Information Security

We (Dis-)Respect your Privacy

Sicherheit und Datenschutz populärer Messaging-Applikationen

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

eingereicht von

Andreas Moser, BSc

is191837

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer: Dipl.-Ing. Peter Kieseberg

St. Pölten, 3. August 2021

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Instant-Messenger sind in der modernen Gesellschaft kaum mehr wegzudenken und werden von Personen sämtlicher Altersgruppen verwendet. Sowohl im privaten als auch im beruflichen Bereich haben sich die Kurznachrichtendienste bereits stark etabliert und stellen einen wichtigen Bestandteil des täglichen Lebens dar. Dienstleister erfreuen sich einem stetigen Zuwachs, da der Download und die Nutzung der Messenger in der Regel kostenlos sind - zumindest aus monetärer Sicht. Nutzerinnen und Nutzer müssen einen wesentlichen Trade-Off bei der Verwendung vieler Applikationen hinnehmen, so werden diese gratis angeboten, finanziert werden sie jedoch über die Sammlung und Weitergabe von Nutzerdaten.

Diese Arbeit beschäftigt sich mit der Analyse und Bewertung verschiedener Messaging-Applikationen in den Bereichen Privatsphäre/Anonymität, Sicherheit und Benutzerfreundlichkeit. Eine besonderer Fokus bei der Bewertung wird auf den von der Applikation erreichten Datenschutz gelegt. Ziel dieser These ist es, eine Grundlage zum direkten Vergleich der einzelnen Apps basierend auf deren Eigenschaften in den oben genannten Domänen zu schaffen. Neben der Evaluierung werden ebenfalls die rechtlichen Grundlagen zum Transfer personenbezogener Daten von EU-Bürger/innen aus dem Europäischen Wirtschaftsraum thematisiert. Vor allem Vereinbarungen und Abkommen zwischen den USA und der EU werden vorrangig behandelt.

Es konnte ermittelt werden, dass die verschiedenen Messaging-Applikationen in den Bereichen Sicherheit und Benutzerfreundlichkeit jeweils gute bis sehr gute Eigenschaften aufweisen. Differenzen können in diesen Bereichen nur vereinzelt wahrgenommen werden. Im Kontrast dazu wurden im Bereich Privatsphäre/Anonymität erhebliche Unterschiede zwischen den Applikationen verzeichnet. Vor allem die Sammlung und Weitergabe von Daten stellt bei einigen Messengern ein erhebliches Datenschutzproblem dar. Als gesetzliche Grundlage zum Transfer personenbezogener Daten aus dem EWR in Drittländer, konnten die Abkommen Safe Harbor und Privacy Shield ermittelt werden. Diese wurden jedoch durch den Europäischen Gerichtshof für rechtswidrig erklärt. Um den Datentransfer weiterhin zu legitimieren, substituieren die so genannte Standard Contractual Clauses vorangegangene Abkommen. Die Übermittlung von Daten in Drittländer ist somit bis auf Weiteres konform gegenüber europäischem Recht.

Abstract

It is hard to imagine modern society without Instant Messengers as they are used by people of all age groups. In both the private and professional spheres, Messengers have already become strongly established and represent an important part of our daily life. Service providers are enjoying steady growth, because downloading and using the messengers is generally free - at least from a monetary perspective. Users have to accept a significant trade-off when using many applications, for example, they are offered for free, but they are financed by collecting and sharing user data.

This thesis deals with the analysis and evaluation of different messaging applications in the areas of privacy/anonymity, security and usability. A particular focus in the evaluation is placed on the level of privacy achieved by the application. The aim of this thesis is to provide a basis for direct comparison of individual apps based on their characteristics in the above-mentioned domains. In addition to the evaluation, the legal basis for the transfer of personal data of EU-Citizens from the European Economic Area will also be addressed. In particular, agreements and treaties between the US and the EU will be prioritized.

It was possible to determine that the various Messaging-Applications each have good to very good characteristics in the areas of security and user-friendliness. Differences can only be perceived in these areas in isolated cases. In contrast, considerable differences between the applications were recorded in the area of privacy/anonymity. In particular, the collection and transfer of data poses a considerable data protection problem with some of the applications.

As a legal basis for transferring personal data from the EEA to third countries, the Safe Harbor and Privacy Shield agreements could be identified. However, these were declared illegal by the European Court of Justice. In order to continue to legitimize the data transfer, the so-called Standard Contractual Clauses substitute previous agreements. The transfer of data to third countries is therefore compliant with European law - at least for now.

Inhaltsverzeichnis

1 Einleitung

Was im Internet passiert, bleibt dort und gerät auch nicht in Vergessenheit. Unter dem Deckmantel der verbesserten User-Experience hat der Wettlauf der Datensammler bereits vor Jahren begonnen. Die meisten im Alltag verwendeten Applikationen zur Kommunikation, zum Datentransfer als auch für die belanglosesten Suchanfragen mögen kostenlos bereitgestellt werden, umsonst sind sie gleichwohl nicht. Besonders die momentanen datenschutzrechtlichen Entwicklungen im Bereich der Messaging-Applikationen stehen im öffentlichem Fokus und verlangen eine genaue Betrachtung und Analyse, wer und zu welchem Zweck Zugriff auf unsere Daten erhält. Datenschutzerklärungen sind oftmals seitenlang und sehr unübersichtlich. Userinnen und User sehen sich mit juristischen Erklärungen zur Datenverarbeitung konfrontiert, welche teilweise oder kaum Einblick bieten, wohin ihre Daten transferiert, wo diese gespeichert und zu welchem Zweck sie verarbeitet werden. Besonders Datentransfers in Drittländer wie die Vereinigten Staaten müssen kritisch hinterfragt werden, da die dort herrschende Gesetzeslage nicht mit der der Europäischen Union vergleichbar ist. Vor allem im Bereich Datenschutz existiert zwischen der EU und den USA eine unterschiedliche Auffassung über das zu erreichende Schutzniveau.

Es existiert bereits eine Vielzahl an Messaging-Applikation, welche neben robusten Sicherheitseigenschaften, ihren Userinnen und Usern den bestmöglichen Schutz der Privatsphäre versprechen. So wird damit geworben, dass Daten lediglich zum Zweck des reibungslosen Betriebs des Services gesammelt und verarbeitet werden. Dabei wird sich auf das Prinzip der minimalen Datenverarbeitung berufen. Es ist jedoch wichtig zu bedenken, dass die meisten Applikationen frei erhältlich sind, dass bedeutet, dass durch den Download und die Nutzung des Dienstes kein Umsatz generiert wird. So stellt sich die Frage, wie die Entwicklung und der Betrieb der Applikation durch die Unternehmen finanziert wird. Dabei gibt es unterschiedliche Herangehensweisen seitens der Anbieter. Zum einen können Unternehmen mittels Investments oder Spenden den Dienst bereitstellen, zum anderen kann mittels Werbepartnern und den entsprechenden Verträgen zur Datenweitergabe und Auswertung Umsatz generiert werden. Letzteres ist bedenklich, da die Weitergabe von Nutzerdaten an Drittanbieter konträr zum Prinzip der Datenminimierung ist. Neben den datenschutzrechtlichen Aspekten müssen Messaging-Applikation vor allem ein

hohes Niveau an Sicherheit bieten, da der Datenschutz in dem Moment obsolet wird, in dem versendete Nachrichten abgefangen, entschlüsselt und eingesehen werden können. Besonders die Vertraulichkeit und Integrität der versendeten Daten beziehungsweise Nachrichten gilt im Bereich Security als oberstes Schutzziel. Eben diese Eigenschaften müssen moderne Messaging-Applikation mittels State-of-the-Art-Technologien wahren. Unternehmen haben bereits eine Vielzahl an Lösungen auf den Markt gebracht, welche ihren Benutzerinnen und Benutzern ein hohes Maß an Sicherheit versprechen. Die Tatsache, dass es mehr als genug Technologien und Sicherheitslösungen im Bereich Messaging gibt und diese stehts weiterentwickelt werden, ist durchaus lobenswert, jedoch führt dies schnell zu einem wesentlichen Problem: Der Unübersichtlichkeit. Viele Anbieter werben damit, dass Ihre Produkte mittels „Militärtechnologie“ entwickelt wurden, was durchaus nicht grundsätzlich falsch ist, doch wird mit dieser Eigenschaft ein verzerrtes Sicherheitsgefühl vermittelt, da dieser Begriff sehr breit ausgelegt ist und auch veraltete Technologien oder Methoden, welche bereits nicht mehr State-of-the-Art und als unsicher eingestuft wurden, sich noch immer im Einsatz befinden können.

Eine weitere und nicht unwesentliche Hürde die es zu überwinden gilt ist die Usability, also die Benutzerfreundlichkeit der Applikation. Ist eine Lösung noch so ausgezeichnet in ihren Eigenschaften im Bereich Sicherheit und Datenschutz, die Benutzerfreundlichkeit jedoch nicht ausreichend gewährleistet und der Einsatz schlichtweg zu kompliziert gestaltet ist, kann kein breites Spektrum an Usern erreicht werden. Da Kurznachrichtendienste nicht nur ausschließlich von technisch affinen Nutzerinnen und Nutzern verwendet werden, muss die Applikation einfach zu bedienen sein, das bedeutet, dass von den Usern nicht vorausgesetzt werden darf, Einstellungen zum Schutz der Daten selbst zu tätigen. Das Prinzip Security- und Privacy by Default muss daher von der Messaging-Applikation umgesetzt sein.

Aus diesen Überlegungen im Bereich Secure-Messaging mit Fokus auf den Datenschutz ergibt sich die erste Forschungsfrage, welche im Zuge dieser Arbeit beantwortet wird:

„Welche modernen Messaging-Applikationen bieten die besten Eigenschaften in den Domänen Privatsphäre/Anonymität, Sicherheit und Benutzerfreundlichkeit?“

Neben dem direkten Vergleich der einzelnen Kurznachrichtendienste sind besonders die rechtlichen Aspekte im Bereich der Datenübermittlung in Drittländer von Relevanz. Da Server-Infrastrukturen in aller Welt, jedoch vor allem in den Vereinigten Staaten gehostet werden, ist mit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) die Legitimität der Transfers durchaus nicht vollständig transparent.

Die DSGVO schreibt vor, dass ein Datentransfer in ein Drittland nur dann zulässig ist, wenn ein entsprechendes Schutzniveau beim Datenverarbeiter vorhanden ist. Dieses Schutzniveau soll mittels gesetzlichen Regelungen und Abkommen erreicht werden, sodass eine Datenverarbeitung nach europäischen Bestimmungen und Vorgaben erfolgen darf. Da jedoch Abkommen wie Safe-Harbor und Privacy-Shield vom Europäischen Gerichtshof für unzulässig erklärt wurden, stellt sich hiermit die zweite zu beantwortende Forschungsfrage:

„Welche gesetzlichen Bestimmungen legitimieren den Transfer personenbezogener Daten von EU-Bürgerinnen und Bürger in die Vereinigten Staaten und andere Drittländer?“

Ziel dieser Arbeit ist neben der Beantwortung der oben genannten Forschungsfragen die Erstellung eines Bewertungsframeworks in tabellarischer Form zum direkten Vergleich der Messaging-Applikationen in den jeweiligen Domänen Privatsphäre/Anonymität, Sicherheit und Benutzerfreundlichkeit. Dieses Framework kann in weiterer Folge durch das Hinzufügen weiterer Applikationen oder zu untersuchenden Eigenschaften erweitert werden.

1.1 Struktur der Arbeit und Methodologie

Diese Arbeit gliedert sich in 3 Hauptteile, welche systematisch das Themengebiet einerseits erörtert, andererseits die Forschungsfragen in ihrer Reihenfolge behandeln und die entsprechenden Ergebnisse liefern.

Im ersten Hauptteil werden die Begriffe der Privatsphäre und der Anonymität im Allgemeinen und in weiterer Folge im Online-Kontext analysiert und erörtert. Zeil davon ist es, ein Grundverständnis über die Bedeutung von Privatsphäre und Anonymität zu schaffen und dieses Verständnis auf die neuen Herausforderungen des World Wide Web zu reflektieren. Aufgrund der wachsenden Vernetzung und dem steigenden Datenaustausch, werden in weiterer Folge die wesentlichen Schutzziele im Bereich der Privatsphäre erläutert. Im Kontrast dazu wird das so genannte *Dilemma der Online Anonymität* behandelt, welches die Chancen und Risiken der Online-Anonymisierung aufarbeitet.

Der zweite Teil beschäftigt sich mit den verschiedenen Messaging-Applikation, welche für die Bewertungen in den Domänen Privatsphäre/Anonymität, Sicherheit und Benutzerfreundlichkeit herangezogen werden. Dabei handelt es sich insgesamt um 6 Messenger – Viber, Telegram, WickrMe, Threema, Si-

gnal und WhatsApp. Jeder Kurznachrichtendienst wird in einer eigenen Untersektion zunächst allgemein beschrieben. Darauf folgend werden die Apps auf die zur Bewertung definierten Eigenschaften systematisch untersucht, ob die jeweiligen Kriterien erfüllt sind. Zur grafischen Darstellung und zum direkten Vergleich werden die Ergebnisse in tabellarischer Form dargestellt. So kann auf einem Blick erkannt werden, welcher Messenger in welcher Domäne besonders gute beziehungsweise schlechte Eigenschaften aufweist.

Im dritten und letzten Hauptteil wird auf die rechtlichen Aspekte zur Übermittlung personenbezogener Daten an Verarbeiter außerhalb der Europäischen Union eingegangen. Hierbei liegt der Fokus besonders auf dem Transfer von Informationen in die Vereinigten Staaten, da überwiegend US-Serverinfrastrukturen zum Betrieb der einzelnen Applikationen im Einsatz sind. Es erfolgt zunächst ein direkter Vergleich gesetzlicher Bestimmungen im Bereich Datenschutz zwischen den USA und der EU. Dabei werden sowohl die unterschiedlichen Verfahren und Regelungen im Bereich der Datenspeicherung und -verarbeitung als auch die jeweiligen Zuständigkeiten aufgezeigt. Des weiteren werden die Abkommen *Safe-Harbor* und *Privacy-Shield*, welche vor der Erklärung auf Rechtswidrigkeit durch den Europäischen Gerichtshof den Austausch personenbezogener Daten aus dem EWR in die USA geregelt hatten, in eigenen Subsektionen behandelt. Im Kontrast dazu werden die aktuellen Abkommen zum legitimen Datenaustausch aufgezeigt.

2 Related Work

Es wurde bereits eine Vielzahl an wissenschaftlichen Arbeiten veröffentlicht, welche sich mit Massaging-Technologien beziehungsweise mit dem Vergleich von Messaging-Applikationen auseinandersetzen.

In dem Paper *Can Johnny Finally Encrypt* [1] vergleichen die Autoren Herzberg und Leibowitz die Messenger WhatsApp, Signal, Telegram und Viber. Neben den Aspekten der Security-Eigenschaften der einzelnen Applikationen, beschäftigen sie sich ebenfalls mit der Sensibilisierung der Userinnen und User. So kommen sie zum Ergebnis, dass Nutzerinnen und Nutzer sehr wohl Wert auf ihre Privatsphäre legen, jedoch fehlt es ihnen an Expertise, wenn technische Eigenschafen wie beispielsweise die Ende-zu-Ende-Verschlüsselung thematisiert wird. So verlassen sie sich in den meisten Fällen auf die Anbieter der Dienste und legen den Datenschutz in die Hände der Unternehmen. Im Bereich der Usability konnten die Autoren feststellen, dass der Authentifizierungsvorgang eine besondere Herausforderung für die Nutzerinnen und Nutzer darstellt, da dieser als relativ umständlich wahrgenommen wird. Das führt dazu, dass gegenseitige Authentifizierungen nur selten durchgeführt werden und die Anfälligkeit für eine MitM-Attacke sehr hoch ist.

Botha et al. untersuchen in ihrem Paper insgesamt 17 Messenger auf unterschiedliche Eigenschaften im Bereich der Sicherheit und Privatsphäre. Sie kommen zu dem Schluss, dass Signal, Telegram, WhatsApp und Viber zu den sichersten frei erhältlichen Messaging-Applikationen zählen. Weiters zeigen die Autoren auf, dass kostenpflichtige Kurznachrichtendienste mindestens genauso gute, wenn nicht sogar bessere Sicherheitseigenschaften aufweisen. Aufgrund der fehlenden Ende-zu-Ende-Verschlüsselung stufen sie die Messenger WeChat, Google Hangouts und Slack als die am wenigsten sicheren Apps ein. Besonders WeChat und Google Hangouts geraten von den Autoren besonders in Kritik, da sie massive Eingriffe in die Privatsphäre der Nutzerinnen und Nutzer durch die Applikationen verzeichnen [2].

Mittels 10 von den Autoren des Papers [3] festgelegten Kriterien, werden die Messenger Telegram, TextSecure und Threema miteinander verglichen. Dabei legen die Autoren besonders auf die Security-

Eigenschaften der einzelnen Applikationen wert. Sie kommen zum Schluss, dass keine der Messenger die Multi-Device-Funktion unterstützt. Sie statuieren, dass es sich bei Telegram um einen der populärsten Kurznachrichtendienste handelt, jedoch fehlt es der App an vielen Sicherheitsfunktionen wie beispielsweise die standardmäßig aktivierte Ende-zu-Ende-Verschlüsselung. Threema gerät aufgrund der fehlenden Secure-Group-Chat-Funktion und dem nicht offengelegten Quellcode in Kritik. Nach den Autoren ist im Vergleich zu Threema und Telegram, TextSecure der sicherste Messenger.

In dem Paper von Mujaj [4] werden eine Vielzahl an Messaging-Applikationen in den Domänen Security und Usability untersucht. Der Autor konnte im Zuge der Arbeit feststellen, dass die Nutzerfreundlichkeit eine erhebliche Rolle bei der Auswahl der einzelnen Dienste spielt. Dies hat jedoch zur Folge, dass Applikationsentwickler überwiegend Fokus auf das Userinterface legen und die Security bei der Entwicklung als zweitrangig betrachtet wird. Pro Messaging-Applikation werden durch den Autor vereinzelte Maßnahmen zur Verbesserung der jeweiligen Schwachstellen vorgestellt. Konkrete Empfehlungen für zu implementierende Features und Überlegungen zu diesen, können aus der Thesis entnommen werden.

3 Privatsphäre und Anonymität

Das folgende Kapitel beschäftigt sich mit den Definitionen der Privatsphäre und der Anonymität. Zunächst erfolgt die allgemeine Erörterung der Begrifflichkeiten inklusive der Bedeutung innerhalb der Gesellschaft. Im Kontrast dazu wird die Privatsphäre und die Anonymität im Online-Kontext analysiert. Vor allem wird auf die damit einhergehenden Herausforderungen und Problemstellungen eingegangen. Neben den Definitionen werden ebenfalls relevante Schutzziele aufgezeigt und näher beschrieben.

3.1 Privatsphäre

Der Begriff Privatsphäre beziehungsweise Privacy hat in den letzten Jahrzenten eine Vielzahl an Bezeichnungen erlebt. Durchgesetzt haben sich vor allem die beiden wesentlichen Definitionen [5]:

- Privacy as a right
- Privacy as a social norm

Privacy as a right ist besonders in der westlichen Gesellschaft als ein fundamentales Recht gesehen, welches als besonders schützenswertes Gut gilt und von den beiden Autoren Warren und Brandies ebenfalls als *„the right to be let alone“* bezeichnet werden [6]. Die Privatsphäre wird in diesem Zusammenhang als Schutz persönlicher Handlungen, ohne Einmischung oder Überwachung durch die Regierung bezeichnet, und schließt die Vertraulichkeit persönlicher elektronischer Kommunikation und Informationen ein. Ebenso gilt, Informationen über andere ohne deren Einwilligung zu publizieren als untersagt [5]. In einem weiteren Paper definiert Ruth Gavison [7] die Privatsphäre als eine Limitierung des Abrufs von Informationen über andere Leute und setzt dabei drei wesentliche Punkte in den Fokus: Verschwiegenheit, Anonymität und Abgeschiedenheit. Ein weiteres essentielles Konzept der Privacy entspringt den Vereinigten Nationen, wobei die Privatsphäre als geltendes Menschenrecht beschrieben wird. So hat jeder Mensch das Recht seine oder ihre Privatsphäre zu schützen [5].

Privacy as a social norm betrachtet das Thema auf einer sozio-kulturellen Ebene und behandelt nach Westin [8] die Bereiche der sozialen Legitimität. In seinem Paper erklärt er, dass eine Gesellschaft gewis-

se Handlungen und/oder Eigenschaften (zum Beispiel ein Kleid, Frisuren, oder ein Lebensstil) billigen und somit kein Erfordernis besteht, dies in irgendeiner Weise zu reglementieren. Somit werden diese Verhaltensweisen als privat gesehen. Wird im Kontrast dazu Verhalten von der Gesellschaft als inakzeptabel wahrgenommen, so wird dies als ein öffentliches Problem betrachtet. Diese sozialen Normen bestimmen somit was als akzeptabel betrachtet wird, was in weiterer Folge die Unterscheidung jedoch schwierig gestaltet. Konsumiert eine Person beispielsweise Marihuana, so obliegt es der sozialen Norm ob, eine solche Handlung als legitim betrachtet wird oder nicht. Die Unterscheidung zwischen öffentlich und privat wird eben an diese Voraussetzung gekoppelt [8].

Eine weitere prävalente soziale Norm ist die Auffassung *"nothing to hide"*. Solove hat in seinem Paper [9] eine neue Konzeptualisierung von Privatsphäre definiert und gleichzeitig aufgezeigt, dass das Argument „Ich habe nichts zu verbergen“ vorrangig als Messlatte für die eigene Privacy dient. So zeigt er auf, dass die Menschen einer Überwachung durch den Staat oder der massiven Datensammlung persönlicher Informationen nicht kritisch entgegen stehen, da stehts die Auffassung besteht sie hätten nichts zu verbergen. Weiters herrscht vorrangig die Meinung, dass Privacy lediglich dann eine Notwendigkeit darstellt, wenn tatsächlich rufschädigende Informationen an die Öffentlichkeit getragen werden könnten, dies jedoch nur für einen Bruchteil der Bevölkerung zutrifft. Somit sind Eingriffe seitens Regierungen oder privaten Anbietern in die Privatsphäre und die damit verbundenen Konsequenzen lediglich das Problem weniger.

3.1.1 Privacy Online

Aufgrund der Komplexitäten von fortgeschrittenen Technologien im digitalen Zeitalter, sind die oben genannten Definitionen nur bedingt anwendbar. Nachdem die Informations- und Kommunikationstechnologie auch ein fester Bestandteil von Regierungen und Unternehmen wurde, so änderte sich das Bild der Privatsphäre der Benutzerinnen und Benutzer. Privacy wurde als Interesse einer Person betrachtet, maßgeblich zu kontrollieren beziehungsweise zu beeinflussen, wie ihre/seine Daten verarbeitet und benutzt werden [10]. Inkludiert sind damit Daten wie beispielsweise Name, Geburtsdatum, Alter, Geschlecht, Adresse und Kontaktinformationen. Ebenfalls schließt dies auch sensible Daten wie Ethnie und Rasse, politische Einstellung, Religion, Gesundheitsdaten und sexuelle Orientierung mit ein. Besonders sensible Daten müssen gesondert betrachtet werden, da sie ein Individuum angreifbar machen können. In Kulturen, in denen beispielsweise Homosexualität nicht toleriert und sogar strafrechtlich

verfolgt wird, sind Informationen dieser Klassifizierung als besonders heikel einzustufen. Neben dem persönlichen und individuellen Interesse am Schutz der Privatsphäre, existiert besonders im Zeitalter von künstlicher Intelligenz ein kollektives Interesse an persönlichen Daten. So geht ein potentielles Risiko durch Gesichtserkennung gepaart mit Machine Learning aus, da der Einsatz solcher Technologien einen Eingriff in die Rechte und Freiheiten von Minoritäten ermöglicht beziehungsweise begünstigt [11].

Smartphones, soziale Medien und Online-Plattformen erschweren weiter die Wahrung der Privatsphäre, da durch diese digitale Fingerabdrücke hinterlassen werden, anhand die Benutzerin oder der Benutzer identifiziert werden kann [12]. Das ist besonders bei Besuchen von Websites ein großes Problem, da es oftmals nicht ganz klar ist, ob und welche Informationen and Drittanbieter weiter gegeben werden. Die vorgegebenen Privatsphäre-Einstellungen als auch unklare Geschäftsbedingungen erschweren einen sicheren Besuch und können die User/innen der Gefahr aussetzen, personenbezogene Daten offenzulegen. Es stellt sich die Frage, wer diese Daten sammelt, speichert und ein Interesse an diesen hat. Die meisten Regierungen speichern elektronische Daten der Bürger wie Steuerunterlagen, Gesundheitsdaten, Studienbescheinigungen und vieles mehr. Diese gespeicherten Informationen können dann, sofern sie anonymisiert wurden, an Drittanbieter weitergegeben werden um, bestimmte Services zu verbessern. Die Anonymisierung muss jedoch in einem solchen Grad durchgeführt werden, dass eine Rückschließung auf die Identität der Person nicht mehr möglich ist.

