringen will, brauche ich mich nicht an die Vorgaben eines Anbieters zu halten, der meine Inhalte kontrolliert: Jeder, auch Behörden, Organisationen oder Institutionen können ihre eigene Infrastruktur zur Verfügung stellen („hosten“).

Einer der für Privatanwender wohl wichtigsten Aspekte ist aber die Freiheit, sich eine Messenger-App oder ein Messengerprogramm auszusuchen, die/das den eigenen Bedürfnissen am ehesten entspricht. Auch hier greift wieder die Analogie zur E-Mail: Der eine verwendet Mozilla Thunderbird, die andere liest ihre E-Mails online[65], und für beide ist die verwendete Methode unerheblich. Genauso kann sich jeder aus einem Angebot für sein Gerät die passende App aussuchen. Für Android-Smartphones könnten das – für den XMPP-Standard – z.B. Conversations, blabber.im, Quicksy (ebenfalls eine Conversations-Variante) und möglicherweise noch weitere sein. Für Apples iPhones gibt es derzeit vor allem die Auswahl zwischen Monal, Siskin und dem teilweise schon etwas angestaubten ChatSecure. Bei der Nutzung von Windows-oder Linux-Computern kann auf Gajim zurückgegriffen werden oder auch eine Browserlösung genutzt werden. Und alle diese verschiedenen Chat-Apps/-Programme (und es gibt noch einige mehr) können ungehindert und transparent miteinander kommunizieren - sie unterscheiden sich lediglich hinsichtlich der Möglichkeiten der Apps bzw. deren Entwicklungsstand.

Ein anderer Freier Standard ist das Matrix-Protokoll, das jüngeren Datums ist als das bereits gut etablierte XMPP. Demzufolge gibt es noch nicht so viele Messenger-Apps; bekannt ist die App Element (früher Riot), die es für verschiedene Plattformen (Betriebssysteme) gibt. Aber auch hier gelten grundsätzlich die gleichen Prinzipien. Bei Matrix liegt der Fokus mehr auf Ausfallsicherheit und etwas weniger auf Datenschutz. Freiheit und die Wahrung der Privatsphäre sind bei beiden Systemen sehr gut möglich.

4.6. Anonyme Nutzung ist möglich

Mag auch mancher Nutzer von klassischen Messengersystemen fälschlicherweise davon ausgehen, nichts zu verbergen zu haben, so ist Anonymität gegenüber Kommunikationspartnern im Internet doch ein wichtiger Baustein des Schutzes wenn vielleicht nicht der Person, so doch der Privatsphäre. Bei freien Systemen gilt: Wenn nicht bekannt ist, wer gerade agiert, dann können die anfallenden Daten auch nicht einem bestimmten Persönlichkeitsprofil zugeordnet werden. Wenn ich an öffentlichen Diskussionsgruppen, („multi-user-chats“) und ähnlichem teilnehme, dann möchte ich unter Umständen selbst dann anonym bleiben und nur unter einem Pseudonym auftreten, wenn die Inhalte, um die es geht, völlig legal sind – wer das nicht nachvollziehen kann, denke etwa an Diskussionsrunden zu verschiedsten Themen (oft zu Hobbies), Forenähnliche Chaträume, den Wochenmarkt oder auch die Anonymen Alkoholiker oder an die Weight Watchers. Nicht jeder möchte in einer Gruppe von ansonsten fremden Menschen ihr Alkoholproblem oder sein Übergewicht mit dem realen Namen verbunden wissen. Dass politische Dissidenten oder auch Journalisten unter autoritären Regierungen Anonymität benötigen, um ihre Arbeit, ihre Freiheit und unter Umständen sogar ihr Leben zu schützen, versteht sich von selbst; jedoch sollen solche extremen Situationen nicht im Zentrum dieses Aufsatzes stehen. Für Journalisten und Aktivisten gibt es sogar noch weiterreichende Lösungen (aber mit weniger Komfort).

Freie Messenger erlauben grundsätzlich die Nutzung ohne ein eindeutiges Identifizierungsmerkmal („Identifier“) (S. 12). Verantwortlich ist nämlich der Betreiber des Servers, auf dem die Nutzer ihr Konto einrichten. Schreibt ein Serverbetreiber eine entsprechende Angabe von personenbezogenen Daten vor, so steht es mir frei, mich für einen anderen Anbieter zu entscheiden – oder eben, wie oben schon dargelegt, meinen eigenen Server aufzusetzen.

Einige der proprietären Lösungen und zentralen Anbieter (z.B. Threema) erlauben die Erstellung eines NutzerInnenkontos ohne die Angabe einer Telefonnummer oder E-Mail-Adresse; diese Angaben sind unter Umständen optional, um überhaupt bestimmte Programmfunktionen erst nutzen zu können. Für die Funktion eines anbieterunabhängigen (freien) Messengers sind solche Angaben unerheblich.

5. Ein paar Grundlagen verschiedener „*wichtiger*“ Systeme

Ich möchte jetzt noch auf einige Systeme, die aus meiner Perspektive von besonderer Bedeutung sind, etwas näher eingehen. Dabei ist mir klar, dass je nach Einsatzszenario, Sicherheits- und Sicherheitsbedürfnissen die Entscheidung darüber, was ein „wichtiges“ System ist, anders ausfallen muss. Meine Auswahl stellt deshalb keinerlei (Ab-)Wertung der hier nicht aufgeführten Systeme dar.