Kizza hat in seinem Paper [13] die allgemeinen Verletzungen der Privacy aufgezeigt, welche sich folgendermaßen einteilen lassen: *Eingriff* (unbefugter Zugriff), *Missbrauch von Informationen*, *Abfangen von Informationen* und *Information-Matching*. Ein Unternehmen hat demnach den Schutz von Computersystemen vor widerrechtlichen Eindringen und Missbrauch zu gewährleisten. Sammelt eine Firma Daten über seine Kundinnen und Kunden, speichert sie in eine Datenbank und verarbeitet diese, so müssen die Datensätze vor einem unautorisierten und zweckentfremdeten Zugriff geschützt werden. Diese Verpflichtung schließt ebenfalls den widerrechtlichen Verkauf von Informationen mit ein. Weiters sind Firmen dazu verpflichtet, ihre UserInnen vor dem Abhören, also dem Abfangen von Informationen durch Kommunikationskanäle, zu schützen. Das Verfahren „Matching-Records“ von verschiedenen Datensätzen aus unterschiedlichen Quellen ist dabei ebenfalls zu betrachten, da ältere als auch fehlerhaft zusammengesetzte Einträge die Konsistenz der Datenbanken beeinträchtigen [7].

3.1.2 Schutzziele

Die sieben Schutzziele entspringen dem Prinzip „Privacy by Design“ und stellen die Anforderungen an eine moderne Datensicherheit und zählen bereits als feste Elemente des europäischen Datenschutzes. So sollen diese Elemente als Rahmenwerk zur Wahrung der Privatsphäre dienen und die allgemeine Sicherheit der Nutzerinnen und Nutzer bestmöglich gewährleisten. In dem Paper von Bock und Rost [14] werden die sieben Grundsätze (Fundamentals) als auch deren Anforderungen systematisch aufgelistet und folgendermaßen beschrieben:

1. **Proactive not Reactive; Preventative not Remedial**

   Der erste Grundsatz befasst sich mit der Notwendigkeit einen proaktiven Ansatz beim Datenschutz zu verfolgen, anstatt reaktiv in einzelnen Phasen nachzubessern. Somit sollen Überlegungen hinsichtlich dem Schutz der Privatsphäre vorab in die Planungsphasen miteinfließen und berücksichtigt werden.

2. **Privacy as Default**

   Dabei sollen es die Standardeinstellungen in jedem System zunächst verbieten, jegliche Form personenbezogener Daten zu verarbeiten. Insofern die Userin oder der User keinerlei Freigaben explizit erteilt, so muss der maximal zu erreichende Grad an Privacy gewährleistet sein.

3. **Privacy embedded into Design**

   Der Schutz der Privatsphäre muss nach diesem Ziel so implementiert werden, dass die Funktionalität der Systeme nicht beeinträchtigt wird, dieser jedoch holistisch und integrativ umgesetzt ist. Privacy darf dabei nicht als reine Zusatzfunktion oder Add-On, sondern als wesentlicher Bestandteil, gehandhabt werden.

4. **Full Functionality - Positive Sum, not Zero-Sum**

   Es gilt die Berücksichtigung aller Interessensgruppen mit dem Ergebnis einer Win-Win-Situation. Die Verbraucher/innen sollen nicht zwischen widersprüchlichen Optionen wie beispielsweise Datenschutz versus Sicherheit wählen müssen. Diese beiden Eigenschaften müssen komplementär in den Systemen integriert sein.

5. **End-to-End-Security, Lifecycle Protection**

   Beschreibt die Anforderung für einen kompletten und abgedeckten Schutz durch den gesamten Lebenszyklus. Die Sammlung von Daten setzt den angemessenen Schutz für den Zeitraum der Aufbewahrung bis zur sicheren Löschung nach der Zweckerfüllung voraus. Die Prozesse der Datenverarbeitung müssen also von Anfang bis Ende berücksichtigt werden und umfassen den

gesamten Lebenszyklus eines IT-Prozesses.

6. Visibility and Transparency

Die Verarbeitung personenbezogener Daten setzt die Prüfbarkeit von Systemen und Prozessen voraus. Durch unabhängige Prüfungen soll gewährleistet werden, dass die Systeme autonom von Geschäftspraktiken oder Technologien, die deklarierten Maßnahmen und Ziele verfolgt.

7. Respect for User Privacy

Dieser Grundsatz fordert die Betreiber von IT-Systemen auf, die Lösungen benutzerzentriert zu gestalten. Die Interessen der Einzelpersonen ebenso wie die Benutzerfreundlichkeit der Systeme stehen dabei um Vordergrund.

3.1.3 Die sieben Cs

Privacy-Lobbyisten als auch Advokaten sehen Eingriffe in die Privatsphäre als eines der signifikantesten Probleme unserer Zeit. Persönliche Daten werden fast ausschließlich in elektronischer Form verarbeitet und zwischen verschiedenen Stellen geteilt. Das exponentielle Wachstum an genutzten Services, welche eine Offenlegung von privaten Daten voraussetzt, führt zu einer immer größer werdenden öffentlichen Diskussion, wobei Bedenken bezüglich des Datenschutzes stetig lauter werden [15]. Jutla und Bodorik haben in ihrem Paper [16] sieben Kriterien definiert, welche als Vorrausetzung zur Steuerung der Privatsphäre-Einstellungen in E-Business-Applikationen fungieren:

1. Comprehension

Die Benutzerinnen und Benutzer müssen in Kenntnis darüber gesetzt werden, wie persönliche Daten genutzt werden, wer und zu welchem Zweck diese sammelt und verarbeitet. Weiters müssen User/innen darüber informiert werden, welche Parteien Zugriff auf diese Datensätze haben, welche Limitierungen bezüglich der Datenverarbeitung existieren, wie lange die Informationen gespeichert werden als auch über das Verfahren nach der Aufbewahrungsfrist.

2. Consciousness

Die User/innen müssen darüber Informiert werden, wann: eine Datensammlung erfolgt, ein Vertrag mit einem Datensammler zu Stande kommt und die Daten verfallen. Ebenso muss aufgezeigt werden, mit wem die Datensätze geteilt und wer auf diese nachträglich Zugriff erhält.

3. Choice

In Bezug auf die Datensammlung muss die Option zum *Opt-In* oder *Opt-Out* zur Verfügung stehen, ob Informationen bereitgestellt werden. Weiters muss auch die Möglichkeit für Benutzerin-

nen und Benutzer eingräumt werden, Korrekturen an den Daten vorzunehmen.

4. Consent

Besonders wichtig ist die explizite und unmissverständliche Einwilligung der Anwenderinnen und Anwender bezüglich der Datensammlung, deren Verarbeitung und Aufbewahrung. Optionen zur Zustimmung müssen explizite Mechanismen zum Verständnis und Bewusstsein über die Sachlage, Limitierungen und Wahlmöglichkeiten integrieren.

5. Context

Privatsphäre-Einstellungen müssen je nach situationsbedingtem Kontext geändert werden können. So mach es beispielsweise einen Unterschied, ob eine Telefonnummer an einen Service-Desk Mitarbeiter durchgegeben wird gegenüber einer Transaktion auf einer Online Plattform, wo durch die Digitalisierung und den bereitgestellten Informationen die Benutzerin oder der Benutzer zweifelsfrei identifizierbar ist. Ebenso ist der Kontext der Daten ein wesentlicher Faktor, da sensible Informationen wie beispielsweise Gesundheitsdaten der selben Person je nach Gegebenheit verschieden interpretiert werden können.

6. Confinement

Den User/innen muss die Möglichkeit geboten werden Limitierungen zu setzen, wer auf ihre persönlichen Informationen und zu welchem Zweck Zugriff erhält und wo und wann diese Daten gespeichert werden.

6. Consistency

Der Benutzer oder die Benutzerin sollte sich im Klaren sein was passiert, wenn Aktionen mit ihren persönlichen Informationen durchgeführt werden. Das das heißt, bestimmte Verfahren sollten absehbar sein, wenn der Benutzer persönliche Informationen herausgibt.

3.2 Anonymität

Nutzerinnen und Nutzer achten immer mehr auf ihre Privatsphäre beim Surfen, so zeigen Surveys das es hierfür verschiedene Gründe gibt [17]. Die Motivation seine/ihre Identität im Internet zu verbergen wurde in verschiedenen Studien erhoben und lässt darauf schließen, dass sie sich einerseits auf bestimmte Online-Aktivitäten, andererseits auf Benutzergruppen projizieren lässt.

Die Anonymität im Online-Kontext ist dabei ein zweischneidiges Schwert, so kann sie einerseits für Freiheit und Sicherheit sorgen, andererseits für schadhafte und illegale Handlungen im Netz dienen. Die Menschen nutzen den Schutz der Anonymität ebenfalls um soziale Risiken zu vermeiden, wenn bei-

spielsweise kritische Themen, in denen die eigene Meinung das persönliche Ansehen beziehungsweise das charakterliche Erscheinungsbild in ein negatives Licht rücken, behandelt werden. Um die Anonymität im Internet zu sichern, existieren verschiedene Mittel auf denen zurückgegriffen wird, darunter Proxy Server, SSL-Technologie, temporäre Mail-Services und Cookie Manager [18]. Diese Technologien werden in der Regel nur von wenigen Benutzerinnen und Benutzer verwendet, obgleich sie Bedenken über ihre Privacy und Sicherheit äußern. So wird in der Praxis eher Wert darauf gelegt, dass eigene Erscheinungsbild gegenüber anderen mittels modifizierten persönlichen Informationen, verschiedenen Mail-Accounts und angepassten Social-Network-Profilen zu verfälschen [19].

Um die Anonymität (zu englisch Anonymity) im wissenschaftlichen Bereich zu erläutern wird in den meisten Fällen die Definition von Gary T. Marx [20] herangezogen, welcher die Frage behandelt, ob eine Person anhand einer der folgenden 7 Dimensionen identifizierbar ist: Offizieller Name, Standort, zurückführbare Pseudonyme, nicht-zurückführbare Pseudonyme welche Indizien zur Identität liefern, aufschlussreiche Verhaltensmuster, Zugehörigkeit sozialer Gruppen sowie Informationen, Kenntnisse oder Gut um auf persönliche Charakteristiken zu schließen. Wird die Anonymität im online Kontext betrachtet, so müssen die Unterbegriffe *Unlinkability*, *Unobservability* als auch *Pseudonymity* gleichermaßen erläutert werden. Um die Terminologie Anonymität zu standardisieren als auch Klarheit in die verschiedenen Konzepte in diesen Bereich zu schaffen, definieren Pfitzmann und Köhntopp die Anonymität selbst folgendermaßen:

„Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.[21]"

Dabei ist das Anonymitätsset das Set aller möglichen Personen, welche eine Aktion setzen. Das heißt, eine Senderin oder ein Sender ist dann anonym, wenn er/sie sich in einem Set weiterer potentieller Sender befindet – dem Anonymitätsset, welches selbst als ein Subset aller möglicher Sender weltweit gesehen werden kann. Selbiges gilt für die Empfängerin beziehungsweise den Empfänger, da er/sie sich im jeweiligen Empfänger-Anonymitätsset befindet. Die beiden Sets können dabei disjunkt, gleich oder überlappend sein. Der Grad an Anonymität steigt mit größer werdenden Anonymitätssets als auch der gleichmäßigen Verteilung der Sender- und Empfängersets, in denen sich Sender und Receiver befinden. Weiters definieren die Autoren Unlinkability wie folgt:

„With respect to the system of which we want to describe anonymity, unobservability, or pseudonymity properties, unlinkability of two or more items means that within this system, these items are no more and no less related than they are related concerning the a-priori knowledge.[21]"

So ist die Wahrscheinlichkeit, dass zwei oder mehr Elemente (zum Beispiel Nachrichten) einander zugehörig sind, vor (A-Priori-Knowledge) und nach (A-Posteriori-Knowledge eines Angreifers) einer Systemausführung, dieselbe. Zwei Nachrichten sind also dann „unlinkable“, wenn die Wahrscheinlichkeit, dass diese vom selben Sender kommen und/oder vom selben Empfänger erhalten werden, der A-Priori-Knowledge gleicht. Wird das Senden und Empfangen von Nachrichten als Interessens-Element (IE) betrachtet, kann die Anonymität als Unlinkability eines IE und Identifier eines Subjekts (ID) definiert werden. Die Anonymität eines IE wird erreicht, wenn dieses einer ID nicht zugeteilt werden kann, die Anonymität einer ID, kann diese keiner IE zugeteilt werden. Die Sender-Anonymität beschreibt somit die Eigenschaft, dass eine bestimmte Nachricht keinem Sender zugeordnet und gleichermaßen keinem Sender eine Nachricht zugeordnet werden kann. Das selbe Prinzip gilt ebenfalls für die Empfänger-Anonymität. Eine abgeschwächte Form der Sender- beziehungsweise Empfängeranonymität ist die so genannte *Relationship-Anonymity*. Dabei kann zwar nachvollzogen werden, wer welche Nachrichten versendet als auch wer welche Nachrichten empfängt, jedoch können die beiden Kommunikationspartner nicht zusammengeführt werden.

Im Kontrast zu *Anonymity* und *Unlinkability*, welche nicht exklusiv das Senden und Empfangen (IE oder auch im Englischen IOI) von Nachrichten verbergen, ist genau dies das Ziel der *Unobservability*. Die Autoren definieren diese Eigenschaft folgendermaßen:

„Unobservability is the state of IOIs being indistinguishable from any IOI at all.[21]“

Somit ist es für einen Beobachter nicht erkennbar, ob überhaupt Nachrichten versendet oder empfangen werden. Gleich dem Anonymitätsset, existierten Unobservability-Sets, welche die Unbeobachtbarkeit in den Kommunikationsnetzwerken sicherstellen. Diese Sets teilen sich wiederum in zwei Bereiche, dem Sender-Unobservability- und dem Receiver-Unobservability-Set, welche jeweils die Parteien schützt.

Bei *Pseudonymen* handelt es sich um Identifier von Personen, also den SenderInnen und EmpfängerInnen. Per Definition ist jede Person, welche durch ein Pseudonym identifizierbar ist, der so genannte Holder. Die Autoren definieren die Pseudonymity als:

„Pseudonymity is the use of pseudonyms as IDs.[21]“

Die Sender-Pseudonymity ist somit der Einsatz einer Pseudonymität seitens der Senderin oder des Senders, die Recipient-Anonymity umgekehrt für die Empfängerin oder den Empfänger. Technisch gesehen ist ein Pseudonym ein Bit-String, welcher einzigartig als ID existiert und den Holder und seine/ihre IE (zum Beispiel Nachrichten) authentifiziert. Der Einsatz von Pseudonymen garantiert jedoch nicht

zwangsweise Anonymität. So kann der mehrfache Einsatz eines einzigen Namen eine Linkablility mit sich ziehen. Dritte können beispielsweise die Identität eines Holders oder einer Holderin im Zuge laufender Ermittlungen oder zum Zweck strafrechtlicher Verfolgungen preisgeben. Der Grad der Anonymität steigt, je unwahrscheinlicher es wird, vom Pseudonym auf die Person zu schließen.

3.2.1 Das Dilemma der Online-Anonymität

Anonymisierung im Internet fördert die Reduzierung der Verantwortlichkeit, senkt die Hemmschwelle und hat einen depersonalisierenden Effekt auf das Veralten und der Kommunikation. Besonders kriminelle Handlungen werden im Schatten der Anonymität erleichtert, da die Chance zur Rechenschaft gezogen zu werden sich mit den stetig weiterentwickelten Technologien sinken. Jedoch zieht die minimierte Haftung auch positive Effekte nach sich, so begünstigt die Anonymität auch das Probieren neuer Dinge, Ideen zu entwickeln, freie Meinungen zu bilden als auch die freie Meinungsäußerung [22]. Gleichermaßen bietet die Online-Anonymity den Schutz vor Repressalien und Verfolgung, was besonders Randgruppen beziehungsweise unterdrückten Bürgern zugutekommt [23].

Im Kontrast dazu ermöglicht die Verschleierung der eigenen Identität vor allem in Chaträumen, Foren und Message-Boards Beleidigungen, Hassreden und Aufforderungen zu Gewalttaten. Diese Verhaltensweisen haben dazu geführt, dass immer mehr seitens der Service Anbieter darauf gedrängt wird, die Angabe des validen Namens zu erzwingen. So setzt Google für die Nutzung von SNS und Google+ wahre Angaben bezüglich der Person voraus [24]. Südkorea hat im Kampf gegen Hasspostings das so genannte *Real Name Verification Law* erlassen, so muss jede Bürgerin und jeder Bürger eine von der Regierung ausgegebenen Identifikationsnummer angeben, bevor Postings getätigt werden können [25]. Die Arbeit von Cho [26] hat jedoch ergeben, dass die Verbreitung beleidigender Postings trotz Angabe persönlicher Daten weiter angehalten hat. Ebenfalls hat seine Studie ergeben, je länger und erfahrener eine Userin oder ein User mit dem Internet ist, desto geringer ist die Wahrscheinlichkeit missbräuchlicher Handlungen durch diese Person. Somit hat dieses Verhalten weniger mit tatsächlichen Angaben als mit entsprechendem Hintergrundwissen zu tun.

Die Studie von Stoehrel und Lindgren [27] befasst sich mit den Aktivitäten der Gruppe Anonymous, welche eine eher politisierte Zielrichtung verfolgen. Unter anderem richten sich Angriffe auf Scientology (Operation Chanology), Visa, Mastercard und auch gegen die Wall Street (Occupy Wall Street). Ebenso wird aufgezeigt, dass die Attribute der Anonymität – kaum Rechenschaftspflicht, Enthemmung

und Deindividualisierung - zu einem starken Gefühl kollektiver Identität und Aktionsbereitschaft beiträgt. Dabei werden diese Handlungen von der Gruppe als eine Form des friedlichen Protests angesehen.

Die Studien zeigen somit, dass die Anonymisierung im Internet als ein Werkzeug zur freien Meinungsäußerung, Gemeinschaftsbildung und ebenso zu einem Instrument kollektiven Handelns dienen kann. Auch im sozialen Kontext profitieren Userinnen und User, da die Anonymität als Schutz der Intimität und offenen Kommunikation einen wesentlichen Beitrag für eine demokratische Gesellschaft liefert. Obgleich die Absicht hinter der Anonymisierung eine gute ist, so wird sie auch missbräuchlich in Form krimineller Handlungen wie beispielsweise Cyberbullying, das Schüren von Hass und Intoleranz bis hin zur Mobilmachung zu Gewalttaten eingesetzt. Die Frage, ob die potentiellen Nachteile und Risiken die Vorteile und Chancen der Anonymität im Internet überwiegen oder nicht, ist bis heute eine offene Debatte welche, schier endlos erscheint [24].

4 Messaging Technologien

Im folgenden Kapitel werden die einzelnen Messaging-Applikationen in den Domänen Privatsphäre/Anonymität, Sicherheit und Benutzerfreundlichkeit bewertet. Als Bewertungsgrundlage werden pro Domäne zu überprüfende Eigenschaften und entsprechende zu erfüllende Kriterien definiert. Als Ergebnis werden die Kurznachrichtendienste tabellarisch gegenübergestellt, so können Leserinnen und Leser auf einem Blick nachvollziehen, welche Applikation in welcher Domäne besonders starke beziehungsweise schwache Eigenschaften aufweisen.

A. Privacy / Anonymity Properties

Proxy-Server: Nachrichten können nicht nur über das eigene Netzwerk, sondern über einen so genannten Proxy-Server versendet werden. Der Server fungiert dabei als „Mittelsmann“ zwischen Sender und Ziel. Versendete Nachrichten kommen zunächst beim Proxy an und werden an das Ziel weitergeleitet. Der Vorteil daran ist, dass die Nachrichten mit der IP-Adresse des Servers ankommen, somit wird kein digitaler Fingerabdruck hinterlassen. Dies ist vor allem dann sinnvoll, wenn Messenger in bestimmten Ländern gesperrt beziehungsweise blockiert sind. Ebenso wird durch die Verwendung eines Proxys ein hohes Maß an Anonymisierung geschaffen, da die eigene IP-Adresse unter Verwendung des Services verschleiert wird.

Minimum Data Collection: Das Sammeln und Speichern von Nutzerdaten als auch die Weitergabe dieser Informationen stellt bei vielen Anbietern von Messengern ein großes Problem dar. Neben den erforderlichen Daten zur reibungslosen Nutzung von Applikationen werden oftmals sensible Informationen über die Benutzer gesammelt [28]. Das Prinzip der Datenminimierung gilt hierbei als Bewertungskriterium. So sollen lediglich Informationen, welche für den Messenger technisch erforderlich sind, von den Anbietern gesammelt und gespeichert werden.

Server Location: Dieses Kriterium setzt sich mit den Serverstandorten als auch mit der Datenhoheit der jeweiligen Messengern auseinander. Um die Privatsphäre der Nutzerinnen und Nutzer bestmöglich sicherzustellen, sollten sich die betriebenen Server in als datenschutzrechtlich sicher eingestuften Län-

dern befinden. Es soll somit gewährleistet werden, dass staatliche Nachrichtendienste wie beispielsweise der US Auslandsgeheimdienst NSA keine rechtlichen Befugnisse zur Datenspeicherung und Analyse geltend machen kann. Vorzugsweise sollten die im Einsatz befindlichen Server innerhalb der Europäischen Union liegen, da der Betrieb der Datenschutzgrundverordnung unterliegt.

Anonymous Usage: Diese Eigenschaft setzt voraus, dass die erfolgreiche Installation als auch der Betrieb der Applikation ohne Angabe persönlicher Informationen wie beispielsweise Telefonnummer oder Mail-Adresse möglich ist. Der Messenger kann von den Benutzerinnen und Benutzer anonym ohne Angabe jeglicher personenbezogener Daten verwendet werden.

No Advertising Information: Beschreibt den Aspekt eines Messengers ob persönliche Informationen zum Zweck der personalisierten Werbung oder zur verbesserten Userexpirience an Drittanbieter weitergegeben werden. Hierbei wird auch vom so genannten Profiling gesprochen, wobei automatisiert Nutzerdaten gesammelt und analysiert werden, um maßgeschneiderte Werbung für die Nutzerinnen und Nutzer zu generieren.

GDPR Compliance: Seit dem 25. Mai 2018 müssen in Europa operierende Firmen ihre Services entsprechend der Datenschutz-Grundverordnung gestalten. Ziel ist es, die Rechte der Nutzer in Bezug auf ihre persönliche Privatsphäre und Datenschutz zu wahren. Chat-Services beziehungsweise Messaging-Applikationen müssen folgendes Kriterium erfüllen, um Konformität gegenüber der Datenschutz-Grundverordnung zu erreichen:

Konventionelle Chat-Services dürfen nur im privaten Bereich verwendet werden. Sobald geschäftliche Kontakte auf dem Mobiltelefon gespeichert werden, wird dies nicht mehr als rein privater Gebrauch behandelt. Die Benutzung von Messaging-Applikationen für Geschäftszwecke stellt einen Verstoß gegen die Datenschutz-Grundverordnung dar, sofern Adressbücher und weitere Nutzerdaten von Applikationen automatisch eingesehen und gesammelt werden. Die Sammlung und Speicherung der Informationen ist nur dann konform Gegenüber der DSGVO, wenn jeder einzelne Kontakt diesem Vorgang einwilligt [29].

Fälschlicherweise wird argumentiert, dass die Datenschutzgrundverordnung bei Privatpersonen nicht relevant ist, da lediglich Verstoße im gewerblichen Umfeld sanktioniert werden. Die DSGVO räumt gerade den Benutzerinnen und Benutzern Rechte ein, über ihre personenbezogenen Daten zu bestimmen und den Gebrauch zu kontrollieren. So steht es Privatpersonen rechtlich zu, die Herausgabe aller gesammelten Daten zu verlangen. Ebenso besteht das Recht, alle Informationen nach Wunsch der Kundin beziehungsweise des Kunden zu ändern als auch zu aktualisieren. Der wohl wichtigste Aspekt der Datenschutz-Grundverordnung ist das Recht auf Löschung aller durch das Unternehmen gesammelten

Datensätze als auch die Einholung des expliziten Einverständnis des Nutzers, bevor die personenbezogenen Daten gespeichert und verarbeitet werden [30]. Für die Bewertung dieses Kriteriums wird der private Gebrauch berücksichtigt.

Deletable Messages: Bereits versendete Nachrichten müssen durch die Userin oder den User wieder für alle Parteien gelöscht werden können. Dies gilt für Privatnachrichten als auch für Gruppenchats.

Self Destructive Messages: Dabei handelt es sich um Nachrichten, welche nach einer bestimmten beziehungsweise von den Benutzern vorkonfigurierten Zeit automatisch gelöscht werden können. Es muss gewährleistet werden, dass auf beiden Seiten der Kommunikationspartner die Nachrichten nicht mehr rückführbar sind.

Screenshot Detection: Beschreibt die Eigenschaft eines Messengers, getätigte Screenshots von Nachrichteninhalten seitens der Kommunikationsparteien zu erkennen. Werden Screenshots von der Empfängerin oder dem Empfänger getätigt, so muss die Messaging-Applikation die Senderin beziehungsweise den Sender über diesen Vorgang informieren.

B. Security Properties

Cryptographic Primitives: Secure-Messaging setzt unter anderem voraus, dass die Kommunikation Ende-Zu-Ende-Verschlüsselt ist und die im Einsatz befindlichen kryptografischen Primitiven zum aktuellen Stand der Technik gehören. Das bedeutet, dass durch die implementierte Kryptografie die verschlüsselten Nachrichten nicht ohne einem unzumutbaren Aufwand entschlüsselt und von Dritten gelesen werden können.

End-to-End Encryption: Bei End-to-End-Encryption handelt es sich um die Verschlüsselung der versendeten Daten über sämtliche Übertragungsstationen hinweg. Lediglich die involvierten Kommunikationspartner, also die jeweiligen Endpunkte der Kommunikation, sind in der Lage, die Nachrichten zu entschlüsseln und folgend zu lesen. Die Verschlüsselung als auch die Entschlüsselung der Nachrichten erfolgt ausschließlich auf dem Endgerät und erfordert keine weitere Infrastruktur. Somit verhindert dieser Mechanismus das Abhören der ausgetauschten Nachrichten durch Serviceprovider und Geheimdienste inklusive der Betreiber der genutzten Messaging-Applikation selbst.

Forward Secrecy: Um verschlüsselten Datenverkehr nachträglich zu entschlüsseln, muss ein Angreifer zunächst die Nachrichten in verschlüsselter Form aufzeichnen. Gelangt dieser zu einem späteren Zeitpunkt in den Besitz des geheimen Schlüssels, so können alle bis dahin aufgezeichneten Daten durch Ableitung des Sitzungsschlüssels rückwirkend entschlüsselt werden. Das stellt eine besonders große Problematik dar, denn durch die immer größer werdende Leistung von Computern, kann nicht ausge-

schlossen werden, dass momentan sichere Schlüssel zukünftig errechenbar werden. Ein ausgemachter Sitzungsschlüssel darf nur für einen definierten Zeitraum gültig sein, bis dieser für weitere Kommunikationen erneuert werden muss. Die nachfolgenden Schlüssel stehen in keinem Bezug zueinander und sind nicht gegenseitig ableitbar. Durch das Bekanntwerden eines einzelnen Schlüssels, können keine Folgeschlüssel ermittelt werden. Eine nachträgliche Entschlüsselung vergangener Nachrichten ist somit nicht möglich.

Backward Secrecy: Das Prinzip gleich der Forward Secrecy, jedoch können durch den Verlust der Langzeitschlüssel nachfolgende verschlüsselte Nachrichten nicht durch eine Angreiferin oder einen Angreifer entschlüsselt werden.

MiTM-Prevention: So genannte Man-in-the-Middle-Attacken sind eine sehr populäre Methode für Angreifer, um den Datenverkehr zwischen Sender und Empfänger abzuhören. Es erfolgt eine Form des Session-Hijacking, wobei nicht nur das mobile Endgerät, sondern auch deren Applikationen betroffen sein können. Über einen von der Angreiferin oder vom Angreifer kontrollierten Proxy wird unbemerkt der Datenverkehr der betroffenen Parteien abgefangen. Bei Messaging-Applikationen werden Schwachstellen im Authentifizierungsvorgang gezielt ausgenutzt, um die Kommunikation abzufangen. Um MiTM-Attacken zu verhindern, müssen Applikationen daher einen starken Authentifizierungsmechanismus implementiert haben. Eine Sicherheitsfunktion, welche Man-in-the-Middle-Attacken verhindern soll, ist die so genannte *Fingerprint-Verification*. Nutzerinnen und Nutzer der Messaging Applikation sind mittels offline Channel oder einem QR-Code in der Lage, die Identitäten der jeweiligen Kommunikationspartner durch den Vergleich der entsprechenden Werte zu verifizieren. Stimmt der Fingerprint überein, so können die Parteien eine sichere Kommunikation aufbauen und ein Abhören ausschließen.

Disk-Encryption: Um digitale Informationen auf einem Gerät vor fremden Zugriff zu schützen, konvertieren Verschlüsselungstechniken die Daten in unlesbaren und nicht zu entschlüsselnden Code. Disk-Encryption-Software beziehungsweise Hardware verschlüsselt dabei jedes einzelne Bit an Daten als auch ganze Datenvolumen, um einem unautorisierten Zugriff entgegenzuwirken. Die Daten sollten durch die Messaging-Applikation in verschlüsselter Form auf den mobilen Endgerät gespeichert werden, damit bei einem physischen Zugang keinerlei Daten extrahiert werden können.

Secure Group Chat: Die Gruppenchat-Funktion ist bei den meisten Messaging-Applikation standardmäßig implementiert, doch es wird ebenfalls vorausgesetzt, dass die Kommunikationen unter den Teilnehmerinnen und Teilnehmer den Sicherheitsanforderungen des Secure-Messaging entspricht.

B. Usability Properties

Multi-Device-Support: Userinnen und Usern muss die Möglichkeit geboten werden, die Applikation auf mehreren Geräten parallel zu verwenden, ohne dabei einen Logout tätigen zu müssen. Ebeso muss das Versenden als auch Empfangen der Nachrichten auf jeden Gerät gleichermaßen funktionieren. Die Sicherheit und der Datenschutz darf jedoch nicht durch dieses Feature geschwächt werden, so müssen die Applikationen auch beim Multi-Device-Support über eine entsprechende Ende-zu-Ende-Verschlüsselung verfügen. Die Datensynchronisierung zwischen den jeweiligen Geräten muss ebenfalls unterstützt werden.

E2E by Default: Die End-to-End-Encryption muss bereits standardmäßig aktiviert sein, sodass die Nutzerinnen und Nutzer keinem Mehraufwand bei der Bedienung der Applikation ausgesetzt sind. Die Messaging-App muss den Usern automatisch das höchste Maß an Sicherheit bieten, ohne weitere Interaktionen oder Konfigurationen seitens dieser vorauszusetzen.

Easy Contact Discovery: Nach erfolgreicher Installation der Messaging-Applikation müssen Kontakte, die den selben Dienst verwenden, durch einen automatisierten Mechanismus erfasst werden. Die Userin oder der User sollte nicht manuell nach Kontakten suchen beziehungsweise diese hinzufügen müssen.

Easy Key Maintenance: Die von der Messaging-Applikation eingesetzten Schlüssel zur sicheren Kommunikation dürfen keine Wartung durch die Anwenderinnen und Anwender voraussetzen. Benutzerfreundliche Systeme vollziehen das Schlüsselmanagement wie Signieren und Erneuern abgelaufener Keys automatisch.

Transcript Consistency: Beschreibt die Eigenschaft innerhalb Gruppenchats, dass Nachrichten konsistent und für alle Teilnehmer in der selben Reihenfolge geladen und angezeigt werden.

Asynchronous: Werden Nachrichten an eine Teilnehmerin oder einen Teilnehmer versendet, so setzt die Applikation nicht voraus, dass diese beziehungsweise dieser Kommunikationspartner/in zur Zeit der Datenübermittlung online und bereit zum Empfang ist. Bei einem Verbindungsaufbau durch den/die Empfänger/in werden die Nachrichten automatisch zugestellt, obgleich der/die Sender/in zur Zeit des Empfangs online oder offline ist.

No Monetary Costs: Die Messaging-Applikation ist für die Nutzerinnen und Nutzer frei verfügbar. Für die Verwendung der Software fallen keine monetäre Kosten an.

1 Viber

Bei Viber handelt es sich um einen Chat-Dienst für Mobiltelefone und Desktop-Computern mit über 900 Millionen Nutzern weltweit. Die Applikation ermöglicht neben dem Versand von Sofortnachrichten auch die IP-Telefonie über das Internet sowie Anrufe über Fest- und Handynetze. Bei diesem Dienst handelt es sich um einen Messenger mit den wohl meisten Funktionen verglichen zur Konkurrenz. Besonders durch die Möglichkeit mit Teilnehmer, welche den Dienst selbst nicht nutzen, in Kontakt zu treten, macht Viber zu einer attraktiven Lösung im Bereich Instant-Messaging. Voice- und Video-Calls wurden in Viber schon vor WhatsApp und Telegram entwickelt und implementiert, so erfreuen sich die User einer besseren Qualität im Vergleich zu anderen Anbietern. Der Messenger wirbt ebenso mit seiner Community-Funktion. Dabei handelt es sich um einen Gruppenchat mit unlimitierter Teilnehmerzahl und verschiedenen Konversationseinstellungen – ein soziales Netzwerk innerhalb des Nachrichtendienstes [31].

1.1 Privacy / Anonymity Properties

Proxy-Server: Der Messenger unterstützt die Verwendung eines Proxy durch die manuelle Konfigurationen in den Einstellungen. Viber verwendet so genannte SOCKS5-Proxies, welche UDP und TCP basiert agieren und zurzeit als Stand der Technik betrachtet werden können [32].

Minimal Data Collection: Bei der Registrierung zum Gebrauch des Services werden von Viber persönliche Informationen wie Name, E-Mail Adresse, Geburtsdatum, Telefonnummer als auch Rechnungsdaten gespeichert und verwaltet. Ebenfalls greift die Messaging-Applikation auf das persönliche Adressbuch der Nutzerin beziehungsweise des Nutzers zu. Dabei wird eine Kopie der gesamten Telefonnummern und Namen der Kontakte gesammelt und auf den firmeneigenen Servern gespeichert. Diese Speicherung erfolgt nicht ausschließlich nur bei Kontakten, welche ebenfalls das Service nutzen, sondern für sämtliche im Adressbuch hinterlegten Kontakte. Erfolgt das Sign-In in den Viber Account mittels Drittanbietern wie Facebook oder Twitter, so erklärt sich die Userin oder der User damit einverstanden, dass Informationen aus diesem sozialen Netzwerk ebenfalls gesammelt werden dürfen. Informationen über weitere Applikation als auch Spiele, welche über Viber heruntergeladen werden, sind ebenfalls Gegenstand der Datensammlung. Die Messaging-Applikation behält sich weiters vor, demographische als auch zusätzliche Kontaktinformationen genauso wie technische Daten über das verwendete Endgerät inklusive Informationen über das verbundene Netzwerk zu sammeln. Das Verhalten bei der Nutzung der Applikation wird ebenfalls von Viber aufgezeichnet. Darunter fallen Informationen wie die Anzahl der versendeten Nachrichten und Anrufe, typische Destinationen, Anruflänge, Netzwerkinformationen und

vieles mehr [33].

Server Location: Die zur Kommunikation verwendeten Server des Messaging-Dienstes sind global verstreut und beschränken sich nicht auf den europäischen Raum. Die Speicherung als auch die Verarbeitung personenbezogener Daten erfolgt auf Servern in den Vereinigten Staaten, Asien, Europa (inklusive Russland), Australien und Brasilien. Das bedeutet, dass persönliche Informationen der Nutzerinnen und Nutzer in Ländern verarbeitet werden, in denen Datenschutz als auch Privatsphärerichtlinien nicht dem Stand der europäischen Datenschutz-Grundverordnung entsprechen [33].

Anonymous Usage: Bei der Registrierung müssen Userinnen und User ihre personenbezogenen Daten wie vollständiger Name, E-Mail Adresse, Geburtsdatum, Alter sowie Telefonnummer angeben. Diesen Informationen werden seitens Viber, mit Zusendung eines Codes auf die angegebene Rufnummer, validiert und die Registrierung abgeschlossen. Somit ist die anonyme Verwendung des Messaging Dienst nicht möglich, da auf jeden Fall eine gültige Anschlussnummer angegeben werden muss [34].

No Advertising Information: Um das Verhalten der Benutzerinnen und Benutzer zu verfolgen, verwendet Viber HTTP-Cookies, Informationen aus dem lokalen HTML5 und Flash-Speicher, Web-Beacons/GIFs, eingebettete Scripts und E-Tags. Diese Erstparteien-Cookies werden vom Unternehmen selbst verwaltet und dienen in erster Linie der Funktionalität des Messengers selbst, die implementierten Drittparteien-Cookies der Partnerunternehmen liegen außerhalb des Machtbereichs von Viber und verwalten die personenbezogenen Daten gemäß den eigenen Datenschutzrichtlinien und Praktiken. Die Messaging-Applikation verwendet ebenfalls zielbezogene Trackingtechnologie. Das bedeutet, dass Informationen basierend auf dem Nutzerverhalten gesammelt und analysiert werden, damit Werbepartner für die Userinnen und User maßgeschneiderte Werbung generieren können. Aktivitätsdaten werden mit den Partnerfirmen geteilt um deren Marketingmaßnahmen zu optimieren. Bei der Registrierung stimmen die Nutzerinnen und Nutzer der Platzierung von einzigartigen Werbeidentifikatoren zu, welche in Kooperation mit Drittpartei-Werbepartnern als auch Werbedienstleistern wie Google, zur Sammlung und Auswertung von Benutzer- und Geräteinformationen dienen. Standortdaten werden ebenfalls für Werbezwecke verwendet, so wird den Usern die so genannte „interessen- und standortbasierte Werbung“ innerhalb des Messengers angezeigt. Soziale Plugins auf der eigenen Website des Unternehmens dienen dem Datenaustausch zwischen Viber und sozialen Netzwerken. Ist die Benutzerin oder der Benutzer auf einem sozialen Netzwerk registriert, so sendet das Plugin Daten an dieses und verknüpft die Informationen mit bereits vorhandenen Nutzerdaten [35].

GDPR Compliance: Den Nutzerinnen und Nutzern steht es jederzeit frei, ihre angegebenen Daten in den Einstellungen zu ändern beziehungsweise zu ergänzen. Das Recht auf Änderungen wird durch Viber

somit eingehalten. Vor der Sammlung als auch der Verarbeitung der personenbezogenen Daten müssen die User/innen diesem Prozess zustimmen, um das Service zu nutzen. Ebenso steht es den User/innen frei, an das Unternehmen bereitgestellte Daten durch die in den Einstellungen zu Verfügung gestellten Optionen zu löschen. Es werden lediglich Daten, welche für die Funktionalität das Dienstes benötigt werden weiterhin aufbewahrt. Deaktiviert die Benutzerin oder der Benutzer den Viber Account, so werden alle Daten inklusive der Chats vollständig gelöscht. Das Recht auf Löschung wird somit ebenfalls von Viber laut DSGVO eingehalten und umgesetzt. Weiters steht es den User/innen frei, mittels Opt-Out gewisse Datenverarbeitungsprozesse wie beispielsweise die Verarbeitung und Analyse der Standortinformationen zu unterbinden. Den Konsumenten steht ebenfalls frei, sämtliche gesammelten Daten durch Viber mittels der vorgesehenen Funktion in den Einstellungen anzufordern. Sämtliche Schutzvorkehrungen um die Daten der Kunden bestmöglich vor unautorisiertem Zugriff zu schützen, werden durch das Unternehmen angeführt. Die Messaging-Applikation erfüllt somit die Anforderungen an die Datenschutz-Grundverordnung für den privaten Bereich. Da jedoch sämtliche Kontakte das persönlichen Adressbuchs bei Verwendung des Dienstes synchronisiert werden, ist der gewerbliche Gebrauch des Messengers nicht DSGVO-konform [36].

Deletable Messages: Damit bereits versendete Nachrichten, welche von den Benutzerinnen oder Benutzer wieder zurückgezogen werden können, bietet Viber die Funktion, diese wieder zu löschen. Das Feature wurde so implementiert, dass Nachrichten im privaten als auch in Gruppenchats für alle Teilnehmer rückstandslos gelöscht werden [37].

Self Destructive Messages: Um versendete Nachrichten nach Ablauf einer bestimmten Zeit automatisch zu löschen, bietet Viber die Funktion der so genannten *Disappearing Messages*. Die Userin oder der User kann vor dem Versenden einen Timer konfigurieren, welcher die Zeit bestimmt, wie lange die Nachricht für den Gesprächspartner angezeigt wird. Nach Ablauf des Timers wird die Nachricht auf beiden Seiten der Konversation vollständig und nicht mehr rückführbar gelöscht. [38].

Screenshot Detection: Um die Privatsphäre der Nutzerinnen und Nutzer weiter zu schützen, wurde die Messaging-Applikation mit dem Feature der Screenshot-Detection erweitert. Wird seitens des Gesprächspartners ein Screenshot der Nachricht durchgeführt, so erfolgt eine Benachrichtigung durch Viber. Diese Funktion ist in den Secret-Chats als auch in den regulären Chats verfügbar und ist standardmäßig nach der Initialisierung des Messengers aktiviert [38].

1.2 Security Properties

Cryptographic Primitives: Während der Installation der Applikation generiert Viber auf den Endgerät ein 256-Bit Curve-25519 Schlüsselpaar, den so genannten ID-Key. Der private Teil bleibt dabei auf den Endgerät der Benutzerin oder des Benutzers, während der öffentliche Teil auf die Viber Server hochgeladen wird. Um One-to-One-Sessions zwischen den einzelnen Clients aufzubauen, werden Pre-Keys ebenfalls mit dieser Methode generiert. Für den sicheren Datenaustausch werden die Nachrichten für jede Session mittels dem Salsa20 Verschlüsselungsalgorithmus in Kombination mit einem flüchtigen One-Time 128-Bit symmetrischen Key verschlüsselt. Durch das so genannte Ratcheting werden für jeden neue Session Schlüsselpaare generiert. Die ausgetauschten Nachrichten werden anschließend mittels HMAC-256 signiert. Die kryptografischen Primitvien, welche bei Viber zur sicheren Kommunikation verwendet werden entsprechen dem Stand der Technik und können als sicher eingestuft werden [39].

End-to-End Encryption: Mit Version 6.0 wurde die Ende-zu-Ende-Verschlüsselung im Messaging-Dienst Viber implementiert, um die sichere Kommunikation der Gesprächspartner durch den gesamten Kanal sicherzustellen. Die Verschlüsselung umfasst sowohl Textnachrichten, Foto- und Videobotschaften, Audio- als auch Videoanrufe inklusive des gesamte Traffic in Gruppenchats. Die End-to-End-Encryption wurde in der mobilen als auch in der Desktopversion realisiert, um den Nutzerinnen und Nutzern einen holistischen Schutz zu gewährleisten. Die verschlüsselten Nachrichten werden mittels Secret-Key auf dem Gerät verschlüsselt, an die Server von Viber gesendet und anschließend auf den Gerät der Empfängerin oder des Empfängers entschlüsselt. Die Nachrichten werden auf den Server lediglich für die Dauer der Zustellung beim Kommunikationspartner in Form eines verschlüsselten Codes aufbewahrt und anschließend gelöscht. Das Unternehmen selbst hat laut eigener Angabe keinen Zugriff auf die verschlüsselten Nachrichten und kann somit ausgetauschte Korrespondenz nicht für analytische Zwecke wie beispielsweise Werbung öffnen, lesen und verkaufen [39].

Forward Secrecy: Durch den Einsatz des so genannten Double-Ratchet Verfahrens und dessen Eigenschaft, stetig neue Session Keys zur Kommunikation zu generieren, verfügt Viber über Forward Secrecy. So können im Fall einer Kompromittierung des Schlüssels vergangene Konversationen nicht entschlüsselt werden [39].

Backward Secrecy: Weiters wird durch die Implementierung des Double-Ratchet ebenfalls die Backward-Secrecy sichergestellt. Nach der Kompromittierung des Schlüsselmaterials ist es für eine Angreiferin oder einen Angreifer nicht möglich, zukünftige Nachrichten zu entschlüsseln [39].

MiTM-Prevention: Um Man-in-the-Middle-Attacken und somit der Kompromittierung der Ende-

zu-Ende-Verschlüsselung entgegenzuwirken, erfolgt die Authentifizierung in der Messaging Applikation im Kontext eines so genannten Viber-Calls. Dabei handelt es sich um einen Anruf in Form von Audio beziehungsweise Video, um den Authentifizierungsvorgang zu initialisieren. Während des Anrufs können die Benutzer auf den angezeigten Lock-Screen tippen, um den von Viber generierten numerischen String aufzurufen. Die zu authentifizierenden Kommunikationspartner sollten den selben berechneten String erhalten, welcher als Vergleichsbasis zur Authentisierung dient. Die Parteien müssen den String dem jeweiligen Partner vorlesen, um eine Manipulation der generierten ID-Keys und somit des Kommunikationskanals auszuschließen. Nach der erfolgreichen Verifikation signalisiert das Symbol eines grünen Vorhängeschloss die sichere Kommunikation. Die Authentifizierungsschlüssel werden von Viber stetig überwacht und überprüft. Erfolgt eine Änderung, so wird dies in Form eines roten Schlosses im Chatmenü angezeigt. Diese Form der Authentifikation findet Anwendung in 1-1-Chats, Secure-Calls als auch in der Gruppenchat-Funktion [39].

Disk Encryption: Das Sicherheitsfeature der Disk-Encryption ist nicht in der Messaging-Applikation von Viber implementiert. Informationen beziehungsweise Nachrichten liegen unverschlüsselt auf dem Endgerät und können durch den Einsatz entsprechender Software bei Verlust des Gerätes von einer Angreiferin oder einem Angreifer extrahiert werden.

Secure Group Chats: Alle Teilnehmer einer Chatgruppe teilen den selben symmetrischen Slasa20 Encryption-Key, welcher weder Viber noch Drittanbietern bekannt ist. Bei der Gründung neuer Gruppen wird dieser Schlüssel vom Ersteller generiert und an alle Teilnehmer via sicherer One-On-One-Sessions verteilt. Wird ein weiteres Mitglied von einer bereits bestehenden Teilnehmerin oder einem bestehenden Teilnehmer hinzugefügt, so wird der Encryption-Key durch diese oder diesen verteilt. Das Group-Secret wird durch den HMAC-256 mit jeder versendeten Nachricht durch den Ratchet erneuert. Jede Gruppennachricht beinhaltet eine Sequenznummer die indiziert, wie oft die Hashfunktion aufgerufen wurde. Die Clients hashen und senden Folgenachrichten ab dieser Sequenz, somit wird sichergestellt, dass Keys nicht erneut verwendet werden. Die Forward-Secrecy wird durch diesen One-Way-Hash-Algorithmus gewahrt. Somit können vergangene Nachrichten auch bei einer Kompromittierung des Schlüsselmaterials nicht entschlüsselt und gelesen werden [39].

1.3 Usability Properties

Multi Device Support: Bei der Messaging-Applikation ist der Account strikt mit dem mobilen Gerät und der dazugehörigen Rufnummer verbunden. Wird Viber auf einem weiteren Smartphone oder ein Tablet mit denselben Nutzerdaten installiert, so werden alle Einstellungen auf dem primären Gerät zu-

rückgesetzt. Der Dienst kann somit lediglich auf einem einzigen mobilen Gerät gebraucht werden. Ein Multi-Device-Support kann bei Viber nur mittels simultaner Verwendung der Desktopversion erreicht werden. Mittels QR-Code-Überprüfung durch das Smartphone beziehungsweise des Tablets kann von den Userinnen oder Usern die Desktopversion am Laptop oder PC parallel zur mobilen Variante genutzt werden. Versendete als auch empfangene Nachrichten werden auf beiden Geräten gleichermaßen angezeigt und synchronisiert. Ende-zu-Ende Verschlüsselung ist seitens der Messaging-Applikation in beiden Kommunikationskanälen sichergestellt [40].

E2E by Default: Der Nachrichtenaustausch zwischen den Kommunikationspartnern ist in Viber standardmäßig durch die Ende-zu-Ende-Verschlüsselung gesichert. Die Nutzerin beziehungsweise der Nutzer muss bei der Initialisierung der Applikation keine weiteren Schritte tätigen, um die Datenverschlüsselung zu aktivieren. So ist der sichere Datenaustausch sowohl in Privatnachrichten als auch in der Gruppenchat-Funktion standardmäßig aktiviert und keine Aktionen Seitens der Benutzer vorausgesetzt [40].

Easy Contact Discovery: Nach der Installation der Applikation müssen die Nutzer ihre Einwilligung erteilen, dass Viber auf das persönliche Adressbuch Zugriff erhält, um sämtliche Kontakte automatisch zu synchronisieren. Ein manuelles Hinzufügen ist somit nicht erforderlich [41].

Easy Key Maintenance: Beim Initialisierungsvorgang der Messaging-Applikation wird der ID-Key automatisch durch das Endgerät erstellt. Der private Teil des Schlüssels wird lokal hinterlegt, während der öffentliche Teil auf die Server von Viber hochgeladen werden. Wird zusätzlich ein zweites Gerät verwendet, so wird der private Schlüssel vom primären Gerät über einen sicheren Link automatisch an des Sekundäre übertragen. Die so genannten Pre-Keys zur sicheren Datenübertragung werden ebenfalls automatisch am Endgerät erzeugt und gewartet. Das Schlüsselmanagement erfolgt somit ohne Interaktion der Nutzer automatisch im Hintergrund. Bei der Erneuerung von Schlüsselmaterial durch einen Kommunikationspartner muss jedoch eine erneute Authentifizierung vorgenommen werden, um mögliche Man-in-the-Middle-Attacken ausschließen zu können. Viber zeigt diesen Status in Form eines roten Schlosses im Chat an [39].