Hier ist m. E. auch der richtige Ort, noch einen weiteren wichtigen Hinweis unterzubringen. Bisher habe ich den Begriff „Sicherheit“ unhinterfragt verwendet, um den Text nicht unnötig kompliziert zu machen. Generell ist immer auch „Sicherheit“ selbst zu hinterfragen. Es können darunter total unterschiedliche Dinge verstanden werden, wie z.B. unter https://www.freie-messenger.de/einfuehrung ausgeführt wird. Auch spezielle „Sicherheits“-Funktionen wie z.B. sogenannte „selbstzerstörende Nachrichten“ können je nach Sichtweise und Anforderung durchaus unterschiedlich (positiv oder negativ) bewertet werden. Vielfach wird nämlich nur eine scheinbare „Pseudosicherheit“ suggeriert (wichtige Beispiele finden sich unter https://www.freie-messenger.de/begriffe/pseudosicherheit).

5.1. Freier Chat mit XMPP

Die aus meiner Sicht wichtigsten Messenger (und nicht nur, weil ich sie selbst nutze) sind solche, die das Protokoll XMPP (das keiner Firma sonder der Allgemeinheit „gehört“) zum Kontakt untereinander nutzen: Sie sind international recht weit verbreitet. Ich habe das Protokoll oben bereits im Zusammenhang mit dem Messenger Conversations kurz angesprochen (S. 16); detaillierte Informationen finden sich unter https://xmpp.org/ und https://www.freie-messenger.de/sys_xmpp. Hier will ich ein paar Punkte kurz ansprechen, die die meisten Alltagsnutzer interessieren dürften.

Ein Protokoll ist praktisch ein international anerkannter Standard, der festlegt, wie Programme im Internet miteinander in Austausch treten. Wir kennen den Begriff aus der Welt der Diplomatie, wo es ganz präzise Regeln dafür gibt, wer beim Staatsempfang neben wem sitzen darf (bzw. muss). Ähnlich schreiben Protokolle vor, auf welche Weise Internetadressen dargestellt werden, wie Informationen transportiert werden, wie Verbindungen aufgebaut werden, und vieles mehr. Es gibt viele Protokolle, das wohl bekannteste dürfte das ***I***nternet-***P***rotocol sein, weil jedeR schon einmal irgendwo von einer „IP-Adresse“ gehört oder gelesen haben dürfte. Aber auch HTML ist ein Standard (für die Darstellung von Internetseiten). Werden solche Standards nicht eingehalten, dann kann ein Browser eine bestimmte Webseite vielleicht nicht finden, oder eine Nachricht kann nicht zugestellt werden.

XMPP bedeutet „Extensible Messaging and Presence Protocol“, also „Erweiterbares Nachrichten- und Anwesenheitsprotokoll“. Die Erweiterbarkeit erlaubt es, Zusatzfunktionen als Erweiterungen zu entwickeln („XEPs,“ „XMPP Extension Protocols“/„XMPP-Erweiterungs-Protokolle“), die von anderen Entwicklern in ihren eigenen Clients implementiert werden können; ein wichtiges Beispiel ist die Verschlüsselung. Es gibt verschiedene Verschlüsselungstechniken und auch die neueste auf der Signal-Verschlüsselung basierte hat als Erweiterung hier Einzug gehalten: Sie heißt hier OMEMO-Verschlüsselung[66]. Diese wird zunehmend in die verschiedenen Messenger-Angebote eingebaut (die Apple-Welt ist hierbei aufgrund der Firmenpolitik Apples etwas zurück, holt aber kontinuierlich auf). Andere Beispiele sind die Möglichkeit, verschlüsselte Telefonate und Videotelefonate zu führen und vieles mehr. Das Protokoll XMPP wird neben Chat auch für Gerätesteuerung oder

dem Internet of Things (IoT) verwendet und ist gut etabliert, wird vielfältig verwendet und ständig weiterentwickelt.

Ein Protokoll ist praktisch die „Sprache“, die der jeweilige Messenger (App/Programm) auf technischer Ebene für den Austausch mit anderen nutzt. Und wie bei natürlichen Sprachen ist es erforderlich, dass beide bzw. sämtliche Partner dieselbe Sprache sprechen – es ist jedoch nicht erforderlich, dass sie aus dem selben Land stammen. Daher gibt es viele verschiedene Programme[67.] für praktisch alle Geräte und Betriebssysteme, ob sie von Google, Microsoft, Apple oder sonst woher stammen, mit denen über den XMPP-Standard kommuniziert werden kann, ohne dass die Beteiligten notwendigerweise wissen müssen, welche Programme die anderen gerade verwenden. Es gibt reine textbasierte Chatprogramme die sich optimal für eine barrierefreie Nutzung eignen, und andere erlauben sogar die Verwendung im Browser des Computers oder als Teil von anderen Anwendungen, ohne dass der Anwender die eigentliche App als solches zu Gesicht bekommt. Probleme ergeben sich in der Regel – von Leitungsengpässen abgesehen, die aber nichts mit dem Kommunikationskanal zu tun haben – lediglich daraus, dass einzelne Systeme die eine oder andere Erweiterung noch nicht oder nicht vollständig implementiert haben oder andere Schwerpunkte setzen. Anders als bei geschlossenen Systemen kann man sich als Nutzer durchaus den für einen selbst am besten passenden Client aussuchen. Das kennen wir, wie bereits beschrieben, auch von E-Mail.