Asynchronous: Wie bei den meisten modernen Instant-Messaging-Applikationen handelt es sich bei Viber um eine Form der asynchronen Kommunikation. Sender und Reciever müssen somit nicht zur selben Zeit online sein, um einen erfolgreichen Nachrichtenaustausch zu vollziehen. Ist die Empfängerin oder der Empfänger während der Datenübertragung nicht verbunden, so werden die Nachrichten für einen begrenzten Zeitraum in verschlüsselter Form auf den Servern von Viber gespeichert. Ist das Endgerät im empfangsbereiten Zustand, so wird die Nachricht weitergeleitet und serverseitig gelöscht

[41].

No Monetary Costs: Der Download des Messaging-Dienstes ist plattformübergreifend für die Nutzerinnen und Nutzer kostenlos. Der Nachrichtenaustausch als auch die Telefon-Funktionen zwischen Viber-Usern/innen ist ebenfalls ohne Zusatzkosten implementiert. Lediglich die Verwendung des Viber-Out-Features ist mit kosten verbunden, da Auslandsanrufe mit Nicht-Viber-Nutzern zu einem entsprechendem Tarif verrechnet werden. Die Viber-Out-Funktion fällt jedoch nicht in die Gewichtung, da lediglich der interne Gebrauch zwischen den Nutzern/innen und damit verbundene Kosten in die Bewertung fallen.

2 Telegram

Telegram wurde 2013 von den Brüdern Nikolai und Pavel Durov, welche das in Russland größte und bekannteste Social-Network *VK* [42] etablierten, als unabhängige non-profit Organisation gegründet. Bei dem Messaging-Dienst handelt es sich um einen Cloud-basierten Service, welcher das Versenden von Multimedia-Nachrichten als auch Sprach- und Videotelefonie unterstützt. Das eigens entwickelte Protokoll für den Messaging-Dienst verspricht die Client-Server- als auch Ende-zu-Ende-Verschlüsselung für sämtliche mobilen Betriebssysteme als auch Webclient und Desktopsysteme. Besonders die Möglichkeit durch die Offenlegung der Telegram API eigene Clients zu implementieren, macht den Dienst für technikaffine Benutzerinnen und Benutzer interessant. Mit Stand Jänner 2021 zählt Telegram über 500 Millionen weltweiten Userinnen und User und macht den Messenger zu einem der populärsten Diensten [43]. Ursprünglich wurde der Dienst als Alternative zum bekannten Instant-Messenger WhatsApp entwickelt, welcher im Bereich Sicherheit als auch Privatsphäre den Kunden ein deutlich höheres Schutzniveau bieten soll. Initial wurde der Firmensitz in St.Petersburg eingetragen, um staatliche Regulierungen zu umgehen wurde der Sitz stetig geändert und befindet sich nun in Dubai, wobei der Dienst offiziell in London registriert ist. Unter den Benutzerinnen und Benutzern erfreut sich Telegram großem Zuspruch wenn es um sicheren Datenaustausch geht. So kam der Dienst zur Organisation und Kommunikation während den Protesten 2019 in Hong Kong als auch im Konflikt in Belarus 2020 zum Einsatz [44].

2.1 Privacy / Anonymity Properties

Proxy-Server: Der Messenger basiert auf den so genannten MTProto (Mobile Telegram Protocol), welcher seinen Kundinnen und Kunden ein besonders hohes Maß an Sicherheit mit zusätzlich hohem Datendurchsatz verspricht. Basierend auf diesem Protokoll wurde von Telegram der MTProto-Proxy

beziehungsweise MTProxy entwickelt, um Ländersperren und Zensur zu umgehen. Dabei handelt es sich um einen Server, welcher den Datenaustausch zwischen Sender und Zielserver übernimmt. Der MTProxy verbirgt den übertragenen Traffic unter dem herkömmlichen TLS (HTTPS), welcher bei fast allen Webseiten standardmäßig implementiert ist. So ist es für staatliche Behörden besonders schwierig, solch einen Proxy-Server unter dem gesamten Datentransfer auszumachen und in weiterer Folge Telegram zu blockieren. Neben dem Einsatz des MTProxy können Benutzerinnen und Benutzer ebenfalls auf SOCKS5-Proxies zurückgreifen. Davon wird seitens der Betreiber jedoch abgeraten, da SOCKS5 einen offenen Transfer von Logindaten inklusive Passwort voraussetzt. Dies kann unter Umständen die Verwendung des Proxies preisgeben, folglich kann dies zur Sperrung des Proxy-Servers führen. Der hauseigene Proxy-Dienst löst dieses Problem partiell, so wird lediglich ein Passwort, welches nicht zum Server selbst weitergeleitet wird, für den Verbindungsaufbau benötigt. Zur Ermittlung der MTProxies stellt Telegram eigene Channels zur Verfügung, welche den Nutzerinnen und Nutzer frei zu Verfügung stehen [45].

Minimal Data Collection: Telegram folgt bei der Speicherung und Verarbeitung von personenbezogenen Informationen zwei wesentliche Prinzipien. Zum einen werden die Nutzerdaten nicht für Werbezwecke an Drittanbieter weitergegeben, zum anderen werden seitens des Messenger-Dienst nur jene Daten gespeichert, welche zur reibungslosen Funktionalität der Applikation beitragen. So werden Telefonnummer und generelle Account-Informationen wie Username und Profilbild zur Identifikation der Teilnehmer gesammelt und öffentlich angezeigt. Die Angabe richtiger Informationen zur Person selbst wird explizit von Telegram nicht vorausgesetzt, den Userinnen und User steht es frei, Angaben diesbezüglich zu tätigen. Eine E-Mailadresse zu hinterlegen ist ebenfalls optional und dient der 2-Step-Verifikation als zusätzliche Sicherheitsfunktion. Da es sich bei Telegram um einen Cloud-Service handelt, werden sämtliche Nachrichten als auch versendete Medieninhalte verschlüsselt auf den eigenen Server des Dienstes gespeichert. Wird auf die Funktion Secret Chat zurückgegriffen, so werden Nachrichten und Logs zu Kommunikationsteilnehmern nicht auf den Servern gespeichert, Mediendateien bleiben jedoch in verschlüsselter Form sehr wohl in der Cloud. Telegram greift auf das Adressbuch der Benutzerin beziehungsweise des Benutzers zu und synchronisiert diese Informationen um weitere Teilnehmer zu identifizieren. Werden Standortdaten in Chatnachrichten geteilt, so speichert der Messenger diese Informationen in Standard- als auch Secure-Chats. Aktiviert die Userin oder der User den Live-Location-Dienst um Teilnehmer in der unmittelbaren Umgebung zu identifizieren, sammelt Telegram Informationen zum Standort bis zur Deaktivierung des Features. Cookies werden von Telegram lediglich zur technischen Funktionalität des Web-Clients eingesetzt und dienen nicht als Gegenstand

zur Analyse und Profiling. Laut Angaben des Messenger-Dienst werden personenbezogene Daten lediglich bis zur Zweckerfüllung auf den Servern gespeichert, bevor sie endgültig gelöscht werden. Um die Nutzerinnen und Nutzer vor Missbrauch und Spam zu schützen, speichert Telegram weiters Metadaten unter anderem wie IP-Adresse, verwendete Gräte als auch die Histore von geänderten Benutzernamen. Der Zeitraum der Aufbewahrung beträgt dabei maximal 12 Monate [46].

Server Location: Die Daten von Nutzerinnen und Nutzer des Europäischen Wirtschaftsraum werden in Datenzentren innerhalb der Niederladen gespeichert und verarbeitet. Die Server als auch das gesamte Netzwerk innerhalb der Zentren werden von Telegram selbst administriert und Drittanbietern nicht zur Verfügung gestellt. Den Usern außerhalb des EWR stehen weltweit verstreute Server zur Kommunikation zur Verfügung, diese sind jedoch abhängig vom jeweiligen Standort nicht durch europäische Datenschutzvorgaben gesichert. Die jeweilige Rechtsprechung in den Staaten wird angewendet. Über die Verteilung als auch den genauen Standort der Server wird seitens Telegram keine nähre Auskunft gegeben [46].

Anonymous Usage: Der Messenger Telegram kann ohne die Angabe einer validen Telefonnummer nicht erfolgreich installiert und verwendet werden. Die Rufnummer dient Telegram als Identifikator und kann nicht durch eine falsche Angabe substituiert werden. Alle weiteren personenbezogenen Information können von der Nutzerin oder dem Nutzer frei angegeben werden. Eine Gültigkeit dieser Daten wird seitens Telegram nicht für die einwandfreie Funktionalität vorausgesetzt [46].

No Advertising Information: Der Messaging-Service speichert und verarbeitet persönliche Daten lediglich zum Zweck der Funktionalität des Service. Es werden keine Daten der Nutzerinnen und Nutzer an Drittanbieter für Werbezwecke weitergegeben. Die Datenhoheit über sämtliche seitens der User angegebenen Informationen bleibt bei Telegram selbst [46].

GDPR Compliance: Nutzerdaten werden von der Messaging-Applikation nur benötigt, um die Funktionalität des Dienstes zu gewährleisten. Mit dem GDPR-Update 4.8.9 für Android und 4.8.2 für Apple wurden weitere Privatsphäre-Einstellungen zur Konformität gegenüber der Datenschutz-Grundverordnung hinzugefügt. Den Nutzerinnen und Nutzern wird das Recht eingeräumt, eine persönliche Kopie sämtlicher von Telegram gespeicherten Informationen anzufordern, persönliche Datensätze zu löschen beziehungsweise zu ergänzen, die Verarbeitung der Daten zu restringieren sowie gespeicherte Informationen abzuändern. Die Datenverarbeitung im privaten Bereich durch den Messaging-Dienst ist gegenüber der Datenschutzgrundverordnung legitim. Da Telegram jedoch Zugriff auf das gesamte Adressbuch der Userin beziehungsweise des Users hat und diese Informationen synchronisiert werden, ist der Gebrauch im Unternehmenskontext nicht konform gegenüber der DSGVO [46].

Deletable Messages: Wird eine Nachricht in der Secret-Chat-Funktion durch einen der Kommunikationspartner gelöscht, so instruiert die Applikation selbiges auf dem anderen Ende durchzuführen. Die gelöschten Nachrichten sind somit nicht wiederherstellbar. In den Cloud-Chats, als den Standard-Chats für 1-zu-1 Konversationen oder Gruppenchats wurde diese Funktion mit Version 5.5 ebenfalls implementiert. Gelöschte Nachrichten werden ganzheitlich auf allen Kommunikationsenden für sämtliche Userinnen und User gelöscht [47].

Self Destructive Messages: Versendete Nachrichten in Secret-Chats können durch die Nutzer so konfiguriert werden, dass diese nach Ablauf eines Timers automatisch von der Applikation gelöscht werden. Nachdem die Nachricht vom Empfänger gelesen wurde, startet der Timer und löscht nach Ablauf die Daten auf beiden Enden der Kommunikation. Dies gilt sowohl für Medieninhalte wie Fotos und Videos als auch für simple Textnachrichten. Diese Funktion ist jedoch lediglich für Secret-Chats verfügbar [47].

Screenshot Detection: In der Messaging-Applikation Telegram wurde die Screenshot-Detection-Funktion für den Secret-Chat implementiert. Tätigt die Empfängerin oder der Empfänger der Nachricht einen Screenshot, so wird die Senderin oder der Sender über diesen Vorgang informiert. Dieses Feature kann lediglich für den Secret-Chat aktiviert werden. In den Cloud-Chats kann somit nicht ermittelt werden, ob Inhalte abfotografiert und extern gespeichert wurden [47].

2.2 Security Properties

Cryptographic Primitives: Anstelle der Implementierung bereits etablierter und als sicher eingestuften kryptografischen Konstrukten, greift Telegram auf das hauseigene Protokoll MTProto zurück. Zum sicheren Nachrichtenaustausch basiert das Protokoll auf der RSA-2048-Bit-Verschlüsselung und der 256-Bit-Symmetrischen-Verschlüsselung. Der sichere Schlüsselaustausch wird mittels Diffi-Hellman-Key-Exchange realisiert. Der Einsatz eigener Protokolle wird oftmals als kontrovers betrachtet, die im Einsatz befindlichen kryptografischen Primitiven gelten jedoch als State-of-the-Art und können als sicher eingestuft werden [3].

End-to-End Encryption: Bei dem Messaging-Dienst Telegram muss beim Nachrichtenaustausch zwischen zwei verschiedenen Modi unterschieden werden. Die Cloud-Chats, also der standardmäßige Nachrichtenaustausch zwischen den Kommunikationsparteien, sind mittels Client-Server-Verschlüsselung geschützt. Nachrichten werden von Telegram auf den eigenen Servern in verschlüsselter Form gespeichert. Um Ende-zu-Ende-verschlüsselte Nachrichten zu versenden, muss die Userin beziehungsweise

der User einen so genannten Secure-Chat-Kanal erstellen. Tritt der Kommunikationspartner diesem Kanal bei, so wird der Ende-zu-Ende-verschlüsselte Chat mittels grünem Schloss symbolisiert. Die Daten sind über den gesamten Kommunikationskanal verschlüsselt und werden nicht auf den Servern gespeichert. Das Weiterleiten von Nachrichten ebenso wie das Abrufen der Nachrichten auf einem anderen Gerät ist nicht mehr möglich. Ende-zu-Ende-Verschlüsselung kann bei der Applikation lediglich mittels der Secure-Chat-Funktion realisiert werden [48].

Forward Secrecy: Damit vergangene Konversationen nicht nach einer Kompromittierung des Schlüsselmaterials durch eine Angreiferin oder einem Angreifer gelesen werden können, wird ein so genannter Re-Keying-Prozess durchgeführt. Das alte Schlüsselmaterial wird nach 100 gesendeten Nachrichten beziehungsweise spätestens nach einer Woche automatisch neu generiert. Alte Schlüssel werden verworfen und können nach dem Austausch, auch durch den Besitz des neuen Schlüsselmaterials, nicht mehr rekonstruiert werden. Der Messaging-Dienst unterstützt mit diesem automatisierten Prozess somit Perfekt-Forward-Secrecy [49].

MiTM-Prevention: Um eine sichere Ende-zu-Ende-Verschlüsselung zwischen zwei Kommunikationspartner zu garantieren und ebenfalls zu gewährleisten, dass der Kanal nicht abgehört werden kann, authentifizieren sich Sender und Empfänger gegenseitig. Beim Messenger Telegram erfolgt die gegenseitige Authentifizierung mittels manuellem Vergleich eines QR-Codes inklusive dem Abgleich einer 64 Zeichen langer Sicherheitsnummer. Stimmen der QR-Code beziehungsweise der Zahlenstring auf beiden Seiten überein, so haben sich die Parteien erfolgreich authentifiziert. Das Abhören mittels einer Man-in-the-Middle-Attacke kann somit ausgeschlossen werden. Das sichere Versenden von Nachrichten über den gesamten Kommunikationskanal ist somit in der Secure-Chat-Funktion gegeben. Die Client-Server-Kommunikation wird während der Diffi-Hellman-Schlüsselerzeugung durch einen in die Client-Software eingebetteten öffentlichen RSA-Schlüssel des Servers vor MiTM-Angriffen geschützt [40] [50].

Disk-Encryption: Nachrichten werden mittels Client-Server- beziehungsweise End-to-End-Verschlüsselung sicher übertragen, jedoch liegen die Informationen unverschlüsselt auf dem Endgerät. Telegram erlaubt es jedoch seinen Nutzerinnen und Nutzern eine PIN-Sperre auf Chats zu legen. Die Nachrichten werden bis zu Freigabe auf dem Gerät gesperrt und können nicht von Dritten ausgelesen werden [47].

Secure Group Chat: In Telegram können Gruppen bis zu 200.000 Mitglieder erstellt werden. Jedoch können die Nachrichten zwischen den Gruppenmitgliedern nicht in E2E-verschlüsselter Form versendet werden. Ende-zu-Ende-Verschlüsselung ist lediglich in der Secure-Chat-Funktion zwischen zwei Kommunikationspartnern implementiert. Ein sicherer Nachrichtenaustausch innerhalb einer Gruppe wird von

Telegram somit nicht unterstützt [3].

2.3 Usability Properties

Multi Device Support: Die Messaging-Applikation erlaubt die parallele Verwendung des Accounts auf mehreren Gräten mit derselben Telefonnummer. Wird ein neues Gerät hinzugefügt, so erhält die Nutzerin beziehungsweise der Nutzer einen Verifikationscode auf das primäre Gerät. Das Senden und Empfangen von Nachrichten kann nach der erfolgreichen Authentifikation auf allen Geräten gleichermaßen vollzogen werden. Die Geräte teilen alle samt die entsprechenden Cloud-Chats, jedoch können bereits versendete Secure-Chat Nachrichten nicht synchronisiert werden, da diese lokal auf dem jeweiligen Gerät gespeichert sind [40].

E2E by Default: Wie bereits erörtert unterscheidet Telegram zwischen zwei verschiedenen Modi zum persönlichen Nachrichtenaustausch. Bei der Kommunikation mittels Cloud-Chat erfolgt die Verschlüsselung mittels Client-Server-Encryption. Das bedeutet, dass Nachrichten auf dem Telegram Server gespeichert werden und nicht durchgehend bis zum Receiver geschützt sind. Die standardmäßige Kommunikation beim Messaging-Dienst ist somit nicht Ende-zu-Ende verschlüsselt, obgleich das Unternehmen mit einer starken Security wirbt. Die Nutzerinnen und Nutzer müssen die End-to-End-Encryption mittels Secure-Chat zunächst aktivieren, um einen ganzheitlichen Schutz über den gesamten Kommunikationskanal sicherzustellen. Dieses Vorgehen wird von Sicherheitsexperten als kritisch betrachtet, da Userinnen und User davon ausgehen, alle Nachrichten seinen standardmäßig E2E-verschlüsselt [47].

Easy Contact Discovery: Nach der erfolgreichen Installation und Registrierung der Messaging-Applikation muss die Userin beziehungsweise der User dem Dienst erlauben, auf das Adressbuch zugreifen zu können. Das gesamte Adressbuch wird von Telegram auf die eigenen Server hochgeladen und dient dem Discovery-Service als Grundlage, vorhandene Telegram Kontakte zu synchronisieren. Nach erfolgreicher Synchronisation werden die Kontakte automatisch angezeigt. Dieser Vorgang wird automatisch in regelmäßigen Abständen wiederholt um die Nutzer zu informieren, sobald ein im Adressbuch befindlicher Kontakt ebenfalls diese Applikation verwendet. Ein manuelles Suchen und Hinzufügen von Kontaken ist seitens der Benutzerinnen und Benutzer nicht erforderlich [44].

Easy Key Maintenance: Bei der Initialisierung der Applikation werden alle notwendigen Schlüssel zur sicheren Kommunikation automatisch erstellt. Bei der Verwendung der Cloud-Chat-Funktion ist keine Aktion seitens Der Userinnen oder User erforderlich um neues Schlüsselmaterial zu generieren. Bei Secure-Chats müssen pro Konversation eigene Schlüssel generiert und verifiziert werden. Löscht

einer der Konversationspartner ihren oder seinen Account, so kann mit der Erzeugung neuer Schlüssel nicht mehr auf diese Konversation zugegriffen werden. Die Authentifizierung muss pro Secure-Chat erneut durch die Userinnen und User vollzogen werden [40].

Transcript Consistency: Telegram unterstützt in der Gruppenchat-Funktion die Transcript-Consitency. Somit wird sichergestellt, dass alle Nachrichten in derselben Reihenfolge für alle Mitglieder angezeigt werden. Neben diesem Feature bietet Telegram ebenfalls die Option, den vergangenen Chatverlauf für neue Mitglieder auszublenden und die Konversationshistorie ab dem Beitrittszeitpunkt zu aktivieren [51].

Asynchronous: Wie bei den meisten modernen Messaging-Applikationen handelt es sich bei Telegram ebenfalls um einen asynchronen Nachrichtenaustausch. Beim Versenden einer Nachricht wird diese auf den Servern zwischengespeichert und in weiterer Folge der Empfängerin beziehungsweise dem Empfänger beim erfolgreichen Verbindungsaufbau zum Telegram-Service zugestellt. Das erfolgreiche Zustellung einer Nachricht wird in Form eines einfachen Hakens angezeigt [46].

No Monetary Costs: Der Download sowie die Verwendung von Telegram ist ohne monetäre Kosten verbunden. Das Unternehmen ist laut eigenen Angaben nicht darauf ausgelegt, mit der Applikation Profite zu generieren. Die Nutzerinnen und Nutzer können sämtliche Features des Messengers kostenlos nutzen.

3 Wickr Me

Bei der Messaging-Applikation Wickr Me handelt es sich laut Medianaussagen um eine Art sicheres Whatsapp, welche vom gleichnamigen Unternehmen 2010 ins Leben gerufen wurde. Dabei unterscheidet sich der Messenger von anderen Apps dadurch, dass eine Version für den Privatgebrauch (Wickr Me) als auch für Unternehmen (Wickr Pro) erhältlich ist. Des weiteren verfolgt die Applikation beim Nachrichtenaustausch eine durchaus andere Herangehensweise als seine Konkurrenten. So obliegt es den Nutzerinnen und Nutzern selbst, wie lange Nachrichten lesbar für die Kommunikationspartner bleiben. Besonders in Zeiten von Hackerangriffen als auch dem missbräuchlichem Umgang mit sensiblen Nutzerdaten durch verschiedene Anbieter, ist der Schutz der Privatsphäre für viele Userinnen und User ein entscheidendes Kriterium bei der Auswahl eines geeigneten Messengers. Eben dies verspricht Wickr Me als Grundsatz, dementsprechend hatte das Unternehmen wenig Probleme mit der Akquirierung von Investoren. Zu diesen zählen unter anderem der Gründer und Vorsitzende der Human Rights Foundation Thor Halvorssen, der ehemalige amerikanische Anti-Terrorismus-Experte Richard Clarke als auch Erik Prince, der Gründer der privaten Sicherheitsfirma Academi ehemals Blackwater. Neben der stetig

steigenden Nutzeranzahl im privaten als auch gewerblichen Bereich, greifen auch immer mehr Politiker auf den Kryptomessenger zurück. Nach dem Hacking-Skandal der US-Präsidentschaftswahl 2016 und der darauf folgenden Veröffentlichung tausender Nachrichten und Dokumente, wechselten Politiker in Scharen zur Messaging-Applikation. Dieses durch die Inhabern hoher politscher Ämter gesetztes Vertrauen in das Unternehmen, macht die Applikation folglich attraktiv für Nutzerinnen und Nutzer im gewerblichen aus auch privaten Bereich [52].

3.1 Privacy / Anonymity Properties

Proxy-Server: Damit Nutzerinnen und Nutzer einen höheren Schutz der eigenen Privatsphäre erreichen als auch mit Teilnehmern kommunizieren können, welche aufgrund staatlicher Zensur verschlüsselte Messaging-Dienste standardmäßig nicht verwenden können, stellt das Unternehmen Proxy-Server zur Verfügung. Die gemeinsam mit dem Unternehmen Psiphon [53] entwickelte Technologie, genannt Wickr Open Access (WOA) sorgt für das Verschleiern des Traffics der Userinnen und User. Dabei verbindet sich der Client über eine Serie global vernetzter Proxy Server, welche zu tausend weltweit verstreut sind. Die Technologie sorgt neben der Umgehung von Zensur ebenfalls für einen bestmöglichen Datendurchsatz über verschiedene Hops und garantiert somit eine störungsfreie Kommunikation sowohl beim Nachrichtenversand als auch bei der Telefonie. Wird Wickr Open Access auf dem Endgerät aktiviert, so initiiert die Applikation einen Verbindungsaufbau mit bis zu 10 verschiedenen, zufällig ausgewählten Servern, welche einen Mix aus unterschiedlichen, als sicher eingestuften Protokollen verwendet und eine verschlüsselte Kommunikation zwischen den Teilnehmern gewährleistet [54].

Minimal Data Collection: Laut eigenen Angaben des Unternehmens werden lediglich Daten der Userinnen und User gesammelt, welche für die reibungslose Funktionalität des Messaging-Dienst erforderlich sind. Für eine erfolgreiche Registrierung werden die erstellte Wickr-ID als auch das festgelegt Passwort von der Applikation gespeichert. Weiters wird das Erstellungsdatum des Accounts, Informationen über das Endgerät auf dem die Applikation installiert wurde, die letzte Anmeldung sowie die gesamte Anzahl and versendeten beziehungsweise empfangenen Nachrichten auf den eigenen Servern gespeichert. Des weiteren werden sämtliche externe IDs, also mit dem Account verbundene Mail-Adressen sowie Telefonnummern, Änderungen der Benutzereinstellungen als auch die Wickr Versionsnummer hinterlegt. Erlaubt die Nutzerin beziehungsweise der Nutzer den Zugriff auf das Adressbuch, so werden die Kontaktdetails als gehashte Werte auf den Servern hinterlegt. Somit wird von der Applikation sichergestellt, dass ein direkter Zugriff auf das Adressbuch seitens des Unternehmens ausgeschlossen werden kann. Die Geräteinformationen werden ebenfalls nach der Installation in gehashter Form hinter-

legt und dienen der Zuordnung zwischen Benutzerkonto und Endgerät. Anonymisierte Nutzerstatistiken wie Anzahl der versendeten Nachrichten, Art der Kommunikation (Textnachricht oder Voice-Chat) werden während der Verwendung der App ebenfalls gesammelt. Versendete Nachrichten als auch statistische Daten werden für einen Zeitraum bis zu maximal 6 Tagen auf den Servern gespeichert [55] [56].

Server Location: Neben den bereits erwähnten Proxy Server, welche weltweit verstreut zur Kommunikation verwendet werden, ist die gesamte Infrastruktur zum Nachrichtenaustausch Cloudbasiert auf den Amazon Web Services gehostet. Somit verfügt das Unternehmen nicht über die vollständige Datenhoheit der gesammelten Informationen der Nutzerinnen und Nutzer. Weiters werden bei der Verwendung der Messaging-Applikation sämtliche Informationen in die Vereinigten Staaten transferiert, verarbeitet und gespeichert. Die Daten liegen zwar in verschlüsselter Form auf den Servern, jedoch fallen sämtliche Informationen unter die umstrittene U.S. Data Protection and Privacy Regulation [55].

Anonymous Usage: Um die Messaging-Applikation zu verwenden, wird von den Nutzerinnen und Nutzern bei der Registrierung keine Angabe personenbezogener Daten vorausgesetzt. Zur Anmeldung als auch um in weiterer Folge von Kontakten gefunden werden zu können, ist die Festlegung einer so genannten Wickr Me ID erforderlich. Das Unternehmen empfiehlt einen leicht zu merkenden Usernamen, weist jedoch ausdrücklich darauf hin, dass dieser Name willkürlich gewählt werden kann. Die festgelegte ID wird in mehreren Runden mittels kryptografischen Operationen in gehashter Form hinterlegt. Dies hat den Vorteil, dass Userinnen und User das Service anonymisiert verwenden können, da die Betreiber anhand der bereitgestellten Informationen nicht in der Lage sind, die tatsächliche Identität hinter einer registrierten ID festzustellen. Die erfolgreiche Installation setzt ebenfalls ein vom User festgelegtes Passwort voraus, welches nicht auf den Servern gespeichert wird und somit den Machtbereich der Nutzerin beziehungsweise des Nutzers nicht verlässt [55].

No Advertising Information: Die von den Userinnen und Usern bereitgestellten Informationen werden vom Unternehmen zum Zweck der Applikationsverbesserung und Werbeaktivitäten als auch für Marketingstrategien an die verschiedenen Partnerunternehmen von Wickr Me weitergeleitet. Obgleich Wickr Me dem Leitsatz der minimierten Datenverarbeitung folgt und dies ausdrücklich in der Privacy Policy verankert ist, so unterliegt die Verarbeitung der weitergeleiteten Daten den Richtlinien der jeweiligen Partnerunternehmen [55].

GDPR Compliance: Nutzerinnen und Nutzern aus dem Europäischen Wirtschaftsraum werden aufgrund der Datenschutz-Grundverordnung weitere Möglichkeiten bezüglich der Datenverarbeitung eingeräumt. Damit die persönlichen Daten den EWR nicht verlassen und somit nicht auf US-Servern gespeichert werden, wird diesbezüglich eine Opt-Out Option geboten. Das Unternehmen weist jedoch

darauf hin, dass dadurch einige Features beziehungsweise Services nicht ordnungsgemäß funktionieren könnten. Um eine vollständige Compliance mit der Datenschutz-Grundverordnung zu erreichen, wird den Nutzern ebenfalls das Recht eingeräumt, sämtliche gespeicherten Daten entweder manuell einzusehen, oder einen vollständigen Auszug vom Unternehmen anzufordern. Ebenso steht es den Userinnen und Usern frei, sämtliche Informationen und Angaben zu korrigieren und etwaige Datensätze zu ändern. Das Recht auf Vergessenwerden wird laut der Privacy Policy ebenso vom Unternehmen gemäß der Datenschutz-Grundverordnung umgesetzt. Eine vollständige Löschung sämtlicher von Wickr Me gespeicherten Informationen können zu jedem Zeitpunkt nach Aufforderung durch die Nutzerin beziehungsweise des Nutzers veranlasst werden. Aufgrund des Privacy-Designs des Services selbst kann der Account nur manuell und nicht durch das Unternehmen selbst gelöscht werden [55].

Deletable Messages: Um versendete Textnachrichten, Files oder Medieninhalte zu löschen, bietet Wickr Me die so genannte Recall-Funktion, welche seit Version 5.54 implementiert wurde. Nutzerinnen und Nutzer sind somit in der Lage, Inhalte nicht nur lokal im eigenen Chatverlauf zu löschen, sondern für sämtliche Kommunikationspartner. Dieses Feature wurde sowohl für 1-1-Konversationen als auch für die Gruppenchat-Funktion eingeführt und löscht restlos sämtliche ausgewählten Nachrichten. Unterstützt wird diese Option von allen mobilen Versionen genauso wie der Desktop-Applikation von Wickr Me [2].

Self Destructive Messages: Die Messaging-Applikation unterstützt die Self-Destruction-Funktion von versendeten Nachrichten mittels zwei Optionen, Expiration und Burn-On-Read (BOR). Bei ersterer Funktion setzt die Nutzerin oder der Nutzer ein benutzerdefiniertes Zeitfenster, in welchem die Nachricht für den jeweiligen Kommunikationspartner sichtbar ist. Der Countdown startet nachdem der Sender die Nachricht von seinem Gerät verschickt. Nach Ablauf dieses Timers wird die Nachricht automatisch sowohl auf dem jeweiligen Endgerät als auch die zwischengespeicherte Kopie auf den Servern restlos gelöscht. Wird die Nachricht vom Empfänger nicht innerhalb dem gesetzten Zeitfensters gelesen, erfolgt eine entsprechende Benachrichtigung über das Versäumnis. Bei letzterer Funktion wird ebenfalls vor der automatischen Löschung ein von der Userin oder dem User konfigurierter Timer initialisiert, jedoch startet der Countdown erst nachdem die Nachricht von der Empfängerin beziehungsweise dem Empfänger gelesen wurde [2].

Screenshot Detection: Um die Privatsphäre der Nutzerinnen und Nutzer um einen zusätzlichen Layer zu erweitern, verfügt Wickr Me über die Screenshot-Detection. Dieses Feature ist dauerhaft aktiviert und kann nicht von den Kommunikationsparteien in den Chat-Einstellungen deaktiviert werden. Wird innerhalb eines Chats eine Bildschirmaufnahme von einem der Mitglieder getätigt, so erfolgt die

Benachrichtigung über diesen Vorgang für die User [57].

3.2 Security Properties

Cryptographic Primitives: Das primäre Ziel des Wickr Secure Messaging Protokolls ist der sichere Nachrichtenaustausch zwischen den einzelnen Kommunikationspartnern. Um dies zu gewährleisten, sind von den Applikationsentwicklern State-of-the-Art-Technologien implementiert. Jede versendete Nachricht erhält einen einzigartigen AES-256 Schlüssel in Kombination mit einem ECDH-P521 Public Key um den Key-Exchange zu vereinbaren. Der Nachrichteninhalt wird mittels dem AES-256-Algorithmus verschlüsselt und kann nur auf dem entsprechenden Endgerät wieder entschlüsselt werden. Der Encryption-Key wird mittels Elliptic-Curve-Diffi-Hellman-P521 mit dem Kommunikationspartner geteilt. Somit wird sichergestellt, dass nur der rechtmäßige Empfänger der Nachricht diese wieder entschlüsseln kann. Für zusätzliche Sicherheit als auch Anonymität sorgt die Header-Encryption, welche ebenfalls mittels AES-256 realisiert wird und sämtliche Header-Parameter mit senderspezifischen Informationen verschlüsselt. Mittels TLS wird die übertragene Nachricht um einen weiteren Security-Layer verstärkt und vor Angriffen im Kommunikationskanal gesichert. Die von der Messaging-Applikation implementierten kryptografischen Verfahren entsprechen den Best-Practices und gelten als hochsicher [58].

End-to-End Encryption: Das Wickr Messaging-Protokoll stellt sicher, dass sämtliche ausgetauschten Nachrichten zwischen den Clients Ende-zu-Ende verschlüsselt übertragen werden. Die End-to-End-Encryption wird mittels einer Kombination aus Public-Key- und Symmetric-Key-Cryptography realisiert. Wickr verwaltet sämtliche Secret-Decryption- und Authentication-Keys lokal auf dem Endgerät, wobei diese zu keinem Zeitpunkt an die unternehmenseigenen Server gesendet werden. Lediglich die öffentlichen Identity-Keys als auch die Ephemeral-Enryption-Keys werden über die Server an den jeweiligen Recipient weitergeleitet. Im Zuge der Authentifikation gegenüber dem Wickr Netzwerk, generiert die Benutzerin beziehungsweise der Benutzer die jeweiligen Identity-Schlüsselpaare. Der öffentliche Schlüssel wird an die Server gesendet, während der geheime Schlüssel am Endgerät gespeichert wird. Zusätzlich werden mittels ECDH-Verfahren flüchtige Public-Keys erstellt und via den generierten Identity-Keys signiert. Die Payload wird mittels AES-256-GCM-Verfahren verschlüsselt und mittels Transport-Layer-Security (TLS) über den gesamten Kanal sicher übertragen. Die Nachrichten können zu keinem Zeitpunkt von Wickr eingesehen werden, da der Private-Key zur Entschlüsselung lediglich lokal auf den Endgeräten hinterlegt ist [59].

Forward Secrecy: Um Forward Secrecy für die Userinnen und User zu garantieren, verwendet das

von Wickr eingesetzte Protokoll Elliptic-Curve-Diffi-Hellman (ECDH). So wird sichergestellt, dass nach einer Kompromittierung des privaten Schlüsselmaterials keine vergangenen Nachrichten rückwirkend entschlüsselt werden können. Der Einsatz von ECDH im Wickr Protokoll stellt dabei einerseits sicher, dass ausgetauschten Nachrichten zwischen den Clients einen nicht voraussagbaren Shared-Key verwenden, andererseits wird der flüchtige Schlüssel der Empfängerin oder des Empfängers nach der Entschlüsselung vernichtet, sodass eine subsequente Entschlüsselung vergangener Messages nicht möglich ist [59].

Backward Secrecy: Neben der Forward Secrecy wird durch das Wickr Protokoll ebenfalls die Backward Secrecy für Folgenachrichten sichergestellt. Ein potentieller Angreifer ist nach erfolgreicher Kompromittierung des geheimen Schlüsselmaterials nicht in der Lage, zukünftige Nachrichten zu entschlüsseln [59].

MiTM Prevention: Damit die Nutzerinnen und Nutzer der Messaging-Applikation vor Fälschung oder Modifikation ausgetauschter Nachrichten geschützt sind, wurden verschiedene Mechanismen seitens der Entwickler implementiert. Das im Einsatz befindliche 521-Bit ECDH-Key-Agreement-Protokoll leitet zwischen den Clients Shared-Secrets ab und kombiniert diese mit den flüchtigen Schlüsseln des Senders und Receivers. Eine mittels dem 521-Bit-ECDSA-Verfahren generierte digitale Signatur stellt sicher, dass die empfangenen flüchtigen Schlüssel authentisch sind. Mittels sicherer Key-Derivation-Function (KDF) werden aus dem Shared-Secret symmetrische Schlüssel abgeleitet, welche wiederum für die Verschlüsselung des Payloads dienen. Der gesamte Nachrichteninhalt wird weiters mittels digitaler Signatur signiert und authentifiziert. Mittels AES-GCM-Mode werden die Daten verschlüsselt und entsprechend bei der Übertragung geschützt. Diese kryptografischen Mechanismen und Verfahren stellen in Kombination sicher, dass der Nachrichteninhalt der Clients nicht durch einen Angreifer verändert oder verfälscht werden kann, ohne erkennbare Fehlermeldungen hervorzurufen [59]. Um einen weiteren Security-Layer zur eindeutigen Identifikation der Kommunikationspartner zu schaffen, bietet Wickr Me die so genannte Key-Verification-Option. Die Nutzerin beziehungsweise der Nutzer kann diese Verifikation für sämtliche im Adressbuch befindlichen Kontakte durchführen. Über den Security-Verifikation-Button kann der geteilte Verifikations-Code angezeigt werden. Es handelt sich hierbei um einen String, welcher als Vergleichswert zwischen den Teilnehmern fungiert. Stimmt dieser Code auf beiden Seiten überein, kann dem Kontakt vertraut werden. Ein weitere Methode zur sicheren Identifikation bietet der Abgleich eines generierten QR-Codes. Die Herausforderung bei diesem Verifikationsverfahren besteht jedoch darin, dass die Kommunikationspartner sich physisch am selben Ort befinden müssen um den Abgleich erfolgreich durchführen zu können. Alternativ wird seitens des Unternehmens empfohlen, mittels

Video-Call den Abgleich durchzuführen. So kann einerseits ein Bild und Stimmabgleich durchgeführt, anderseits der Security-Code verbal verglichen werden [60].

Disk Encryption: Nach der Installation der Applikation wird auf dem Endgerät ein verschlüsselter Storage-Container erstellt, in welchem sensible Daten wie die Identity-Keys, Nachrichten und Accountinformationen abgelegt werden. Während der aktiven Logon-Session wird der Inhalt für die vollständige Funktionsfähigkeit und Operation entschlüsselt. Loggt sich die Nutzerin beziehungsweise der Nutzer wieder aus, wird der Container mittels dem Local-Storage-Device-Key (Klds) wieder verschlüsselt. Der Klds wird in einem verschlüsseltem Format gespeichert und beim nächsten erfolgreichen Login wiederhergestellt. Der Key zum ver- und entschlüsseln des Local-Storge-Device-Key wird mittels *Scrypt* aus dem Passwort der Userin oder des Users abgeleitet. Um auch die Usability zu gewährleisten, können Nutzerinnen und Nutzer den abgeleiteten Schlüssel im bereitgestellten Secure-Storage ablegen und so eingeloggt verweilen. Ist die Wickr-App im inaktiven Zustand, so werden die Daten automatisch verschlüsselt und vor unautorisiertem Zugriff geschützt [58].

Secure Group Chat: Wickr unterstützt die Gruppenchat-Funktion mittels einer Erweiterung des Core-Protokolls. Der Mechanismus zur sicheren Kommunikation im Kontext des Group-Chats basiert auf dem so genannten Pairwise-Messaging-Protokoll des Unternehmens. In diesem System übermittelt der Admin Management-Messages an die User über das Pairwise-Protokoll, um diese der Gruppe hinzuzufügen. Diese Nachrichten werden gleich den Techniken des Core-Protokolls authentifiziert. Die Server von Wickr können selbstständig einer bestehenden Gruppe keine Mitglieder hinzufügen, somit wird sichergestellt, dass ein kompromittierter Server keine eigenständigen Gruppenbildungen vollziehen kann. Um Nachrichten an die Members zu versenden, muss jede Teilnehmerin oder Teilnehmer initial einen Pairwise-Key mit jedem anderen Mitglied austauschen. Ein einziger Payload-Encryption-Key wird wiederholt kopiert und mittels dem Pairwise-Encryption-Mechanismus für jede Device-Device-Relationship mehrmals verschlüsselt. Der Nachrichteninhalt wird wiederum mit dem Payload-Encryption-Key verschlüsselt. Um Nachrichten zwischen den Teilnehmer auszutauschen, übernimmt der in den Servern implementierte One-to-Many-Mechanismus die korrekte Zustellung der verschlüsselten Nachrichten an die Mitglieder der Gruppe. Resultierend aus diesem implementierten Design, garantiert die Gruppenchat-Funktion der Messaging-Applikation die identischen Sicherheitsstandards gleich dem Core-Protokoll [59].

3.3 Usability Properties

Multi Device Support: Wickr Me erlaubt es seien Userinnen und Usern den jeweiligen Account auf mehreren Geräten gleichzeitig zu verwenden. Dazu muss lediglich die Messaging-Applikation erneut auf dem zweiten Gerät installiert und mit den bestehenden Credentials eine Authentifizierung vollzogen werden. Im Wickr Secure Messaging Protokoll werden die Endgeräte als so genannte Nodes bezeichnet. Werden Nachrichten vom zweiten Gerät an einen Reciever, welcher ebenfalls mehrere Geräte im Einsatz hat, versendet, so wird die Message an alle Nodes zugestellt. Um die Ende-zu-Ende-Verschlüsselung zu gewährleisten, erstellt jede neu hinzugefügte Node bei der Initialisierung ein neues Set von Schlüsselmaterial zur sicheren Kommunikation. Ein wesentlicher Nachteil ist die fehlende Datensynchronisierung zwischen den Geräten. Ältere Konversationen können auf einem neuen Gerät nicht wiederhergestellt werden. Dieses Feature wurde vom Unternehmen lediglich für die kostenpflichtige Wickr Pro Version implementiert. Die Datensynchronisierung kann in den Einstellungen der Applikation mittels QR-Code-Verifizierung konfiguriert und freigegeben werden [58].

E2E by Default: Das Wickr Me Secure-Messaging-Protokoll erlaubt den Nachrichtenaustausch generell nur mittels Ende-zu-Ende-Verschlüsselung. Eine Client-Server-Verschlüsselung wurde von den Entwicklerinnen und Entwicklern nicht vorgesehen und ist bis dato auch nicht implementiert. Jeglicher Datenaustausch ist standardmäßig über den gesamten Kommunikationskanal gesichert. Nach der Installation und Initialisierung müssen seitens der Userinnen und User keine weiteren Einstellungen zur sicheren Übertragung getätigt werden. Die End-to-End-Encryption ist somit der standardmäßige Modus zur Kommunikation [58].

Easy Contact Discovery: Die Messaging-Applikation verfolgt den Ansatz, die Privatsphäre der Nutzerinnen und Nutzer bestmöglich zu schützen, gleichermaßen soll die Nutzerfreundlichkeit nicht eingeschränkt werden. Kontakte können mittels der festgelegten Wickr-ID gefunden und zum eigenen Adressbuch hinzugefügt werden. Voraussetzung dafür ist, dass eine Einwilligung zur Contact-Discovery einhergeht, somit wird die Userin oder der User nur mittels Opt-In für andere Kontakte sichtbar. Weiters bietet die Applikation die Möglichkeit, die Discovery-Funktion generell zu deaktivieren. Ist dies der Fall, so müssen Kontakte manuell dem Adressbuch hinzugefügt werden. Um mögliche Kontakte zu identifizieren, welche ebenfalls den Messaging-Dienst verwenden, steht es den Usern ebenfalls frei, dass Adressbuch in gehashter Form auf die Wickr-Server zu hinterlegen. Dies hat den Vorteil, dass die Kontaktlisten veröffentlicht werden, dass Adressbuch jedoch nicht frei zugänglich auf den firmeneigenen Servern gespeichert wird. Durch diese Methode wird ein hoher Grad an Privatsphäre erzielt, da

es den Nutzerinnen und Nutzern frei steht, Kontaktdetails zu teilen und mittels Opt-In-Entscheidungen Einstellungen proaktiv zu konfigurieren [61].

Easy Key Maintenance: Nach der Installation der Messaging-Applikation auf dem Endgerät, werden alle für die sichere Kommunikation erforderlichen Schlüssel automatisch generiert. Die flüchtigen Schlüssel werden in so genannten Pools auf den eigenen Servern des Unternehmens verwaltet und bedarf keiner manuellen Wartung durch die Userin oder den User. Sämtliches Schlüsselmaterial wird bei jeder Verwendung automatisch durch den Root-of-Trust signiert und validiert. Das gesamte Schlüsselmanagement wird durch Wickr Me übernommen und setzt keine Interaktion seitens der Nutzerinnen oder Nutzer voraus [58].

Transcript Consistency: In der Gruppenchat-Funktion der Messaging-Applikation sorgt das Protokoll durch den One-to-Many-Mechanismus neben der Verschlüsselung des Nachrichteninhalts auch für die korrekte Nachrichtenreihenfolge bei der Zustellung. Versendete Nachrichten werden auf den Wickr-Servern verschlüsselt in eine Queue gepuffert und anhand der Nachrichten-ID an die jeweiligen Gruppenmitglieder gemäß ihrer Reihenfolge versendet und angezeigt [59].

Asynchronous: Auch bei dieser Applikation handelt es sich um einen Messenger, welcher für die erfolgreiche Nachrichtenzustellung nicht voraussetzt, dass die Empfängerin oder der Empfänger zur Zeit des Nachrichtenempfangs online ist. Versendete Nachrichten werden von den Wickr-Servern verschlüsselt zwischengespeichert und beim erfolgreichen Verbindungsaufbau seitens des Receivers zugestellt. Das Protokoll unterstützt somit den asynchronen Nachrichtentransfer [58].

No Monetary Costs: Die Wickr Me Applikation ist für sämtliche mobilen Endgeräte als auch Desktopvarianten kostenlos erhältlich, wobei alle beschriebenen Funktionen dabei unterstützt werden. Lediglich Upgrades in den Formen Silver, Gold und Platinum erfordern die Verrichtung einer monatlichen Gebühr. Diese Pakete sind jedoch im Unternehmenskontext relevant und wurden für diese Analyse nicht einbezogen [62].

4 Threema

Bei Threema handelt es sich um ein Unternehmen aus der Schweiz, welches 2012 den gleichnamigen Messaging-Dienst veröffentlicht hat. Laut eigenen Angaben liegt der Schwerpunkt der Applikation auf starker Security inklusive dem Schutz der Privatsphäre. Ein vom Unternehmen veröffentlichtes Dokument [63] zeigt, dass die Nutzerzahlen bereits 8 Millionen überstiegen haben, somit zählt der Kurznachrichtendienst aktuell zu den beliebtesten Lösungen im europäischen Raum. Anders als bei der Kon-

kurrenz, handelt es sich bei Threema um eine kostenpflichtige Software. Die Einnahmen erlauben es dem Unternehmen, sich eigenständig zu finanzieren, somit werden Werbeschaltungen obsolet und die Privatsphäre hinsichtlich personalisierter Werbung gewahrt. Der Name des Messengers ist nicht zufällig gewählt, so leitet er sich aus dem englischen Begriff der Ende-zu-Ende-Verschlüsselung ab. Aus „End-to-End Encrypting Messaging Application“, abgekürzt EEEMA, wurde schließlich Threema.

4.1 Privacy / Anonymity Properties

Proxy Server: Die Messaging-Applikation Threema unterstützt keinen Nachrichtenaustausch über Proxy-Server beziehungsweise wurde eine entsprechende Funktion nicht implementiert. Ein von Staaten verhängtes Geo-Blocking kann dementsprechend nicht von den Nutzerinnen und Nutzern umgangen werden. Die Verwendung des Kurznachrichtendienstes ist somit nicht ganzheitlich anonym und beschränkt sich auf Userinnen und User, welche sich in Ländern aufhalten, in denen die Nutzung der Applikation zugelassen ist. Aktuell gibt es seitens der Betreiber keine Pläne, Proxy-Server als weiteres Feature zu implementieren.

Minimal Data Collection: Bei der Nutzung der Messaging-Applikation sollen laut Aussage des Unternehmens lediglich Daten für die ordnungsgemäße Funktionalität gesammelt und gespeichert werden. Nachrichten werden zur asynchronen Datenübermittlung bis zur erfolgreichen Zustellung an den Kommunikationspartner in verschlüsselter Form auf die Server zwischengespeichert und anschließend restlos gelöscht. Dies gilt sowohl für 1-1- als auch für Gruppenchats. Die Kontaktlisten der Nutzerinnen und Nutzer werden zum Zweck der Synchronisation anonymisiert (gehasht) an die Server übermittelt und nach Abschluss des Abgleichvorgangs ebenfalls wieder gelöscht. Diese Funktion ist standardmäßig deaktiviert, die Nutzerin oder der Nutzer muss dieser Synchronisierung zunächst zustimmen. Kontakte können standardmäßig manuell beziehungsweise über die QR-Code-Verifizierung dem Adressbuch hinzugefügt werden. Weiters werden die Useraktivitäten als auch IP-Adressen nicht geloggt, somit kann nicht nachvollzogen werden, welche Parteien miteinander kommunizieren. Optional angegebene Telefonnummern als auch Mailadressen der Nutzerinnen und Nutzer werden als Hash auf den Servern hinterlegt. Des Weiteren speichert das Unternehmen das Datum der Erstellung der Threema-ID als auch das Datum des letzten Logins durch die Userin oder den User. Aufgrund der eingeschränkten Datensammlung ist das Konzept Privacy-by-Design umgesetzt und der Grundsatz der minimalen Datenverarbeitung wird beim Messaging-Dienst eingehalten [64] [65].