Ein weiterer Fortschritt gegenüber vielen zentralen Messengersystemen mit ihren meist eigenen Protokollen ist, dass der offene Standard es erlaubt, Clients auf verschiedenen Geräten parallel zu verwenden. WhatsApp und manche andere Insellösungen können dagegen nur auf einem Gerät betrieben werden; will ich das Gerät wechseln, muss ich die App neu installieren und mit mehr oder weniger Aufwand einrichten. Interessanterweise beruht die Funktionsweise von WhatsApp ausgerechnet auf XMPP; die Firma hat das ursprünglich Freie Protokoll aber für ihre eigene Zwecke *so* weiterentwickelt und verändert, dass die Offenheit nicht mehr vorhanden ist.

Bei den „echten“ XMPP-Messengern ist es demzufolge unerheblich, ob es sich um denselben oder um verschiedene Clients handelt. Ob ich blabber.im auf einem Android- und Monal auf einem Apple-Smartphone verwende, dazu Gajim auf meinem Windows-Notebook und Dino auf dem Linuxrechner – alle Clients zeigen mir in der Regel den gleichen Stand meiner Chatverläufe, ich finde die zugestellten Fotos auf allen meinen Endgeräten. Wenn ich will, kann ich auch mehrere Messenger parallel auf einem Gerät betreiben – zu Testzwecken zum Beispiel. Auch das kennen wir von der E-Mail: E-Mails stehen üblicherweise auf dem Smartphone und dem PC gleichzeitig und synchron zur Verfügung.

Es gibt verschiedene Brücken zu anderen Systemen, die hier „Transporte“ genannt werden. Großer Nachteil aller Brücken/Transporte (auch bei denen des nachfolgend beschriebenen Matrix-Protokolls) ist jedoch, dass nie alle Funktionen eines Systems von einem anderen

System – quasi 1:1 – umgesetzt werden können. Das führt in der Praxis zu häufigen Enttäuschungen.

Dadurch, dass der internationale Standard bereits längere Zeit existiert, ist er ausgereift und erprobt - für die oder den durchschnittlichen Endnutzer dürften sich nach einer kurzen Eingewöhnung kaum Probleme auftun. Diese Tatsache machen sich auch Großorganisationen zunutze: Die NATO arbeitet z.B. schon lange Zeit mit diesem Standard[68]. Auch das „Internet of Things" profitiert sehr stark von den Möglichkeiten, das das freie Protokoll XMPP bietet[69].

5.2. Matrix

Matrix ist ein weiteres offenes und Freies Kommunikationsprotokoll für Kommunikation in Echtzeit[70]. Es kann in seiner Ausrichtung und Funktionalität – wenn man von grundsätzlichen Unterschieden zwischen Protokoll und Anwendungssystem absieht – am ehesten mit der „kollaborativen" (für Gruppenarbeit besonders geeignet, daher auch „Groupware" genannt) Software *Slack*[71] verglichen werden. Matrix ist im Vergleich zu XMPP noch sehr jung: Erst im Jahr 2019 hat es das letzte Teststadium verlassen und wurde als voll funktionsfähig und stabil der Öffentlichkeit übergeben[72]. Der Große Unterschied besteht in de konzeptionellen Architektur des System – so liegt der Fokus eindeutig bei der Ausfallsicherheit (dazu gleich mehr) und weniger bei der Freiheit und Privatsphäre. Die dahinterstehende Organisation weist selbst darauf hin[73], dass damit noch nicht alle Möglichkeiten ausgeschöpft sind, die das Protokoll einmal bieten soll.

Auch das Matrix-Protokoll bietet eine sehr sichere Verschlüsselung durch den Einsatz der „Olm"- und „Megolm"-Standards, wobei „Olm die Verschlüsselung in direkter Kommunikation übernimmt, „Megolm" die Verschlüsselung von großen Chatgruppen. Beide bauen wie OMEMO ebenfalls auf dem Signal-Protokoll auf. Hinsichtlich der Messengerfunktionalität „kann" Matrix derzeit schon vieles von dem, was Messenger, die XMPP beherrschen, auch können.

Auch bei Matrix ist es möglich, dass Nutzer ihren eigenen Server betreiben und damit die volle Kontrolle über die bei ihnen anfallenden Metadaten erhalten – wie bei XMPP. Nicht veröffentlichte Berichte aus der Praxis weisen allerdings darauf hin, dass die Hardware bei solchen Heim-Servern augenscheinlich sehr stark belastet wird und der Energieverbrauch wenigstens derzeit noch sehr hoch sein soll. Auch besteht ein weiteres möglicherweise datenschutzrelevantes Problem: Die Chats und Daten aller NutzerInnen werden über alle an einer Konversation beteiligten Server der Teilnehmenden verteilt und überall auf sehr lange und teils unbegrenzte Zeit gespeichert[74]. Es ist damit praktisch unmöglich, den Verbleib einer einmal gesendeten Nachricht nachzuverfolgen, analog zu XMPP, WhatsApp, der Briefpost usw.

Wenn auch die Inhalte stark verschlüsselt sind, so ist das nicht jedermanns Sache. Problematisch kann das sein, wenn ich etwa als gewerblicher Nutzer mit einem (Matrix-)Anbieter

einen Auftragsdatenverarbeitungsvertrag schließe, und der Anbieter eine Föderation mit anderen Matrix-Servern erlaubt (Standardeinstellung?). In dem Fall wird der komplette Chatverlauf, die Inhalte sowie alle Nutzer auch auf den (Dritt-)Servern gespiegelt (besser: synchronisiert), auch dort gespeichert und vorgehalten.. Bei Ausfall meines Servers könnte dann dort sogar weitergearbeitet werden - der Vertrag würde aber nicht mehr eingehalten bzw. müsste mit jedem beteiligten Matrix-Serverbetreiber geschlossen werden. Eine organisationsinterne Nutzung ohne „Föderation“ mit anderen Matrix-Servern außerhalb könnte für dieses Problem eine Lösung bieten, würde aber eine eine Kommunikation nach „draußen“, außerhalb der eigenen Organisation prinzipiell erschweren, wenn nicht ein übergreifender Nachrichtenaustausch über „Brücken“ (dazu gleich mehr) in andere Systeme ermöglicht wird.

Wie es bei XMPP sogenannte „Transporte“ zu anderen Messengersystemen gibt, so wird von der Matrix-Organisation an der Entwicklung von „Brücken“ („Bridges“) gearbeitet, die ebenfalls verschiedene Systeme miteinander verbinden sollen. Solche Brücken sind jedoch bezüglich der Datenschutzthematik sehr umstritten[75]. Derzeit ist die Arbeit an den Brücken auch noch nicht sehr weit fortgeschritten[76]; besonders hin zu Unfreien Systemen gibt es bisher kaum Erfolge zu vermelden, und jede Brücke kann schnell durch individuelle Änderungen seitens des zentralen Anbieters des Unfreien Systems, der als einziger die Freiheit zur Veränderung „seines“ Systems hat, schnell zerstört werden.

Dem Matrix-Protokoll wird von maßgeblichen Seiten viel Aufmerksamkeit zuteil: Sowohl die französische Regierung[77] als auch die Bundeswehr[78] stecken viel Einsatz und Ressourcen in die Entwicklung von Matrix-Messengern. In Frankreich nahm der interne Messenger (der also nur für die Angehörigen der Verwaltung nutzbar und somit nicht wirklich frei ist) seinen Dienst auf – mit gehörigen Startschwierigkeiten[79]. Dennoch kann noch einmal darauf hingewiesen werden, dass eine Matrix-basierte Anwendung innerhalb von Organisationen eine gute Lösung für ausfallsicheren Gruppenchat mit Zusatzfunktionen sein kann, da mehrere (eigene) Bereiche/Organisationseinheiten/Ländervertretungen ihre „eigenen“ Matrixsever haben können. Benötigen Organisationen aber Zugang „nach außen“, so sollte zumindest eine stabile Brücke für Standardfunktionalitäten zu anderen freien Systemen (z.B. zu XMPP) eingerichtet werden, um durch diese Kombination die Vorteile beider Systeme nutzen zu können.

5.3. Peer-to-Peer und „Chatten via Email“

An dieser Stelle möchte ich noch auf zwei letzte Freie Systeme aufmerksam machen. Das eine kann besonders hohen Sicherheitsansprüchen genügen, ist aber für den Alltagsgebrauch aus verschiedenen Gründen nur bedingt geeignet, nämlich *Briar*.

Briar unterscheidet sich von den anderen Freien Messengern vor allem dadurch, dass es direkte Verbindungen zu anderen NutzerInnen aufbauen kann, ohne auf Server zuzugreifen („Peer-to-Peer“, Nutzer-zu-Nutzer). Im Internet verbindet sich Briar über das Tor-Netz-

werk[80.], wodurch eine Überwachung der Metadaten und eine Zuordnung zu einem bestimmten Nutzer durch Angreifer sehr erschwert bzw. fast unmöglich wird. Verbindungen sind auf kurze Entfernung auch vollständig ohne das Internet, über WLAN oder Bluetooth, möglich[81.]. Jede Kommunikation ist stark verschlüsselt, wodurch auch ein Angriff auf die Inhalte kaum vorstellbar ist.

Ein besonderes Sicherheitsmerkmal von Briar ist, dass sich die Kommunikationspartner verifizieren müssen: Man kann also sicher sein, dass man wirklich demjenigen schreibt, dem man auch schreiben will. Musste man sich dazu bisher persönlich treffen, was bei weit entfernt lebenden Partnern oft ein Problem darstellte, so ist es in der neuesten Version 1.2 jetzt möglich, diese Überprüfung („Verifikation“) über Links vorzunehmen[82.].

Die Alltagstauglichkeit von Briar wird unter anderem durch den hohen Stromverbrauch eingeschränkt, wie er aus Tests[83.] und Erfahrungsberichten[84.] bekannt geworden ist. Auch ein paar andere Punkte werden den durchschnittlichen Nutzer abschrecken, wie zum Beispiel, dass üblicherweise beide Kommunikationspartner gleichzeitig online sein müssen (zeitversetzte Kommunikation ist nur mit besonderem Aufwand möglich), dass keine Übermittlung von Bildern oder Telefonie möglich ist, und ähnliches. Insofern gehört Briar als Freies Messenger-System mit seinem ganz anderen Ansatz zwar in diesen Aufsatz, wird aber wohl nur für Menschen interessant sein, die Angriffe oder Repressalien starker Gegner wie etwa Regierungen befürchten müssen.