Server Location: Das Schweizer Unternehmen betreibt sämtliche für die Applikation notwendigen Server im Großraum Zürich. Jegliche Nutzerdaten werden auf diesen gespeichert und verlassen den

Europäischen Wirtschaftsraum zu keinem Zeitpunkt. Zusätzlich sind die Rechenzentren ISO 27001-zertifiziert, was deutlich die implementierten Sicherheitsstandards wiederspiegelt [66].

Anonymous Usage: Der Nachrichtendienst kann ohne Angabe personenbezogener Daten von den Nutzerinnen und Nutzern installiert und verwendet werden. Die Identifizierung der einzelnen Teilnehmerinnen und Teilnehmer erfolgt mittels Vergabe einer Threema-ID, welche bei der Initialisierung zufällig generiert wird. Das Hinzufügen einer Telefonnummer und/oder Mailadresse ist dabei optional und dient lediglich dem Zweck der erleichterten Contact-Discovery. Threema setzt die Angabe einer gültigen Rufnummer nicht voraus und kann somit anonym und ohne den Upload von Telefonbuchdaten genutzt werden. Den Betreibern selbst ist es laut eigener Angabe nicht möglich, die tatsächliche Identität hinter einer Threema-ID zu ermitteln, sofern nur diese als Identifikator seitens der Userinnen und User hinterlegt wird [64].

No Advertising Information: Da es sich bei Threema um einen kostenpflichtigen und somit durch die Nutzerinnen und Nutzer finanzierten Kurznachrichtendienst handelt, ist das Unternehmen nicht an Partnerschaften mit Werbe- und Analyseunternehmen angewiesen. Die Applikation schaltet somit keine Werbungen und gibt Nutzerdaten, sofern diese überhaupt relevant für eine Auswertung oder Analyse wären, nicht an Dritte weiter [64].

GDPR Compliance: Neben den technischen und organisatorischen Maßnahmen und dem damit verbundenem Schutz vor unbefugtem Datenzugriff und Missbrauch, erfolgt die Datenverarbeitung im Einklang mit den geltenden Bestimmungen der Datenschutz-Grundverordnung. Der Zweck der Datenverarbeitung laut der Datenschutzerklärung von Threema beschränkt sich auf die Bearbeitung von Supportanfragen. Jegliche für diesen Zweck verarbeitete Daten werden spätesten nach 6 Monaten Inaktivität dauerhaft gelöscht. Den Nutzerinnen und Nutzern wird das Recht eingeräumt, jederzeit Auskunft über die von Threema gespeicherten personenbezogenen Informationen zu erhalten. Ebenso haben Userinnen und User das Recht, Änderungen beziehungsweise Ergänzungen der Datensätze und die Löschung sämtlicher Informationen zu veranlassen. Neben der Compliance gegenüber der Datenschutz-Grundverordnung ist Threema als Schweizer Unternehmen weiters verpflichtet, den Anforderungen des Schweizer Datenschutzgesetzes (DSG) genauso wie der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) nachzukommen [65] [66].

Deletable Messages: Nachrichten können sowohl in 1-zu-1-Chats als auch in der Gruppenchat-Funktion von den Nutzerinnen und Nutzern gelöscht werden, jedoch erfolgt dieser Vorgang nur lokal auf dem Endgerät. Bereits versendete Nachrichten können somit nicht für sämtliche Teilnehmerinnen und Teilnehmer einer Konversation zurückgezogen werden. Um ausgetauschte Inhalte gänzlich zu löschen,

müssen sämtliche Empfänger den lokalen Wipe vollziehen. Das Fehlen dieses Features stellt neben Datenschutzbedenken auch ein potentielles Sicherheitsrisiko dar, besonders wenn sensible Informationen versehentlich an die falsche Person gesendet werden und diese nicht mehr rückholbar sind [64].

Self Destructive Messages: Neben der fehlenden Eigenschaft, versendete Nachrichten auf allen Empfängergeräten zu löschen, unterstützt die Messaging-Applikation ebenfalls keinen Versand von selbstzerstörenden Nachrichten. Für eine Löschung sind die Nutzerinnen und Nutzer somit von ihren Gesprächspartnern abhängig. Threema begründet das Fehlen beider Features mit der Möglichkeit, gelöschte Nachrichten und deren Inhalte mittels dem Auslesen des Benachrichtigungs-Logs des Betriebssystems rückführen zu können. Somit wird die Verlässlichkeit und Sicherheit dieser Funktionen in Frage gestellt. Diese Annahme ist durchaus richtig, jedoch erfordert dieser Vorgang ein gewisses Maß an technischer Affinität. Aus Sicht eines Angreifers kann dies sicherlich ausgenutzt werden, jedoch wird dieses Feature an dieser Stelle innerhalb der Domäne der Privatsphäre und nicht der Security analysiert [67].

Screenshot Detection: Hinsichtlich der Screenshot-Detection wurde von Threema keine Funktion implementiert, welche die Senderin oder den Sender auf eine Bildschirmaufnahme hinweist. Es kann somit nicht nachvollzogen werden, ob versendete Nachrichten extern von den Kommunikationspartnern gespeichert werden [67].

4.2 Security Properties

Cryptographic Primitives: Für die Kommunikation und die Verschlüsselung benutzt die Messaging-Applikation die quelloffene Programmbibliothek NaCI. Das Protokoll bedient sich 255-Bit langen asymmetrischen Schlüsseln, welche mittels Elliptic-Curve-Verfahren erzeugt werden und nach Angaben der NIST mit 2048-Bit langen RSA-Schlüsseln vergleichbar sind. Dieser generierte Schlüssel wird dazu eingesetzt, um für jede versendete Nachricht einen einmaligen symmetrischen 256-Bit-Key zu erzeugen. Zur endgültigen Verschlüsselung der einzelnen Nachrichten bedient sich Threema dem XSalsa20 Stream Cipher. Um Manipulationen am Inhalt der Nachricht vorzubeugen, wird ein 128-Bit langer Verifikationscode inklusive einer zufälligen Anzahl an so genannten kryptografischen Füllbytes (Padding) zu jeder Nachricht hinzugefügt. Der private Schlüssel wird bei der Initialisierung der Applikation mittels Random Number Generator auf den Endgerät erzeugt. Der korrespondierende öffentliche Schlüssel wird anschließend mittels Curve25519 kalkuliert. Die Key-Fingerprints werden mittels SHA-256 in Kombination mit Teilen des öffentlichen Schlüssel erstellt. Die von Threema eingesetzten kryptografischen Primitiven zum sicheren Nachrichtenaustausch entsprechen dem Stand der Technik und können als sicher eingestuft werden [68].

End-to-End Encryption: Wie bereits erwähnt, verwendet Threema zur sicheren Kommunikation die Open Source Bibliothek NaCI als Verschlüsselungsprotokoll. Zum Einsatz kommen dabei zwei Verschlüsselungsschichten, die End-to-End-Schicht zwischen den Kommunikationsparteien und die Client-Server-Schicht als zusätzlicher Security-Layer, welche vor dem Abhören der Verbindung zwischen App und Server schützt. Einer Angreiferin beziehungsweise einem Angreifer soll es dadurch unmöglich sein, durch abgefangene Netzwerkpakete herauszufinden, wer mit wem kommuniziert. Die Verschlüsselung und Entschlüsselung erfolgt ausschließlich auf dem jeweiligen Endgerät, da lediglich die Benutzerin oder der Benutzer die entsprechenden Keys besitzt. Somit wird sichergestellt, dass auch Threema selbst versendete Nachrichten nicht entschlüsseln und lesen kann. Beide Verschlüsselungs-Layer kommen beim Senden und Empfangen von Nachrichten zum Einsatz. Dabei ist wichtig zu erwähnen, dass die Ende-zu-Ende-Schicht ungehindert über den Server übertragen wird und nicht aufgebrochen werden kann. Sämtliche Nachrichten inklusive Mediendateien und Audioaufnahmen werden ausnahmslos End-to-End-Verschlüsselt übertragen. Die asymmetrischen Schlüssel werden wie erwähnt auf den Endgeräten mittels ECC-Verfahren generiert, wobei lediglich der öffentliche Schlüssel auf den Servern gespeichert wird. Neben der Verschlüsselung erfolgt die Authentifizierung der Nachrichten mittels der so genannten Box-Modell-NaCl-Networking-and-Cryptography-Library. Die Ende-zu-Ende-Verschlüsselung ist bei der Messaging-Applikation standardmäßig aktiviert und kann nicht von der Userin oder dem User umgangen werden. Die eingesetzten Methoden und Verfahren gelten als State-of-the-Art und bieten den Kommunikationsparteien einen holistischen Schutz über den gesamten Kanal [68].

Forward Secrecy: Die Messaging-Applikation erfüllt dieses Kriterium nur partiell, da Forward Secrecy lediglich für die Client-Server-Netzwerkverbindung implementiert wurde, jedoch nicht für die Ende-zu-Ende-Schicht zwischen den Kommunikationsteilnehmern. Zufällige temporäre Schlüssel werden zwischen Client und Server ausgehandelt, welche ausnahmslos im RAM gespeichert und bei jedem Neustart der Applikation neu generiert werden. Diese Methode soll verhindern, dass eine Angreiferin oder ein Angreifer aufgezeichneten Netzwerk-Traffic im Nachhinein in Verbindung mit dem Private-Key des Servers oder des Clients entschlüsseln kann. Laut Angaben des Unternehmens wurde auf Forward Secrecy im Bereich der Ende-zu-Ende-Kommunikation aufgrund der Protokollkomplexität verzichtet. Die Implementierung würde die Zuverlässigkeit des Protokolls beeinträchtigen, was wiederum zu Sicherheitslücken führen könnte. Es ergibt sich jedoch ein hohes Sicherheitsrisiko durch das Fehlen dieser Funktion, da die Kompromittierung des privaten Message-Keys zur Nachrichtenverschlüsselung das Lesen vergangener Korrespondenz ermöglichen könnte [68] [69] [70].

Backward Secrecy: Auf die Implementierung von Backward-Secrecy wurde seitens des Unterneh-

mens gänzlich verzichtet. Aufgrund der erwähnten Probleme durch die steigende Komplexität des Protokolls durch die Implementierung dieser Art von Sicherheitsmechanismen, wird dieses Feature auch nicht auf der Client-Server-Ebene eingesetzt. Folgenachrichten können somit durch den Verlust des Schlüsselmaterials entschlüsselt und gelesen werden [68].

MiTM Prevention: Die Verbindung zwischen der Threema-Applikation und dem Server wird gegen Angriffe gesichert, indem sich der Server mittels Schlüssel authentifiziert, welcher hardcoded in die App einprogrammiert ist und der entsprechende Private-Key lediglich dem legitimen Server bekannt ist. Kontakte werden beim Kurznachrichtendienst mittels Vertrauensstufen verifiziert. Diese Stufen dienen als Maß für die Sicherheit, dass der gespeicherte Public-Key eines Kommunikationspartners tatsächlich zu diesem gehört. Bei Stufe 1 muss die ID und der öffentliche Schlüssel vom Server heruntergeladen werden, da vom Kontakt erstmalig eine Nachricht eingetroffen ist. Aufgrund der fehlenden Einträge (Mail oder Mobilnummer) im Adressbuch, kann nicht verifiziert werden, ob der Kontakt legitim ist. Mit Vertrauensstufe 2 lässt sich mit einer gewissen Sicherheit sagen, dass der Kontakt durchaus die vorgegebene Person ist, da die entsprechenden Einträge im Adressbuch lokalisiert werden können. Die Vertrauensstufe 3 bietet das höchste Maß an Vertrauen, da neben den passenden Einträgen auch eine gegenseitige Verifizierung mittels QR-Scan die Vertrauenswürdigkeit des jeweiligen Kontakts sicherstellt. Die jeweiligen Stufen werden mittels Farbcodierung von rot bis grün neben den jeweiligen Einträgen im Adressbuch angezeigt [68].

Disk Encryption: Die Messaging-App speichert die lokalen Daten, also versendete und empfangene Nachrichten genauso wie das Adressbuch, verschlüsselt auf dem Endgerät. Die Methode zur Verschlüsselung und zur Speicherung variiert von Plattform zu Plattform. Beim iOS-Betriebssystem werden die Daten in der Core-Data-Database gespeichert, welche sich im Private-Data-Directory der Applikation befindet. Durch das Sandboxing wird sichergestellt, dass andere Apps keinen Zugriff auf die jeweiligen Informationen erhalten. Die Files werden weiters durch das iOS-Data-Protection-Feature geschützt. Der entsprechende Encryption-Key wird von der UID des Geräts in Kombination mit einer Passphrase abgeleitet. Bei Android werden die Daten in einer SQLite-Datenbank innerhalb des Private-Data-Directory der Applikation gespeichert. So lange das Gerät nicht gerootet wird, können andere Applikationen nicht auf die Daten zugreifen. Die Datenbank selbst ist mittels SQLCipher in Kombination mit AES-256 verschlüsselt. Der entsprechende Schlüssel wird bei der Initialisierung des Datenbank randomisiert erstellt und mittels Passphrase gesichert [68].

Secure Group Chat: In Threema werden die Gruppen ohne Involvierung des Servers verwaltet. Die Server können in der Theorie nicht ermitteln, welche Teilnehmerinnen oder Teilnehmer einer be-

stimmten Gruppe angehören. Wird eine Nachricht von der Senderin oder den Sender an die jeweiligen Mitglieder verschickt, so wird der Inhalt individuell verschlüsselt und an jedes Gruppenmitglied separat zugestellt. Der Nachrichtenaustausch erfolgt über einen verschlüsselten Session-Channel zwischen Client und Server, von wo diese an die jeweiligen Empfänger weitergeleitet werden. Der Schlüsselaustausch erfolgt via einer mit dem Long-Term-Key verschlüsselten Group-Message, welche über den Encrypted-Session-Channel an die entsprechenden Mitglieder verteilt wird. Simple Textnachrichten als auch Media-Files werden gleich dem 1-zu-1-Chat Ende-zu-Ende-verschlüsselt übertragen [68] [69].

4.3 Usability Properties

Multi Device Support: Derzeit ist es noch nicht möglich, die Applikation mit derselben Threema-ID auf mehreren Geräten zu verwenden. Aktuell wird nur die gleichzeitige Verwendung der Web-Applikation unterstützt, da hierbei eine Verbindung zum Mobilgerät aufgebaut wird und dadurch eine Synchronität erreicht werden kann. Um die Messaging-Applikation auf mehreren mobilen Endgeräten gleichzeitig verwenden zu können, müssen Userinnen und User auf einen Workaround zurückgreifen. Pro Device wird eine andere Threema-ID eingerichtet, die IDs werden anschließen in einer Gruppe als Members verwaltet. Aktuell arbeitet das Unternehmen daran, die Multi-Device-Funktion mittels Mediator-Server zu realisieren. Sowohl die Gerätesynchronisation als auch die Nachrichtenreflektion sollen mit derselben ID auf jedem Endgerät ermöglicht werden [64] [71].

E2E by Default: Versendete Nachrichten, obgleich diese simple Textmessages oder Media-Files sind, werden standardmäßig Ende-zu-Ende-verschlüsselt übertragen. Das in Threema implementierte Protokoll sieht ebenfalls keine Client-Server-seitige Nachrichtenverschlüsselung vor, somit müssen Userinnen und User keine Einstellungen zur sicheren Datenübertragung tätigen beziehungsweise vorab einen Secure-Channel erstellen [68].

Easy Contact Discovery: Um Kontakte dem Adressbuch hinzuzufügen, bietet der Kurznachrichtendienst den Userinnen und Usern mehrere Möglichkeiten. Neue Kontakte können über die jeweilige Threema-ID, welche aus einer 8-stelligen Kombination aus Zahlenwerten und Buchstaben besteht, manuell hinzugefügt werden. Entscheidet sich die Nutzerin beziehungsweise der Nutzer dazu, dass eigene Adressbuch mittels Opt-In-Option als gehashten Wert auf die Server von Threema zu übermitteln, so werden Kontakte automatisch hinzugefügt und angezeigt. Bei dieser Option erfordert es keiner manuellen Tätigkeit seitens der User. Alternativ können Kontakte mittels einen dafür generierten QR-Code-Scan hinzugefügt werden. Dies ist die sicherste Methode, da der Scanvorgang von den jeweiligen Kommunikationspartnern persönlich vorgenommen werden muss und damit eine gleichzeitige Verifikation

sichergestellt wird [66] [68].

Easy Key Maintenance: Sämtliches zur sicheren Kommunikation erforderliches Schlüsselmaterial wird initial von der Applikation generiert. Der private Teil verbleibt auf dem jeweiligen Endgerät, die öffentlichen Keys werden automatisch an die Server übermittelt und gefetched. Session-Keys werden ebenfalls pro Nachricht automatisch generiert. Die Userin beziehungsweise der User muss zum Nachrichtenaustausch kein Schlüsselmanagement übernehmen. Ein großer Nachteil ist jedoch im Key-Backup zu finden. Um mit der Threema-ID das eigene Konto auf einem anderen Gerät verwenden zu können, muss der Private-Key manuell mittels Passwort gesichert werden. Verliert die Nutzerin oder der Nutzer das Schlüsselmaterial oder vergisst das Passwort, kann der Account nicht mehr wiederhergestellt werden [68].

Transcript Consistency: Jede versendete Nachricht wird mittels einer so genannten Reference-ID versehen und gleich dem 1-zu-1-Chat an die jeweiligen Gruppenmitglieder einzeln versendet. Der Identifikator besteht dabei aus einer randomisierten Nummer inklusive einem Zeitstempel, um die Nachrichten in ihrer korrekten Reihenfolge an die Empfänger zu senden. Die Messaging-Applikation erfüllt somit die Anforderung an die Transcript Consistency [72].

Asynchronous: Auch bei Threema werden versendete Nachrichten auf den eigenen Server zur asynchronen Datenübertragung in verschlüsselter Form zwischengespeichert. Die Senderin beziehungsweise der Sender ist nicht gezwungen darauf zu warten, bis der Receiver online ist um eine erfolgreiche Nachrichtenübertragung vollziehen zu können. Ist die Empfängerin oder der Empfänger zur Zeit der Zustellung offline, so bleibt die Nachricht so lange auf den Servern zwischengespeichert, bis ein erfolgreicher Verbindungsaufbau hergestellt und die Nachricht letztendlich weitergeleitet werden kann. Kann die Nachricht nicht zugestellt werden, so wird diese nach einer bestimmten Zeit von den Servern restlos gelöscht [66].

No Monetary Costs: Der Kurznachrichtendienst ist weder für die mobile noch für die Desktopversion frei erhältlich. Threema bietet den Nutzerinnen und Nutzern verschiedene Versionen, vom privaten bis zum kommerziellen Gebrauch, welche dementsprechend in anderen Preiskategorien zu finden sind. Das Unternehmen begründet die Kosten für den Erwerb der Applikation durch die damit verbundene Sicherung der Privatsphäre, da Threema nicht auf Einnahmen durch Werbepartner angewiesen ist und die persönliche Informationen im Machtbereich der Nutzerinnen und Nutzer bleibt [66].

5 Signal

Der Kurznachrichtendienst Signal wurde von den beiden US-Amerikanern Moxie Marlinspike und Stuart Andersen entwickelt, welche bereits seit dem Jahr 2008 an verschlüsselten Applikation arbeiten. Mit dem NSA-Whistleblower Edward Snowden als Fürsprecher für die App, genießt Signal einen besonders guten Ruf unter den Messaging-Diensten. Der ehemalige WhatsApp-Mitbegründer Brian Acton investierte 2018 eine Summe von 50 Millionen US-Dollar in die neu gegründete non-profit Signal Foundation. Das in der App implementierte Ende-zu-Ende-verschlüsselte Signal-Protokoll gilt in der Kryptoszene als der neue Standard und wurde auch von den Konkurrenten WhatsApp und dem Facebook-Messenger übernommen. Nachdem WhatsApp die Datenschutzerklärung geändert und angekündigt hatte, Daten mit dem Mutterkonzern Facebook auszutauschen, erfolgte eine regelrechte Nutzerabwanderung. Besonders Signal erfreute sich an einem massiven Zuwachs. Die Nutzerzahlen der Applikation betragen mit Stand Jänner 2021 zirka 40 Millionen User. Das Protokoll selbst ist Open-Source und die Applikation steht zum kostenlosen Download zur Verfügung. Somit generiert das Unternehmen keine Einnahmen durch App-Downloads, sondern erhält über Spenden der Nutzerinnen und Nutzer beziehungsweise durch Investoren die notwendigen Ressourcen zum Betrieb und zur Weiterentwicklung der Applikation [70] [73].

5.1 Privacy / Anonymity Properties

Proxy Server: Um staatliche Zensur zu umgehen, hat Signal den Quellcode zum Aufsetzen eigener Proxy Server veröffentlicht. Dieser soll laut Angaben des Unternehmens relativ leicht zu konfigurieren sein und bedarf keiner speziellen Kenntnis im Bereich der Informationstechnik. Das Feature wurde vor allem zur Unterstützung der iranischen Userinnen und User ins Leben gerufen, da die dort geltenden Gesetzte den Einsatz der Applikation verbieten. Über den TLS-Proxy wird der gesamte Datenverkehr geleitet und somit die Blockade umgangen. Anders als beim simplen HTTP-Proxy, lässt sich über den verschlüsselten TLS-Traffic nicht ermitteln, ob der Datenverkehr über einen Proxy geroutet wird. Weiters werden bei Signal für jeden Server TLS Zertifikate ausgestellt, somit wird es für Staaten schwieriger den Traffic über Fingerprinting zu analysieren. Der Client baut demnach eine normale TLS-Verbindung zum Proxy auf, welcher in weiterer Folge die versendeten Bytes an den Endpoint weiterleitet. Nicht-Signal-Traffic wird dabei geblockt und verworfen. Neben der Ende-zu-Ende-Verschlüsselung wird somit sämtlicher Traffic verschleiert. Aktuelle Proxy-Server werden in verschiedenen Foren und Social-Media-Seiten wie beispielsweise Twitter veröffentlicht und aktualisiert [74] [75].

Minimal Data Collection: Zur erfolgreichen Registrierung müssen Userinnen und User ihre Te-

lefonnummer hinterlegen, welche von Signal gespeichert werden. Optional können weitere Account Informationen wie Profilname und Profilbild angegeben werden. Diese Informationen werden stehts über einen Unique-Profile-Key Ende-zu-Ende-verschlüsselt und über den Signal-Protokoll-Messaging-Channel ausgetauscht. Das Unternehmen kann somit nicht auf diese Accountinformationen zugreifen. Nachrichten werden lediglich auf den Severn bis zur erfolgreichen Übermittlung zwischengespeichert und anschließend wieder gelöscht. Technische Informationen zum reibungslosen Betrieb des Services wie Authentication-Token und Schlüsselmaterial werden auf den Server gespeichert, jedoch auf ein absolutes Minimum beschränkt. Optional können Nutzerinnen und Nutzer ihr Adressbuch in gehashter Form zum Zweck der Easy-Contact-Discovery auf die Server hochladen. Die Datensammlung beschränkt sich beim Messaging-Dienst auf das absolute Minimum [76].

Server Location: Der Messaging-Dienst greift beim Hosting der Server-Infrastruktur auf Firmen wie Google, Amazon und Microsoft zurück. Das bedeutet, dass eine Vielzahl an Servern außerhalb des Europäischen Wirtschaftsraum beheimatet sind, und Daten zwangsläufig in die Vereinigten Staaten übermittelt werden. In den Nutzerbedingungen ist dies so festgehalten und Userinnen und User müssen dieser Übermittlung vorab einwilligen. Da jedoch das Protokoll auf dem Zero-Knowledge-Prinzip aufbaut, tut diese Tatsache der Sicherheit von Signal keinen Abbruch. Nachrichten und Informationen können durch die im Einsatz befindlichen Verfahren weder von Drittanbietern noch von Signal selbst gelesen werden. Es ist den Userinnen und Usern zwar möglich, eigene Server und somit einen eigenen Signal-Dienst zu betreiben, deren Nutzer könnten jedoch nicht mit jenen des offiziellen Dienstes kommunizieren [76] [77].

Anonymous Usage: Signal verfolgt den Ansatz der minimalen Datenspeicherung als auch dem Zero-Knowledge-Prinzip und hält so gut wie keine Informationen über die Nutzerinnen und Nutzer der Applikation. Da jedoch die Angabe einer validen Telefonnummer als Voraussetzung zur erfolgreichen Registrierung mittels zugesendetem SMS-Code vorausgesetzt wird, kann der Dienst nicht völlig anonym verwendet werden. Obgleich weder Signal noch Drittanbieter auf die angegeben Daten aufgrund starker Verschlüsselung nicht zugreifen können, so existiert eine Komponente, welche auf eine natürliche Person Rückschlüsse geben kann [78].

No Advertising Information: Da es sich bei Signal um eine Non-Profit-orientierte Organisation handelt und Umsätze lediglich durch Investments und Spenden generiert werden, beinhaltet der Messenger keine Werbung und gibt gesammelte Informationen nicht an Drittanbieter weiter. Da aufgrund der Privacy-Policy und dem Leitsatz zum Schutz der Privatsphäre grundsätzlich keine relevanten Daten vorhanden sind, würde sich eine Weitergabe der Datensätze als kaum sinnvoll darstellen. Weiters

zeichnet sich der Dienst durch den Verzicht von Tracking und Affiliate-Marketing, also datengestütztes Marketing, aus [76].