Auch „Chatten via E-Mail“ ist möglich, und die Anführungszeichen verweisen bereits darauf, dass der Ausdruck nicht ganz richtig ist. In Wirklichkeit geht es darum, die etablierten E-Mail-*Protokolle* (vgl. S. 21) IMAP, SMTP und IMF zu verwenden, um Nachrichten wie bei einem Messenger zu versenden. Die bekannteste Anwendung für diese Form des Chattens ist das relativ neue Delta Chat[85.], allerdings lassen sich auch viele der gängigen E-Mail-Programme verwenden. Delta Chat ist ein Freier Messenger; er kann in der jeweils richtigen Version auf verschiedenen Plattformen wie Windows, Android, iPhone usw. verwendet werden. Auch Delta Chat verschlüsselt Nachrichten – solange beide Partner Delta Chat verwenden. Wird die Nachricht auf einem „normalen“ E-Mail-Client empfangen oder von ihm gesendet, so bleibt sie prinzipiell unverschlüsselt[86.], der E-Mail-Anbieter kann sie also lesen. Eine Ausnahme gibt es nur dann, wenn das E-Mail-Programm eine entsprechende Verschlüsselung unterstützt und der Nutzer diese auch verwendet – was (noch?) nicht besonders häufig der Fall ist.

Ein wichtiger Vorteil von Delta Chat ist gleichzeitig ein Nachteil: Der Verzicht auf eigene Server. Es gibt zwar keine eigene Anbieter-Instanz, der man vertrauen muss, dafür aber gibt es diese Notwendigkeit gegenüber dem E-Mail-Anbieter. Je nach dessen Sicherheitsstandards kann es passieren, dass Chats als lesbare „Postkarten“[87.] versendet werden. Leider gehören viele E-Mailanbieter (wie z.B. G-Mail) selbst zu den Datensammlern und -verwertern[88.].

6. Ein Plädoyer

Mein Plädoyer ist wahrscheinlich im Verlauf dieses Textes deutlich geworden. Ich bin ein Verfechter Freier Messengersysteme (und anderer Freier Software, obwohl das nicht an diese Stelle gehört). Ich glaube, dass Freie Messenger die ideale Lösung darstellen, um auf Dauer unsere private Kommunikation und unsere persönlichen Daten unter unserer eigenen Kontrolle und in unserer eigenen Hand zu behalten.

Gerne will ich zugeben, dass auch manche proprietären und zentralen Systeme einen Fortschritt gegenüber Anbietern darstellen, die – wie WhatsApp/Facebook – fundamental darauf ausgerichtet sind, aus dem Kommunikationsverhalten und den Angaben ihrer Nutzer Kapital zu schlagen, egal, welche Folgen das für diese hat. Systeme wie Signal oder Threema, nicht allerdings Telegram und schon gar nicht Skype, haben vieles richtig gemacht auf dem Weg, ihre Nutzer zu schützen; es bleibt aber die Tatsache bestehen, dass man ein erhebliches Maß an Vertrauen in die Anbieter und vor allem dahin aufbringen muss, dass sie ihre Grundsätze in der Zukunft nicht ändern. Der Schritt zum „Überwachungskapitalismus[89].“ ist nur noch ein sehr kleiner. Mir ist das zu viel Vertrauen, und mir fehlt hier auch Zukunftssicherheit.

Daher will ich meine Wünsche und mein Plädoyer noch einmal konkret formulieren:

- Ich wünsche mir und plädiere dafür, das Freie Messenger (anbieterunabhängige Apps und Programme) mehr und regelmäßiger genutzt werden und damit zum Schutz von *unser aller* Privatsphäre beitragen.
- Ich wünsche mir und plädiere dafür, dass meine Kontaktdaten von weniger Menschen zu WhatsApp/Facebook hochgeladen werden (durch Nutzung des Messengers), als das jetzt der Fall ist (möglichst gar keinen), damit mein Online-Nutzerprofil (und die meiner Freunde und Verwandten) „löchriger“ und mein Privatleben weniger durchsichtig wird. **Mein Freundes- und Familienkreis gehört mir!**
- Ich wünsche mir auch und plädiere dafür, dass die Bedeutung Freier Software als Grundlage freier und privater Kommunikation als ein Bürgerrecht angesehen wird. Die Beschäftigung mit dieser weit verbreiteten Alltagssoftware „Messenger“, das Nachdenken darüber, warum man auf bestimmte Systeme verzichten und auf andere setzen sollte, könnte dazu beitragen, dass mehr Menschen über die Implikationen der von ihnen benutzten Software nachdenken.
- Ich wünsche mir und plädiere dafür, dass die allgemeinen Freiheitsrechte aus der vordergründigen Verbindung mit dem potentiell Illegalen oder zumindest Unmoralischen heraustreten („Datenschutz ist Täterschutz!“) und als das angesehen werden, was sie sind: Eine wichtige Grundlage für ein gleichberechtigtes Miteinander aller Menschen in einer Gesellschaft, die sich zwar einen Staat gibt, weil der ein notwendiges und funktionales Werkzeug der Organisation und Verwaltung ist, nicht je-

doch, damit dieser sich in die privaten, persönlichen Bereiche des individuellen Alltags drängt, dort Vorschriften macht und Informationen sammelt.