GDPR Compliance: Signal ist aufgrund der minimalen bis kaum vorhandenen Datenspeicherung konform gegenüber der Datenschutz-Grundverordnung. Neben der Telefonnummer werden lediglich technische Informationen zum reibungslosen Betrieb des Messaging-Dienstes seitens des Unternehmens aufbewahrt. Kontaktdaten werden nur dann gespeichert, wenn die Nutzerin beziehungsweise der Nutzer eine explizite Berechtigung hierfür erteilt. Es werden zu keinem Zeitpunkt sensible Daten gespeichert, noch kann Signal Nachrichten oder Anrufe entschlüsseln. Ausgetauschte Messages werden lediglich bis zur Zustellung in verschlüsselter Form auf den Servern zwischengespeichert und anschließend restlos gelöscht. Ebenso ist die gesamte Nachrichtenhistorie ausschließlich auf dem Endgerät gespeichert und wird niemals auf die Signal-Server übermittelt. Das Recht auf Auskunft, Änderung genauso wie die Löschung der von den Userinnen und User bereitgestellten Daten wird diesen ohne Einschränkung eingeräumt [77].

Deletable Messages: Bei der Messaging-Applikation können Userinnen und User einzelne versendete Nachrichten oder gar ganze Unterhaltungen lokal auf dem Endgerät oder für alle Teilnehmer löschen. Beide Optionen werden im Chatmenü zur Verfügung gestellt. Ein großer Nachteil ist jedoch, dass lediglich Nachrichten nicht älter als drei Stunden gelöscht werden können. Wird diese Zeit überschritten, so können Messages lediglich lokal auf dem Gerät entfernt werden, für Gesprächspartner beziehungsweise Gruppenmitglieder sind diese weiterhin vorhanden [79].

Self Destructive Messages: Nutzerinnen und Nutzer haben die Möglichkeit, versendete Nachrichten mit einem Timer zur automatischen Löschung für alle Teilnehmer zu versehen. Hierbei wird wieder zwischen zwei verschiedenen Modi unterschieden. Zum einen gesendete *Verschwindende Nachrichten*, zum anderen empfangene *Verschwindende Nachrichten*. Beim ersteren startet der konfigurierte Timer ab den Zeitpunkt des Sendens der Nachricht. Dabei macht es keinen Unterschied, ob die Empfängerin oder der Empfänger die Nachricht gelesen hat oder nicht. Die Message zerstört sich selbst nach Ablauf der Zeit. Letzteres wartet auf die Lesebestätigung des Receiver. Erst nachdem die Nachricht tatsächlich vom Kommunikationspartner gelesen wurde, startet der Timer zur automatischen Löschung. Die Userinnen und User können dabei ein Zeitintervall zwischen 5 Sekunden bis zu einer Woche vorkonfigurieren. Durch eine grafisch dargestellte Uhr neben der entsprechenden Message wird diese als selbstzerstörend gekennzeichnet. Dieses Feature ist sowohl für alle mobile Versionen als auch für die Desktop-Applikation verfügbar [80].

Screenshot Detection: In Signal gibt es keine Möglichkeit eine Empfängerin oder einen Empfän-

ger daran zu hindern, Screenshots vom Chatverlauf zu tätigen. Auch werden Sender nicht darüber informiert, dass eine solche Aktion getätigt wurde. Der Kurznachrichtendienst bietet zwar die Option Bildschirmaufnahmen zu sperren, jedoch nur lokal auf dem eigenen Endgerät. Somit ist lediglich ein partieller Schutz vorhanden. Die vorhin erwähnten Verschwindenen Nachrichten können somit mühelos extern von der Kommunikationspartnerin oder dem Kommunikationspartner gespeichert werden, bevor der Timer abläuft und der Inhalt gelöscht wird [80].

5.2 Security Properties

Cryptographic Primitives: Das Signal-Protokoll verwendet standardisierte kryptografische Algorithmen, welche bereits von einer Vielzahl an Security-Researchern auf Herz und Nieren geprüft wurden und als absolut sicher eingestuft sind. Für die symmetrische Verschlüsselung kommt der Advanced-Encryption-Standard (AES), teils mit Cipher-Block-Chaining-Mode (CBC) inklusive Füllbits nach PKCS 5 und teils im Counter-Mode (CTR) ohne Füllbits, zum Einsatz. Der Nachrichtenauthentifizierungscode wird mittels HMAC auf Basis von SHA-256 generiert. Für den Diffi-Hellman-Ratchet bedient sich das Protokoll am ECDH in Verbindung mit der elliptischen Kurve Curve25519. Für den Hash-Ratchet wird der Keyed-Hash-Message-Authentication-Code verwendet. Diese kryptografischen Verfahren stellen neben dem sicheren Nachrichtenaustausch auch die Signatur als auch die Authentifizierung der Messages sicher. Der essentielle Mechanismus im Signal-Protokoll stellt der so genannte Double-Ratchet dar, welcher das Ableiten der symmetrischen Keys für die Nachrichtenverschlüsselung im asynchronen Environment sicherstellt. Diese Schlüssel werden aus dem Shared-Secret der Kommunikationsparteien, welches aus dem X3DH-Key-Agreement-Protokoll generiert wurde, abgeleitet. Die digitalen Signaturen basieren auf den XEdDSA- und VXEdDSA-Signatur-Schemata [1].

End-to-End Encryption: Das Signal-Protokoll stellt neben der Verschlüsselung des Nachrichteninhalts über den gesamten Transportweg auch die Authentifikation des Kommunikationspartners und die Absicherung gegen Manipulation der Messages sicher. Der Austausch der Nachrichten erfolgt über den bereits erwähnten Double-Ratchet-Algorithmus, welcher als grundlegendes Konzept die so genannte KDF-Kette verwendet. Die Key-Derivation-Funktion (KDF) generiert mit Hilfe eines geheimen Schlüssel inklusive Eingabedaten mehrere Ausgabewerte. Eines dieser Werte ist ein neuer Key, welcher wiederum als Eingabewert für die KDF dient und dadurch eine Chain bildet. Insgesamt bildet der Algorithmus drei KDF-Ketten. Die Wurzelkette erzeugt mittels Diffi-Hellman neue Ausgabeschlüssel, welche als KDF-Schlüssel für die Nachrichtenketten (Sende und Empfang) verwendet werden. Mit Hilfe dieser Nachrichtenketten wird für jede einzelne Nachricht ein neuer Key generiert, mit der die Message

verschlüsselt wird. Weiters wird durch den Algorithmus erreicht, dass zusätzlich zur Inhaltsverschlüsselung auch der Nachrichtenkopf verschlüsselt übertragen werden kann. Signal als auch Drittanbieter sind durch den starken Verschlüsselungsmechanismus nicht in der Lage, Korrespondenz zwischen den jeweiligen Kommunikationspartnern zu lesen [81].

Forward Secrecy: Um Forward Secrecy zu erreicht, bedient sich die Messaging-Applikation dem Diffi-Hellman-Key-Exchange. Dabei wird jede einzelne versendete Nachricht mit einem neu generiertem Key verschlüsselt. Dieser flüchtige Schlüssel wird nach der erfolgreichen Zustellung wieder restlos gelöscht. Über den Ephemeral-Key-Exchange gelangt das erforderliche Schlüsselmaterial zu den jeweiligen Peers, wobei alle eingesetzten Parameter ebenfalls nach dem Empfang verworfen werden. Damit wird erreicht, dass auch nach der Kompromittierung des geheimen Schlüsselmaterials durch eine Angreiferin oder einem Angreifer, diese oder dieser nicht in der Lage ist, vergangene Korrespondenz zu entschlüsseln. Das Protokoll sieht ebenfalls keine Langzeitschlüsseln voraus, somit existiert kein Master-Key um alle ausgetauschten Nachrichten zu entschlüsseln [72].

Backward Secrecy: Diese Eigenschaft erreicht der Messenger mit dem gleichen Verfahren des Diffi-Hellman-Key-Exchange. Da jede Nachricht mittels einem eigenen Key verschlüsselt wird und dieser anschließend nach der erfolgreichen Zustellung wieder gelöscht wird, kann eine Angreiferin oder ein Angreifer nachfolgende Nachrichten auch nach einer Kompromittierung des Schlüsselmaterials nicht entschlüsseln. Das Protokoll ist gegen Angriffe in diesem Bereich absolut robust [72].

MiTM Prevention: Um sicherzustellen, dass die Verbindung nicht durch eine Man-in-th-Middle-Attacke kompromittiert wurde, erfolgen bei Signal Authentifizierungsverfahren sowohl für Client-Server- als auch Client-to-Client-Verbindungen. Signal hat 3 verschiedene Main-Server, einer für das Versenden von Textnachrichten und zwei für die Übertragung von Voice-Calls, wobei alle mittels TLS abgesichert sind. Die Serverzertifikate werden stehts mit der eigenen Certificate-Authority signiert, die Zertifikate wiederum sind in der Applikation als BKS Trust-Stores gepinned. Alle Verbindungen werden mittels diesen Trust-Stores sowohl für Textnachrichten als auch für Voice-Calls gesichert. Der Client kann sich somit sicher sein, dass der verbundene Server legitim ist. Der Client authentifiziert sich gegenüber dem Server mittels Basic-Access-Authentication. Mittels einem generierten Passwort bei der Registrierung des Endgeräts und der respektiven Rufnummer kann sich der Client beim Server authentifizieren. Für die Client-zu-Client-Authentifikation, generiert jeden Endgerät einen Unique-Identity-Key. Möchte ein Client einem anderen eine Nachricht senden, werden beiden Identity-Keys dazu verwendet, einen flüchtigen Shared-Key abzuleiten. Die Identity-Keys werden dabei vom Signal-Server abgerufen und auf dem Gerät gespeichert. Nachdem der Handshake erfolgreich durchgeführt wurde, können die Clients

den berechneten Fingerprint vergleichen. Stimmt dieser überein, können die Kommunikationsparteien einen Man-in-the-Middle-Angriff ausschließen. Ändert sich zu einem Zeitpunkt der Identity-Key eines Clients, so erfolgt eine Benachrichtigung an diese. Eine erneute Authentifizierung muss durchgeführt werden, um die Sicherheit zu gewährleisten [70].

Disk Encryption: Signal erlaubt es seinen Userinnen und Usern sämtliche Nachrichten lokal auf dem Endgerät zu verschlüsseln. Im Zuge der Registrierung wird ein so genannter Master-Key aus dem Userpasswort abgeleitet, welcher zum ver- und entschlüsseln der Nachrichten dient. Für den Verschlüsselungsprozess kommt der AES-CBC und HMAC-SHA1 zum Einsatz. Eine Angreiferin oder ein Angreifer kann somit auch beim physischen Zugriff auf des Gerät die verschlüsselten Nachrichten nicht lesen [70].

Secure Group Chat: Die Gruppenchat-Funktion bei Signal ist ähnlich der Funktion von Threema. Nachrichten werden als Direct-Message gewertet, wobei die Group-ID am verschlüsselten Plaintext angehängt wird. Der Signal Server ist somit theoretisch nicht in der Lage, zwischen einer Gruppennachricht und einer Direktnachricht zu unterscheiden. Jede Nachricht wird Ende-zu-Ende-verschlüsselt an die Gruppenmitglieder versendet. Die Verbindung zwischen den Clients und dem Server wird gleich den Direktnachrichten mittels TLS gesichert. Kommt die Nachricht beim Server an, so wird die Receiver-ID mit der Sender-ID ausgetauscht und anschließend an die entsprechenden Empfänger zugestellt. Die Sicherheit der Gruppenchat-Funktion von Signal ist somit als gleichwertig dem Direct-Messaging zu betrachten [72].

5.3 Usability Properties

Multi Device Support: Neben dem mobilen Endgerät kann das Signal Konto auch gleichzeitig in der Desktop-Applikation und auf Apple iPads verwendet werden. Sowohl mehrere mobile Geräte als auch Android-Tablets unterstützen derzeit nicht die Multi-Device-Funktion. Kompatible Geräte werden mittels QR-Code-Scan an das mobile Endgerät gekoppelt. Senden und Empfangen ist nach der erfolgreichen Koppelung auf beiden Clients möglich. Die Daten werden ebenfalls automatisch synchronisiert und konsistent gehalten [82].

E2E by Default: Das Signal-Protokoll ist so konzipiert, dass sowohl sämtliche Text- als auch Audionachrichten standardmäßig über den gesamten Transportweg Ende-zu-Ende-verschlüsselt übertragen werden. Die Nutzerin oder der Nutzer muss keine weiteren Einstellungen tätigen, um die sichere Kommunikation zu gewährleisten. Eine unsichere Client-Server-verschlüsselung ist in Signal nicht vorgese-

hen. Neben der standardmäßigen E2E-Verschlüsselung bietet Signal Android Clients die Möglichkeit, die Applikation als Default-SMS/MMS-App zu konfigurieren [1].

Easy Contact Discovery: Bei der Messaging-Applikation können Kontakte auf zwei unterschiedliche Art und Weisen hinzugefügt werden. Möchte die Userin oder der User den bestmöglichen Schutz der Privatsphäre im Bereich der Contact-Discovery erreichen, so müssen Kontakte manuell mittels Rufnummer dem Adressbuch hinzugefügt werden. Wird der App jedoch die Berechtigung für den Zugriff auf das Adressbuch erteilt, so wird jede im Adressbuch gefundene Nummer mittels SHA256 gehasht und auf die Signal Server übertragen. Verwendet ein im Adressbuch gefundener Kontakt ebenfalls den Kurznachrichtendienst, so wird dieser automatisch hinzugefügt. Die Nutzerinnen und Nutzer werden anschließend über diese Aktualisierung mittels Benachrichtigung informiert [83].

Easy Key Maintenance: Die Schlüsselerzeugung zur sicheren Kommunikation über den gesamten Transportweg inklusive den implementierten Authentifizierungsverfahren werden automatisch bei der Initialisierung erstellt und die öffentlichen Teile an die entsprechenden Endpunkte übermittelt. Die flüchtigen Keys zur Nachrichtenverschlüsselung werden automatisch ohne jegliche Interaktion der Userin oder des Users generiert. Ändert sich der Public-Key eines Kommunikationspartners, so erfolgt eine automatische Benachrichtigung. Es obliegt der Nutzerin beziehungsweise dem Nutzer, diesem neuen Key zu vertrauen oder eine neue Authentifikation vorzunehmen. Die Wartung des Schlüsselmaterials wird durch die Applikation automatisiert durchgeführt und setzt keine Handlungen durch den Client voraus [70].

Transcript Consistency: Damit Nachrichten in der Gruppenchat-Funktion weder Dupliziert noch in verschiedener Reihenfolge an die jeweiligen Members zugestellt wird, werden sämtliche Nachrichten mit einer Message-ID inklusive einem Timestamp versehen. Die eingehenden Nachrichten werden anhand dieser ID geprüft und anschließend auf Basis des Zeitstempels geordnet und zugestellt [72].

Asynchronous: Da jede Nachricht mit einem eigenen Key verschlüsselt wird um so Perfect Forward Secrecy zu gewährleisten, müssen für das asynchrones Messaging PreKeys erstellt und von der Empfängerin oder dem Empfänger gefetched werden, sobald wieder eine Verbindung zum Server besteht. Dazu werden bei der Registrierung signierte PreKeys erstellt und auf dem Server gespeichert. Ist die Empfängerin oder der Empfänger offline, so wird die Nachricht auf dem Server zwischengelagert. Sobald der Client wieder online ist, werden Nachrichten und die dazugehörigen Keys vom Server gepushed [70].

No Monetary Costs: Der Kurznachrichtendienst ist in sämtlichen Version kostenlos erhältlich. Eine kostenpflichtige Variante für Unternehmen existiert nicht. Da Signal non-profit-orientiert ist, werden sämtliche Einnahmen mittels Spenden und Investments generiert. Das stellt mitunter einen großen Vor-

teil für die Applikation dar, da keine Abhängigkeiten zu Drittanbietern beziehungsweise Werbeagenturen besteht, und somit die Privatsphäre der Nutzerinnen und Nutzer gewahrt wird, da Daten zu Einnahmewecken nicht weitergegeben werden [76].

6 Whatsapp

Bei WhatsApp handelt es sich um einen im Jahr 2009 gegründeten Instant-Messaging-Dienst, welcher 2014 von Facebook Inc. übernommen wurde. Bis Anfang 2016 war die Nutzung der Applikation kostenpflichtig, danach wurde sie frei zugänglich für alle Nutzerinnen und Nutzer. WhatsApp gilt auch nach der umstrittenen Änderung der Allgemeinen Geschäftsbedingungen, welche die Weitergabe von Userdaten an den Mutterkonzern Facebook vorsieht, als Platzhirsch mit rund 2 Milliarden Nutzer [84] (Stand Juli 2021) unter den Messengern. Nach den Negativschlagzeilen erfolgte jedoch eine regelrechte Abwanderung zu den Konkurrenten Signal und Threema, doch bleiben die meisten Userinnen und User der App treu. Was die Applikation besonders auszeichnet, ist sowohl die plattformunabhängige Nutzung des Dienstes als auch die angebotenen Features sowie eine besonders hohe Nutzerfreundlichkeit. Im Bereich der Sicherheit ist ein robustes Protokoll im Einsatz mit einer starken Ende-zu-Ende-Verschlüsselung inklusive einer Zwei-Faktor-Authentifizierung, welche optional eingestellt werden kann. Kritik wird jedoch von Datenschutzexperten geäußert, da WhatsApp nicht sparsam im Bereich der Datensammlung über seine Userinnen und User ist.

6.1 Privacy / Anonymity Properties

Proxy Server: Im Messaging-Dienst kann der Datenaustausch nicht über Proxy-Server erfolgen, da das Unternehmen keine entsprechende Funktionalität implementiert hat. Es existieren zwar Lösungen hierfür von Drittanbietern, jedoch sollte aus Sicherheitsgründen davon abgesehen werden. Ebenfalls kann durch den Einsatz von Proxies der Service beziehungsweise einige Features nicht richtig funktionieren. WhatsApp selbst ist nicht darauf ausgelegt, mit Proxy- oder VPN-Diensten kompatibel zu sein, dementsprechend wird dafür kein Support geboten [85].

Minimal Data Collection: WhatsApp erhebt neben dem Zweck zum ordnungsgemäßen Betrieb der Applikation auch Informationen zur Verbesserung, Individualisierung und Vermarktung des Dienstes. Die Breite der Datensammlung hängt dabei von der Art und Weise ab, wie Userinnen und User die Messaging-Applikation und deren Features nutzt, das heißt, die Verwendung optionaler Funktionen berechtigt weitere Datensammlungen. Zur Erstellung eines Accounts müssen die Nutzerinnen und Nutzer ihre valide Telefonnummer als auch einen Profilnahmen angeben. Diese Informationen werden auf den

WhatsApp Servern dauerhaft gespeichert. Grundsätzlich werden Nachrichten nach der erfolgreichen Zustellung von den Servern gelöscht. Eine Ausnahme stellen nicht zugestellte Nachrichten genauso wie Mediendateien dar. Nachrichten werden für einen Zeitraum von bis zu maximal 30 Tagen in verschlüsselter Form auf den Servern gespeichert, bevor diese restlos gelöscht werden. Mediendateien werden ebenfalls temporär auf den Server zwischengespeichert, um die Zustellung von Weiterleitungen effizienter zu gestalten. WhatsApp mach jedoch keine Angabe, wie lange diese Inhalte genau aufbewahrt werden. Falls die Userin oder der User der Applikation Zugriff auf das Adressbuch gewährt, so wird dieses als Hashwert vom Unternehmen gespeichert. Neben Statusinformation werden auch Gruppenzugehörigkeiten von der Applikation erfasst und mit den Accountinformationen verknüpft. Werden die von WhatsApp angebotenen Zahlungsdienste verwendet, so erhebt das Unternehmen Zahlungskonto- und Transaktionsinformationen inklusive Zahlungsmethode, Versanddetails und Transaktionsbetrag. Zu den vom WhatsApp automatisch erhobenen Daten zählen unter anderem Nutzungs- und Protokollinformationen. Zu diesen zählen dienstspezifische Informationen sowie Daten zu Diagnosezwecke und Performanceevaluierung. Ebenfalls werden Aktivitätsdaten, also die Häufigkeit und Dauer der Nutzung, erfasst. Darüber hinaus werden Informationen zu genutzten Funktionen gespeichert und verarbeitet. Neben den Nutzungsdaten sammelt das Unternehmen Geräte- und Verbindungsdaten. Zu diesen zählen Hardware-Modell und Betriebssystem, Batteriestand, Signalstärke, App-Version, Informationen zum Browser und zum verwendeten Mobilfunknetz, einschließlich Telefonnummer, Mobilfunk- oder Internetanbieter, Sprache und Zeitzone inklusive IP-Adressen. Genaue Standortinformationen zur Ortung können nach der Zustimmung durch die User ebenfalls erhoben werden. Eine komplette Verweigerung zur Erhebung ist jedoch nicht möglich, da die App auch ohne expliziter Zustimmung IP-Adressen und Vorwahlen speichern, und so den ungefähren Standort ermitteln kann. Wird die webbasierte Version von WhatsApp verwendet, so werden Cookie-Informationen mit dem Argument des verbesserten Nutzererlebnis und individueller Anpassung gesammelt [86].

Server Location: WhatsApp nutzt für die Datenübertragung die globale Infrastruktur vom Mutterkonzern Facebook, unter anderem auch in den USA. Informationen, welche vom Unternehmen gesammelt und gespeichert werden, werden für die in der Datenschutzerklärung beschriebenen Zwecke in die USA und Drittländer übermittelt und verarbeitet. Diese Übermittlung ist laut Angaben des Unternehmens für den globalen Betrieb des Messengers unerlässlich. Um diese Übermittlung konform gegenüber europäischen Bestimmungen zu halten, greift WhatsApp auf die *Standard Contractual Clauses* (SCC) zurück [87]. Diese Klausel bestimmt, dass Daten von EU-Bürgerinnen und Bürger lediglich dann außerhalb des Europäischen Wirtschafsraum verarbeitet werden dürfen, wenn das Schutzniveau den geltenden

Datenschutzbestimmungen innerhalb der EU, äquivalent sind. Der Datentransfer aus dem EWR in die USA ist durch diese Klausel legitim [86].

Anonymous Usage: Neben dem durchaus hohen Grad der Datensammlung, kann WhatsApp auch nicht anonym verwendet werden, da bei der Installation eine valide Telefonnummer angegeben werden muss. Anderenfalls kann die Messaging-Applikation nicht verwendet werden, da im Zuge der Registrierung ein Identifikationscode auf die Rufnummer geschickt wird. Aufgrund der enormen Nutzerdaten wie beispielsweise Standortinformationen und IP-Adressen, welche WhatsApp durchgehend sammelt, kann eine anonymisierte Nutzung des Dienstes nicht realisiert werden [86].

No Advertising Information: WhatsApp arbeitet mit Drittanbietern und anderen Facebook-Unternehmen zusammen, um nach eigenen Angaben die Nutzererfahrung des Dienstes stetig zu verbessern, zu individualisieren und zu vermarkten. Diese Partnerunternehmen führen im Auftrag von WhatsApp Marketingtätigkeiten, Umfragen und Forschungen durch. Personenbezogene Daten über die Nutzerinnen und Nutzer werden dementsprechend für diesen Zweck an Drittanbieter und Facebook-Unternehmen weitergegeben. Werden innerhalb der Applikation externe Dienste verwendet, so erfolgt ebenfalls ein Datenaustausch mit dem jeweiligen Unternehmen. Die Nutzung von Drittanbieterdiensten und Services zieht mit sich, dass die jeweils eigenen Bedingungen und Datenschutzrichtlinien in Kraft treten. Werden von WhatsApp selbst Nutzerdaten an Partnerunternehmen weitergegeben, so gibt das Unternehmen laut der Datenschutzerklärung an, dass sämtliche Datenverarbeitung nur im Einklang mit den Anweisungen und Vorgaben von WhatsApp selbst erfolgen darf. Keine der Informationen, die WhatsApp auf dieser Grundlage weitergibt, dürfen für die eigenen Zwecke der Facebook-Unternehmen oder Drittanbietern verwendet werden [86].