Weil Chatten (und somit die Werkzeuge „Messenger“) ein zentraler Teil der alltäglichen Kommunikation in unserer Gesellschaft geworden ist, ist es meiner Meinung nach sinnvoll, hier anzufangen, um ein Bewusstsein dafür zu entwickeln, welche Wege unsere Texte, Fotos und Videos nehmen und was alles daran hängt, wie wir miteinander kommunizieren. Gerade wegen ihrer Alltäglichkeit halte ich es für sinnvoll, Alternativen zum allgegenwärtigen (oft genutzten) WhatsApp zu zeigen, um vielleicht einen Nachdenkprozess in Gang zu bringen.

Die Covid-19-Pandemie hat das Ausmaß elektronischer Kommunikation im Alltag (wieder einmal?) deutlich gemacht und neue Notwendigkeiten geschaffen. Sie hat auch dafür gesorgt, wenn auch aus meiner Sicht in noch unzureichendem Maße, dass über die Sicherheit der Daten nachgedacht und öffentlich diskutiert wird – es waren die Kinder, deren Schutz im Digitalen auf einmal zur Disposition stand, was auch (sogar?) die Bürokratie stellenweise für das Notwendige sensibilisiert hat.

Nutzen wir die Gelegenheit, durch immer breitere Nutzung Freier Messenger unsere Mitmenschen darauf aufmerksam zu machen, dass wir nicht nur Katzenvideos durch die Gegend schicken, sondern vor allem Informationen über uns selbst und über unsere Chatpartner. Unsere Freunde, Familien, Kollegen, … sollten es uns wert sein, auch ihr Privatleben zu schützen.

Werden wir zunächst einmal **datenbewusst** und dann auch **datensouverän**. Freie Messenger sind ein wichtiger und vor allem leicht gehbarer erster Schritt dazu.

7. Anmerkungen siehe nächste Seite

1.) … und natürlich der Schüler**innen**. Aber aus Platzgründen verzichte ich in diesem Text aufs Gendern
2.) https://www.notebookcheck.com/Internet-E-Mail-vs-WhatsApp-und-soziale-Medien.127983.0.html (die Statistik stammt bereits von 2014!); https://winfuture.de/news,116073.html; https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html
3.) https://www.messengerpeople.com/de/weltweite-nutzer-statistik-fuer-whatsapp-wechat-und-andere-messenger/
4.) https://www.whatsapp.com/about/?_fb_noscript=1
5.) https://www.zdf.de/nachrichten/digitales/whatsapp-neue-agbs-dsgvo-100.html
6.) z.B.: https://www.hna.de/welt/whatsapp-update-agb-alternative-datenschutz-messenger-chat-signal-threema-telegram-kassel-hna-zr-90167434.html; https://www.merkur.de/wirtschaft/whatsapp-datenschutz-regeln-update-aenderungen-zwang-facebook-user-zuckerberg-reaktionen-zr-90170973.html; https://www.buzzfeed.de/welt/whatsapp-update-agb-alternative-datenschutz-messenger-chat-signal-threema-telegram-kassel-hna-zr-90167434.html
7.) https://www.wiwo.de/erfolg/trends/forbes-liste-2021-das-sind-die-reichsten-menschen-der-welt/26281100.html
8.) https://netzpolitik.org/2018/die-ultimative-liste-so-viele-datenskandale-gab-es-2018-bei-facebook/
9.) https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern
10.) https://media.kuketz.de/blog/messenger-matrix.png
11.) https://www.kuketz-blog.de/messenger-matrix-uebersicht-vergleich-der-aktuellen-messenger/
12.) https://www.gnu.org/philosophy/free-sw.html#n1 letzter Zugriff: 04.02.2021
13.) https://www.gnu.org/philosophy/free-sw.html#n1
14.) Für Leser, die nicht so tief in der Materie stecken: Als „Quellcode“ bezeichnet man den von Menschen lesbaren eigentlichen Programmcode, den ein Programmierer schreibt, und der erst in Maschinensprache übersetzt werden muss, um lauffähig zu sein.
15.) Wie z.B. gemeinnützige Organisationen, HackerInnengruppen, Datenschutzbeauftragte, FirmenberaterInnen, ...
16.) z.B. https://www.golem.de/news/landesdatenschutzbeauftragter-datenschuetzer-sollen-open-source-empfehlen-2009-151141.html; https://anoxinon.media/blog/interview_kelber/
17.) https://www.pro-linux.de/news/1/19968/bundestagswahl-positionen-der-parteien-zu-freier-software.html; https://netzpolitik.org/2020/was-bedeutet-der-cdu-beschluss-zum-einsatz-freier-software/
18.) https://www.datenschutz.org/schule/; https://www.heise.de/news/Schulen-brauchen-Klarheit-beim-Datenschutz-4993139.html; https://www.heise.de/news/Schulen-brauchen-Klarheit-beim-Datenschutz-4993139.html; https://www.heise.de/news/Schulen-brauchen-Klarheit-beim-Datenschutz-4993139.html
19.) z.B.: https://digitalcourage.de/nichts-zu-verbergen; https://www.amnesty.de/informieren/artikel/7-gruende-weshalb-ich-habe-nichts-zu-verbergen-die-falsche-reaktion-auf; https://www.nachdenkseiten.de/?p=57856;

20.) Es gibt eine Reihe von Initiativen, die sich diesbezüglich auch die Förderung digitaler Kompetenz, insbesondere bei Schülern auf die Fahnen geschrieben haben, z.B. https://www.teckids.org/de/; https://digitalcourage.de/; https://www.klicksafe.de/
21.) https://www.computerwoche.de/a/android-apps-kommunizieren-heimlich-mit-werbenetzwerken,2354656
22.) https://www.br.de/nachrichten/deutschland-welt/so-kann-das-bka-heimlich-bei-whatsapp-mitlesen,S5J8CwA
23.) https://www.heise.de/mac-and-i/meldung/Entwickler-Facebook-kann-WhatsApp-Chats-einsehen-trotz-Ende-zu-Ende-Verschluesselung-4023461.html
24.) Videotelefonie: Skype, WhatsApp und Co. im Vergleich
25.) Vaas, Lisa: Microsoft is reading Skype messages, naked security by sophos, 22.05.2013, https://nakedsecurity.sophos.com/2013/05/22/microsofts-reading-skype-messages/
26.) http://www.h-online.com/security/news/item/Skype-with-care-Microsoft-is-reading-everything-you-write-1862870.html
27.) https://netzpolitik.org/2021/verschluesselung-sichere-kommunikationsanbieter-warnen-vor-hintertueren/
28.) Beide Abbildungen finden sich im Original bei Mike Kuketz unter https://www.kuketz-blog.de/conversations-sicherer-android-messenger/
29.) z.B. https://mobilsicher.de/ratgeber/messenger-app-signal-kurz-vorgestellt
30.) z.B. https://netzpolitik.org/2020/bits-telegram-ist-nicht-so-sicher-wie-das-image-verspricht/; https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html
31.) https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html
32.) https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip
33.) z.B. https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/
34.) Mayer-Schönberger, V./Cukier, K.: Big Data. A Revolution That Will Transform How We Live, Work and Think, London 2013
35.) z.B. https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/; Christl, W.: Kommerzielle digitale Überwachung im Alltag. Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele, Wien 2014, S. 16 ff.
36.) https://www.youtube.com/watch?v=NSaGl2uO5w8
37.) Es sei denn, sie weiß *vor* meinen Eltern, dass ich als 15-Jährige schwanger bin, vgl. Mayer-Schönberger, V./Cukier, K.: Big Data. A Revolution That Will Transform How We Live, Work and Think, London 2013, S. 58; für Hintergrund vgl. auch: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/
38.) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html; https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
39.) https://www.aclu.org/blog/privacy-technology/consumer-privacy/chinas-nightmarish-citizen-scores-are-warning-americans

40.) vgl. Mayer-Schönberger, V./Cukier, K.: Big Data. A Revolution That Will Transform How We Live, Work and Think, London 2013, S. 56 f.
41.) https://en.wikipedia.org/wiki/Walled_garden
42.) z.B. https://www.bbc.com/news/technology-37318031; https://www.welt.de/wirtschaft/webwelt/article158040350/Facebook-gibt-im-Streit-ueber-Napalm-Maedchen-nach.html; https://www.aljazeera.com/news/2016/9/10/facebook-reverses-decision-on-napalm-girl-photo
43.) https://www.zeit.de/politik/deutschland/2018-06/bundesjustizministerin-katarina-barley-whats-app-messenger-oeffnung
44.) z.B. https://praxistipps.chip.de/wegwerf-email-adressen-diese-anbieter-gibts_1674
45.) https://netzpolitik.org/2018/die-ultimative-liste-so-viele-datenskandale-gab-es-2018-bei-facebook/
46.) https://www.whatsapp.com/legal/terms-of-service?_fb_noscript=1: „**Adressbuch.** Du stellst uns regelmäßig die Telefonnummern von WhatsApp Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können."
47.) https://rp-online.de/digitales/apps/urteil-weitergabe-von-kontaktdaten-an-whatsapp-unzulaessig_aid-19417281 ; https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE190000030
48.) https://www.whatsapp.com/legal/terms-of-service/?lang=de&_fb_noscript=1: „Du stimmst unseren Nutzungsbedingungen („Bedingungen") zu, indem du unsere Apps, Dienste, Funktionen, Software oder Webseite (gemeinsam die „Dienste") installierst, nutzt oder auf diese zugreifst."
49.) https://www.whatsapp.com/legal/privacy-policy?_fb_noscript=1: Vorab: Anmerkung: Unter dieser Webadresse findet man die WhatsApp Datenschutzrichtlinie. Es folgen verschiedene Überschriften, unter denen sich die Informationen zu den folgenden Endnoten lesen lassen. Nun zur ersten: „WhatsApp erhält bzw. sammelt Informationen, wenn wir unsere Dienste betreiben und bereitstellen. Dies geschieht unter anderem, wenn du unsere Dienste installierst, nutzt oder auf sie zugreifst." Dann folgt eine lange Liste...
50.) https://www.whatsapp.com/legal/privacy-policy?_fb_noscript=1: „Wir verwenden alle uns zur Verfügung stehenden Informationen als Unterstützung dafür, unsere Dienste zu betreiben, anzubieten, zu verbessern, zu verstehen, zu individualisieren, zu unterstützen und zu vermarkten." Und wieder folgt eine lange Liste...
51.) https://www.whatsapp.com/legal/privacy-policy?_fb_noscript=1
52.) https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report
53.) z.B. https://mobilsicher.de/ratgeber/was-sammelt-google-ueber-mich
54.) https://gizmodo.com/how-facebook-outs-sex-workers-1818861596
55.) https://allfacebook.de/toll/state-of-facebook; für Deutschland: https://www.messengerpeople.com/de/whatsapp-nutzerzahlen-deutschland/#WhatsApp-Nutzerzahlen-Dautschland-Statistik-2021
56.) https://www.youtube.com/watch?v=Nj3YFprqAr8; zu Gegenargumenten z.B. hier: https://www.heise.de/forum/heise-online/News-Kommentare/Krypto-Experte-Keine-Backdoor-in-WhatsApp/Moxie-Marlinspike-ist-nicht-gerade-vertrauenswuerdig/posting-29787920/show/
57.) ...was ich beispielsweise automatisch mache, wenn ich die WhatsApp-App auf meinem Smartphone installiere, vgl. die WhatsApp-AGB, Anm. 48.

58.) Der Film „Minority Report“ mit Tom Cruise zeigt eindrücklich, zu welchen Folgen das führen könnte
59.) Edward Snowden hat unter großer internationaler Beachtung aufgedeckt, dass die NSA durchaus solche Ziele verfolgte: Snowden, Edward J.; Greiners, Kay: Permanent Record. Meine Geschichte, Frankfurt am Main 2019
60.) https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2010/bvg10-011.html
61.) https://play.google.com/store/apps/details?id=eu.siacs.conversations
62.) Ich danke dem Entwickler von Pix-Art und blabber.im, Christian Schneppe, für diese Infos!
63.) https://www.heise.de/news/Threema-Apps-sind-nun-komplett-quelloffen-4993753.html
64.) https://www.heise.de/security/artikel/OMEMO-fuer-Jabber-eine-Einordnung-3603601.html ; https://conversations.im/omemo/
65.) … was nicht die beste Idee ist, weil Browser beliebte Angriffsziele im Internet sind!
66.) https://conversations.im/omemo/; https://omemo.top/
67.) Eine meist aktuelle Übersicht gibt https://xmpp.org/software/clients.html
68.) https://www.isode.com/whitepapers/military-forms-using-xmpp.html; https://xmpp.org/about/faq.html
69.) https://xmpp.org/uses/internet-of-things.html
70.) https://www.privacy-handbuch.de/handbuch_74g.htm
71.) https://slack.com/intl/de-de/
72.) https://matrix.org
73.) https://matrix.org/blog/2019/06/11/introducing-matrix-1-0-and-the-matrix-org-foundation
74.) Element: Messaging über die Matrix – Messenger Teil7 ⋆ Kuketz IT-Security Blog
75.) vgl. Kuketz https://www.kuketz-blog.de/messenger-bruecken-sind-datenschutzrechtlich-bedenklich/
76.) https://matrix.org/bridges/
77.) https://www.linux-magazin.de/news/frankreichs-regierung-bekommt-open-source-messenger/; https://www.golem.de/news/statt-whatsapp-frankreich-wandert-in-die-matrix-1902-139167.html
78.) https://www.heise.de/news/Matrix-steht-als-Messenger-fuer-Soldaten-und-zivile-Angehoerige-zur-Verfuegung-4963211.html; https://t3n.de/news/matrix-neuer-messenger-bundeswehr-behoerden-1282086/
79.) Tchap: Frankreichs (nicht so) exklusiver Regierungschat | heise online
80.) https://www.torproject.org/de/
81.) https://briarproject.org/how-it-works/
82.) https://briarproject.org/news/2019-briar-1.2-released-remote-contacts/
83.) z.B. https://www.kuketz-blog.de/briar-anonymitaet-und-sicherheit-gehen-vor-messenger-teil8/; https://mobilsicher.de/ratgeber/messenger-app-briar-kurz-vorgestellt
84.) z.B. https://forum.golem.de/kommentare/security/briar-der-messenger-fuer-die-krise/leider-sehr-stromintensiv/133876,5628565,5628565,read.html
85.) https://delta.chat/de/
86.) Transportverschlüsselung ist natürlich trotzdem wirksam, das spielt an dieser Stelle aber keine Rolle
87.) https://www.kuketz-blog.de/leserfrage-ist-delta-chat-praxistauglich/

88.) Ein paar Beispiele findet man hier: https://www.privacy-handbuch.de/handbuch_31.htm ; dass gmail nicht empfehlenswert ist, ist wahrscheinlich bekannt; falls nicht, gibt es hier (https://mobilsicher.de/ratgeber/was-sammelt-google-ueber-mich) ein paar Hinweise

89.) Zuboff, Sh: Das Zeitalter des Überwachungskapitalismus, Frankfurt/New Your 2018; Surveillance Capitalism - Überwachungskapitalismus – Essay (http://www.bpb.de/apuz/292337/surveillance-capitalism-ueberwachungskapitalismus, Lizenz: CC BY-NC-ND 3.0 DE)