GDPR Compliance: WhatsApp steht seit den angekündigten Änderung seiner AGB und der Datenschutzrichtlinie unter massiver Kritik. Diese Änderung beinhaltet die die Weitergabe von Nutzerdaten an den Mutterkonzern Facebook. Sollte dem nicht zugestimmt werden, so kann der Dienst nicht mehr genutzt werden, zumindest nach dem Tenor der Medien. Tatsächlich muss bei WhatsApp zwischen zwei Unternehmen unterschieden werden, WhatsApp Ireland Limited und WhatsApp LLC. Ersteres ist für den Europäischen Wirtschaftsraum zuständig, und die Nutzung unterliegt der geltenden Datenschutzbestimmung, welche durchaus im Einklang mit geltendem europäischen Recht ist. Außerhalb der EU fällt der Zuständigkeitsbereich unter die Datenschutzbestimmungen von WhatsApp LLC, welche im Bezug auf den Schutz der Privatsphäre deutlich schwächer ist. Mit der Aktualisierung der Allgemeinen Geschäftsbedingungen ändert sich für die Nutzer aus dem EWR nichts, da die Weitergabe personenbezogener Daten an Facebook-Unternehmen wie beispielsweise Telefonnummer oder IP-Adresse bereits in

der alten AGB verankert war und die Nutzerin beziehungsweise der Nutzer dieser Weitergabe ausdrücklich zustimmen muss. Facebook darf ebenfalls keine Daten dazu verwenden, personalisierte Werbung anzeigen zu lassen. Dafür müsste WhatsApp gemäß der Datenschutz-Grundverordnung eine ausdrückliche Einwilligung einholen. Diese ist jedoch ungültig, wenn sie nicht freiwillig erfolgt, da hier das Koppelungsverbot in Kraft tritt. Außerhalb der EU erfolgt jedoch ein deutlich größerer Datenaustausch mit Facebook. So können die Nutzerdaten von nicht europäischen Userinnen und User an den Mutterkonzern zum Zweck der personalisierten Werbung und auch für deren Produkte verwendet werden. Für die User aus dem EWR ändert sich mit der neuen AGB nichts. Gemäß den geltenden Datenschutzbestimmungen haben Nutzerinnen und Nutzer des Kurznachrichtendienstes das Recht auf Auskunft, Berichtigung, Übertragbarkeit beziehungsweise Löschung der bereitgestellten Informationen. Ebenfalls wird ihnen das Recht eingeräumt, bestimmten Verarbeitungen der personenbezogenen Informationen einzuschränken und zu widersprechen. Bereits erteilte Einwilligungen können jederzeit widerrufen werden. Bei einem Widerspruch wird die Verarbeitung eingestellt, sofern diese nicht aus berechtigten oder rechtlichen Gründen erforderlich ist. Die Messaging-Applikation ist aufgrund der einzuholenden Einwilligungen sowie der an die Userinnen und User gegebenen Rechte zur Modifikation beziehungsweise Einschränkung der Datenverarbeitung, konform gegenüber der DSGVO [86].

Deletable Messages: Die Messaging-Applikation bietet die Funktion, versendete Nachrichten sowohl lokal auf dem Endgerät als auch für alle Teilnehmer in den Gruppenchat-Funktion und 1-zu-1-Chats restlos zu löschen. Die gelöschte Nachricht wird mit dem Text „Diese Nachricht wurde gelöscht“ substituiert. Zu beachten ist jedoch, dass diese Funktion nur dann verfügbar ist, wenn alle Teilnehmer die aktuellste Version auf dem Endgerät installiert haben. Des weiteren können Nachrichten mit Medieninhalten nicht für andere Teilnehmer gelöscht werden, da zum Beispiel Fotos automatisch in die Galerie des Mobiltelefons verschoben werden, und der Sender keinen Zugriff darauf hat. Die Löschfunktion für alle Teilnehmer ist nach dem Versand der Nachricht lediglich für eine Stunde verfügbar, danach kann diese nicht mehr zurückgezogen werden [85].

*Self Destructive Messages:*Nutzerinnen und Nutzer können in den Chateinstellungen festlegen, dass Nachrichten nach Ablauf eines Timers automatisch gelöscht werden. Diese Funktion ist sowohl im Gruppenchat als auch 1-zu-1-Chat verfügbar. Das Zeitintervall kann jedoch nur auf 7 Tage festgelegt werden und startet ab dem Zeitpunkt des Versendens der Nachricht. Für Medieninhalte ist diese Funktion nur partiell geeignet. Ist das automatische Herunterladen von Medien aktiviert, so kann diese Nachricht nicht gelöscht werden [85].

Screenshot Detection: Aktuell ist diese Funktion nicht in der Messaging-Applikation implementiert.

Es lässt sich somit nicht bestimmen, ob ein Kommunikationsteilnehmer versendete Nachrichten mittels Screenshot extern auf dem Endgerät speichert. Nutzerinnen und Nutzer sind somit der Gefahr ausgesetzt, dass sensible Nachrichten beziehungsweise Inhalte mit anderen geteilt werden [85].

6.2 Security Properties

Cryptographic Primitives: WhatsApp verwendet für die sichere Kommunikation das von Open Whisper Systems entwickelte Signal Protokoll. Während der Installation auf dem Endgerät werden mittels Curve25519 initial das Signed-Prekey-Schlüsselpaar und mehrere One-Time-Prekey-Pair generiert. Der Identity-Public-Key und die öffentlichen Schlüssel der Prekey-Pairs werden anschließend mit dem Identity-Secret-Key signiert und auf den Server hochgeladen. Der Diffi-Hellman-Key-Agreement beziehungsweise der Diffi-Hellman-Handshake erlaubt es den Kommunikationspartnern über einen Public-Channel ein Shared-Secret zu vereinbaren. Über den X3DH wird das Key-Agreement im asynchronen Environment realisiert. Der Nachrichtenauthentifizierungscode wird mittels HMAC auf Basis von SHA-256 generiert. Das Protokoll verfügt ebenfalls über den Double-Ratchet-Mechanismus, welcher für jede neue Nachricht neue Keys zum verschlüsseln ableitet. Mittels Diffi-Hellman-Verfahren wird nach jedem Ratcheting-Vorgang ein neues Secret zwischen Sender und Receiver vereinbart, aus dem in weiterer Folge Root- und Chain-Keys generiert werden. Über den Chain-Key werden mittels Ableitungsfunktion die Keys zum verschlüsseln der Nachrichten erstellt. Die kryptografischen Primitiven sind allesamt auf Herz und Nieren geprüft und gelten aktuell als State-of-the-Art im Bereich Secure-Messaging [88].

End-to-End Encryption: Im Jahr 2016 wurde die Ende-zu-Ende-Verschlüsselung im Messaging-Dienst implementiert. Sowohl WhatsApp als auch Dritte haben keine Möglichkeit, Nachrichteninhalte einzusehen oder Anrufe abzuhören, da die Ver- und Entschlüsselung der Inhalte ausschließlich auf den jeweiligen Endgeräten stattfindet. Über den gesamten Kommunikationskanal existiert keine Zwischenstelle, welche die Secret-Keys zum entschlüsseln der Nachrichteninhalte besitzt. Sämtliches privates Schlüsselmaterial wird bei der Initialisierung auf dem Endgerät generiert und verlässt dieses zu keinem Zeitpunkt. Die WhatsApp beziehungsweise Facebook Server haben somit keinen Zugriff auf die Private-Keys der Userinnen und User. Die Kommunikation zwischen den WhatsApp Clients und den respektiven Servern erfolgt über einen separaten verschlüsselten Channel. Die Verbindungen werden über so genannte Noise-Pipes mit Curve25519 in Verbindung mit AES-GCM und SHA-256 gesichert [88].

Forward Secrecy: Um die Forward Secrecy, also das Verhindern der Entschlüsselung vergangener Nachrichten durch Kompromittierung des Schlüsselmaterials, zu gewährleisten, stützt sich das Protokoll auf den bereits erwähnten Double-Ratchet-Mechanismus, welcher aus dem Symmetric- und den Diffi-

Hellman-Ratchet besteht. Der Erstere ist für die Erneuerung der Chain-Keys und der Message-Keys verantwortlich. Jede versendete Nachricht wird also mit einem neuen Schlüsselmaterial verschlüsselt. Eine Kompromittierung würde somit nicht bedeuten, dass durch Verlust der privaten Schlüssel sämtliche bereits in der Vergangenheit gesendeten Inhalte entschlüsselt werden können [88].

Backward Secrecy: Damit Folgenachrichten durch die Kompromittierung des Schlüsselmaterials von einer Angreiferin oder einem Angreifer nicht gelesen werden können, werden durch den Double-Ratchet die Chain-Keys auf Basis des Diffi-Hellman-Verfahrens stetig erneuert [89].

MiTM Prevention: Nutzerinnen und Nutzer des Kurznachrichtendienstes haben die Möglichkeit, dass Schlüsselmaterial des Kommunikationspartners und so die Ende-zu-Ende-Verschlüsselung zu verifizieren. Das soll eine Man-in-the-Middle-Attacke seitens eines Attackers oder WhatsApp selbst ausschließen. Die Verifikation kann auf zwei verschiedene Arten vollzogen werden. Die erste Variante ist das Scannen eines generierten QR-Codes, welcher aus einer Version, dem User-Identifier und dem Identity-Key der beiden Parteien besteht. Beim Scanvorgang werden die entsprechenden Schlüssel mit dem Identity-Key, welcher auf den Servern gespeichert ist, verglichen. Bei der zweiten Variante wird ein 60 Zeichen langer String als Basis zu Verifikation herangezogen. Dieser String besteht aus zwei 30 Zeichen langen numerischen Fingerprints der jeweiligen Identity-Keys der Clients. Der Vorteil an dieser Variante besteht darin, dass die Gesprächspartner nicht physisch an einem Ort sein müssen, um den Vergleich zu vollziehen [88].

Disk Encryption: Die Applikation kann mittels Fingerprint für Android-Geräte beziehungsweise Touch- und Face-ID auf iPhones gesperrt werden. Die App wird mittels biometrischen Daten gelocked und soll Dritte daran hindern, Nachrichten auszulesen, sollten diese in den Besitz des Gerätes kommen. Über die genauen Details und Verfahren gibt es aktuell keine Aufzeichnungen, deshalb kann nicht mit Sicherheit davon ausgegangen werden, dass Inhalte ganzheitlich geschützt sind [90].

Secure Group Chat: Nachrichten in der Gruppenchat-Funktion werden ebenfalls über den gesamten Kommunikationskanal Ende-zu-Ende-verschlüsselt übertragen. Der WhatsApp Server ist für die Zustellung an die Gruppenmitglieder basierend auf der jeweiligen Group-ID zuständig. Das Signal-Key-Exchange-Verfahren ist auch in der Group-Chat-Funktion im Einsatz, jedoch in einer abgeänderten Variante. Anstatt an jedes Mitglied einzeln verschlüsselte Nachrichten zu senden, generiert jede Teilnehmerin beziehungsweise jeder Teilnehmer symmetrische Schlüssel (Chain-Key) und verschlüsselt den Inhalt für die gesamte Gruppe. Über das Diffi-Hellman-Verfahren wird der entsprechende Schlüssel an die Gruppenmitglieder verteilt. Die Nachrichten zwischen dem Client und dem Server werden auf Transportebene mittels TLS geschützt. Auf dem End-to-End-Layer ist der Nachrichteninhalt mittels

Symmetric-Ratchet-Encryption (SRE) verschlüsselt [72].

6.3 Usability Properties

Multi Device Support: Die Messaging-Applikation kann aktuell nicht auf mehreren Geräten gleichzeitig verwendet werden, da der Account auf die Rufnummer der Userin oder des Users gemappt ist. Eine simultane Nutzung kann lediglich über die Web- oder Desktop-Applikation beziehungsweise mittels Tablet-Version realisiert werden. Bei diesen Varianten handelt es sich um eine Erweiterung des eigentlichen WhatsApp-Accounts. Die Authentifizierung erfolgt über das Mobiltelefon mittels QR-Code-Scan. Die Synchronisation zwischen Mobilgerät und dem Computer erfolgt automatisch, somit werden sowohl sämtliche versendete und eingehende Nachrichten als auch der gesamte Chatverlauf auf beiden Endpunkten konsistent angezeigt [86].

E2E by Default: Bei WhatsApp werden sowohl sämtliche Chats als auch Video- oder Audio-Calls standardmäßig verschlüsselt. Wird ein neuer Chat geöffnet, so erfolgt eine automatische Benachrichtigung am Anfang des Verlaufs über die Ende-zu-Ende-Verschlüsselung. Das Protokoll ist so konzipiert, dass ein Umgehen der Verschlüsselung nicht möglich ist. Eine Client-Server-Verschlüsselung der Nachrichten ist nicht vorgesehen. Die Userinnen und User müssen keine Konfigurationen treffen oder eigene Secure-Chatkanäle erstellen, um Nachrichten sicher über den gesamten Transportweg zu versenden [1].

Easy Contact Discovery: Den Nutzerinnen und Nutzern steht es mittels Opt-In-Option frei, dass gesamte Adressbuch als kryptografischen Hashwert an die WhatsApp-Server zu übermitteln. Wird die Einwilligung erteilt, dass die Applikation auf die Kontaktliste Zugriff erhält, so werden automatisch alle Teilnehmer hinzugefügt, welche ebenfalls den Messenger verwenden. WhatsApp greift regelmäßig auf das Adressbuch zu und aktualisiert beziehungsweise synchronisiert die Informationen [86].

Easy Key Maintenance: Sämtliches Schlüsselmaterial zur sicheren Kommunikation wird bei der Initialisierung der Applikation auf dem jeweiligen Endgerät automatisch generiert. Die entsprechenden Public-Keys werden ebenfalls automatisch auf den Servern publiziert. Die für die Verschlüsselung benötigten Keys werden über das Ratchet-Verfahren für jede Nachricht selbstständig abgeleitet. Die Applikation kümmert sich um das gesamte Schlüsselmanagement, sodass keine Tätigkeiten seitens der User vorausgesetzt wird [88].

Transcript Consistency: Damit die versendeten Nachrichten innerhalb von Gruppenkonversationen ordnungsgemäß zugestellt werden, wird jede einzelne Message mit einer Group-ID und einem Message-Identifier versehen. Der Server hängt zusätzlich eine Sender-ID als auch einen Timestamp an jede zuzu-

stellende Nachricht an. Anhand dieser Informationen wird der sämtliche Nachrichtenverlauf konsistent gehalten [72].

Asynchronous: Da WhatsApp auf dem Signal-Protokoll basiert, wird das asynchrone Massaging in Kombination mit Forward Secrecy ebenfalls mittels Pre-Keys realisiert. Diese werden auf den Servern gespeichert und zum sicheren Verbindungsaufbau von der Empfängerin oder dem Empfänger gefetched, sobald ein erfolgreicher Verbindungsaufbau hergestellt wird. Die zwischengespeicherte Nachricht wird anschließend zugestellt. Die Clients müssen somit nicht zur selben Zeit online sein, um Nachrichten auszutauschen [88].

No Monetary Costs: Seit 2016 ist der Kurznachrichtendienst für sämtliche Betriebssysteme kostenlos verfügbar. Aktuell gibt es seitens des Unternehmens keine Pläne, kostenpflichtige Versionen anzubieten.

7 Vergleich Messenger

Die Tabelle 4.1 zeigt den direkten Vergleich der einzelnen Messaging-Applikation. Dabei werden die Bewertungskriterien unter die jeweiligen Domänen Privacy / Anonymity, Security und Usability gegliedert. Zur Bewertung wird zwischen *Erfüllt*, *Partiell-Erfüllt* und *Nicht-Erfüllt* unterschieden. Durch dieses Bewertungs-Framework können die einzelnen Applikation pro Domäne direkt verglichen und Aussagen über die jeweiligen Eigenschaften auf einem Blick getätigt werden.

Tabelle 4.1: Gegenüberstellung

Messenger:	Viber	Telegram	WickrMe	Threema	Signal	WhatsApp
Privacy / Anonymity Properties						
Proxy Server	●	●	●	○	●	○
Minimal Data Collection	○	●	○	●	●	○
Server Location	○	●	○	●	○	○
Anonymous Usage	○	○	●	●	○	○
No Advertising Information	○	●	○	●	●	○
GDPR Compliance	●	●	●	●	●	●
Deletable Messages	●	●	●	○	●	◐
Self Destructive Messages	●	◐	●	○	●	◐
Screenshot Detection	●	◐	●	○	◐	○
Security Properties						
Cryptographic Primitives	●	●	●	●	●	●
End-to-End Encryption	●	◐	●	●	●	●
Forward Secrecy	●	●	●	◐	●	●
Backward Secrecy	●	-	●	○	●	●
MitM Prevention	●	●	●	●	●	●
Disk Encryption	○	◐	●	●	●	◐
Secure Group Chat	●	○	●	●	●	●
Usability Properties						
Multi Device Support	◐	●	●	◐	◐	◐
E2E by Default	●	○	●	●	●	●
Easy Contact Discovery	●	●	●	●	●	●
Easy Key Maintainance	●	●	●	◐	●	●
Transcript Consistency	-	●	●	●	●	●
Asynchronous	●	●	●	●	●	●
No Monetary Costs	●	●	●	○	●	●

● = Erfüllt; ◐ = Partiell Erfüllt; ○ = Nicht Erfüllt;

- = Keine Informationen vorhanden;

5 Rechtliche Aspekte

In diesem Kapitel werden die rechtlichen Aspekte analysiert, welche einen Transfer personenbezogener Daten von EU-Bürgerinnen und EU-Bürgern legitimieren. Zunächst erfolgt ein Vergleich der Datenschutzbestimmungen zwischen der Europäischen Union und den Vereinigten Staaten. Des Weiteren werden vergangene Abkommen zwischen der EU und den USA, welche einen Datenaustausch bis zum jeweiligen EuGH-Urteil regelten, analysiert. Zum Schluss werden die aktuellen Vereinbarungen und Regelungen zum rechtskonformen Transfer personenbezogener Daten und deren Verarbeitung aufgezeigt und erörtert.

1 Datenschutzbestimmungen - Vergleich EU und USA

Anders als in Österreich mit dem Datenschutzgesetzt auf staatlicher und mit der Datenschutz-Grundverordnung auf europäischer Ebene, existiert in den Vereinigten Staaten kein allgemein für alle Staaten verbindliches Datenschutzgesetzt. In den USA werden datenschutzrechtliche Bestimmungen branchenspezifisch, beispielsweise für das Gesundheitswesen oder dem Finanzsektor geregelt. Für diese Bereiche gelten eigens verabschiedete Gesetze im Hinblick auf den Datenschutz der Bürgerinnen und Bürger. So sind Unternehmen mit Sitz in den Vereinigten Staaten nach den jeweiligen Datenschutzgesetzten dazu verpflichtet, für die Sicherheit der personenbezogenen Daten zu garantieren. Gleich den europäischen Bedingungen sind die Unternehmen nach einem Databreach dazu verpflichtet, einer umfassenden Meldepflicht nachzukommen. Grundsätzlich gilt jedoch, dass es den Firmen obliegt ihr eigenes Datenschutzniveau festzulegen. Erfolgt ein Verstoß gegen das Versprechen zur Datensicherheit, so wird dies als trügerisches und unlauteres Verhalten gewertet, was wiederum wettbewerbsrechtliche Konsequenzen nach sich zieht. Die US-Aufsichtsbehörde verfügt in diesem Fall über ausreichend Mittel, um die Vorgaben zum Datenschutz durchzusetzen. Verlangte Änderungen innerhalb des Unternehmens können durch langfristige Überprüfungsmaßnahmen erzwungen und kontrolliert werden. Bei schweren Verfehlungen drohen den Firmen hohe Sanktionen [91].

Neben der fehlenden allgemeinen gesetzlichen Regelung ist die Sichtweise in Bezug auf den Datenschutz ebenfalls eine wesentlich andere als die der Europäischen Union. Der Schutz von personenbezogenen Daten ist in Europa als Grundrecht definiert. Im Kontrast dazu gilt der Datenschutz in den USA als Teils des Verbraucherschutzes, was wiederum ein Element des Wirtschaftssektors darstellt. Dieser wirtschaftliche Ansatz manifestiert sich im Hinblick auf die zuständige Behörde. Die datenschutzrechtliche Aufsicht in den USA obliegt der Federal Trade Commission (FTC), also der Bundeshandelskommission, welche für die wettbewerbsrechtliche und verbraucherschutzrechtliche Kontrolle von Unternehmen zuständig ist. In den Mitgliedstaaten der Europäischen Union sind dafür unabhängige Datenschutzbehörden und deren Beauftragte für öffentliche und nicht-öffentliche Stellen zuständig [92].

Obgleich gesetzliche Bestimmungen beziehungsweise vereinzelte Gesetzt in den unterschiedlichsten Wirtschaftssektoren der USA gelten, so ist der Schutz der personenbezogenen Daten auf keinem Fall in dem Maße gewährleistet, wie es in der Europäischen Union der Fall ist. Eingriffe in die Privatsphäre der Bürgerinnen und Bürger gehen nicht primär von den Unternehmen, vielmehr von staatlicher Seite aus. Die Grundlage und somit die rechtliche Legitimität wurde durch den so genannten Patriot Act, welcher nach den Anschlägen vom 11 September verabschiedet wurde, erreicht. Durch dieses zur Terrorabwehr erlassene Gesetzt wurden die Befugnisse der Sicherheitsbehörden extrem ausgeweitet. So sind Behörden seitdem in der Lage, ohne richterliche Anordnung auf Daten zuzugreifen, welche auf US-Servern gespeichert sind. Somit gelten personenbezogene Daten, welche in die USA übermittelt werden, als nicht mehr sicher [92].

Nach den europäischen Datenschutzbestimmungen ist eine Übermittlung personenbezogener Daten aus dem EWR somit nicht vertretbar und rechtlich nicht zulässig. Um eine gesetzliche Basis und somit die Legitimität für einen Datenaustausch zwischen der Europäischen Union und den Vereinigten Staaten zu schaffen, wurden Sonderregelungen ausgehandelt, welche unter dem Namen *Safe Harbor* und *Privacy Shield* bekannt sind. Bei diesen Vereinbarungen handelt es sich um Vereinbarungen, in denen sich amerikanische Unternehmen dazu verpflichten, ein ausreichendes Schutzniveau für die Daten sicherzustellen, sodass der Datentransfer vereinbar mit dem europäischen Datenschutz und die Übermittlung erlaubt ist [91].

2 Safe Harbor

Bei Safe Harbor handelt es sich um ein Abkommen zwischen den Vereinigten Staaten und der Europäischen Union, welches von 2000 bis 2015 den Transfer personenbezogener Daten legitimierte. Konkret handelt es sich um einen Beschluss der EU Kommission auf Basis eines Verfahrens des US-Handelsministeriums. Nach der europäischen Datenschutzrichtlinie, welche als Vorläufer der DSGVO gilt, war eine Übermittlung personenbezogener Daten laut Artikel 25 nicht zulässig, wenn kein angemessener Schutz der Daten gewährleistet wurde. Eben dieses mangelhafte Schutzniveau wurde im US-Datenschutz identifiziert. Nach Artikel 26 konnten jedoch Ausnahmen von der Regelung realisiert werden. Eine solche Ausnahme stellte das Datenschutzabkommen zwischen den USA und der EU. Safe Harbor gewährleistete eine rechtliche Grundlage für den Datenaustausch zwischen den beiden Parteien [93].

Um gegenüber dem Abkommen Konformität zu erreichen und somit den Datentransfer zu legitimieren, mussten Unternehmen an Safe Harbor teilnehmen. Eine externe Zertifizierung wurde jedoch nicht vorausgesetzt beziehungsweise galt nicht als zu erfüllendes Sicherheitskriterium. Unternehmen, welche unter das Abkommen fallen wollten, mussten grundsätzlich nur öffentlich erklären, dass sie sich an die vom Handelsministerium vorgegebenen Prinzipen halten. Dabei wurde vorausgesetzt, dass die folgenden 7 Grundsätze eingehalten werden:

- **Informationspflicht:** Unternehmen müssen sicherstellen, dass ihre Kunden über die erhobenen Daten und den entsprechenden Verwendungszweck aufgeklärt werden.
- **Wahlmöglichkeit:** Die Betroffenen können anderweitigen Nutzungen der Daten widersprechen, sofern diese nicht für den Betrieb der Dienstleistung erforderlich sind.
- **Weitergabe:** Die Kunden müssen vor einer Weitergabe der personenbezogenen Daten an Drittanbieter in Kenntnis gesetzt werden. Gleichzeitig muss eine Opt-Out-Möglichkeit (siehe zweiter Punkt) bestehen.
- **Sicherheit:** Das Unternehmen hat dafür zu sorgen, dass die gespeicherten Daten ausreichend vor unbefugtem Zugriff geschützt werden.
- **Datenintegrität:** Sämtliche gesammelten Informationen müssen vollständig und konsistent sein.
- **Auskunftsrecht:** Die beziehungsweise der Betroffene hat das Recht, über sämtliche gespeicherten Daten Auskunft zu erhalten. Gleichzeitig können Änderungen der Informationen oder eine

Löschung der Datensätze veranlasst werden.

- **Durchsetzung:** Bei Beschwerden müssen sich die Betroffenen an eine entsprechende Stelle wenden können. Diese Stelle muss notfalls in der Lage sein, die Konformität gegenüber den Prinzipien mittels Sanktionen zu erzwingen.

Unter den Voraussetzungen dieser Grundprinzipien von Safe Harbor wurden Unternehmen auf eine Liste des US-Handelsministeriums aufgenommen. Da jedoch die Umsetzung der Vorgaben nicht vom Ministerium selbst geprüft wurden, handelte es sich um eine Selbstzertifizierung. Mit Aufnahme in die Liste wurde den Firmen ein angemessenes Datenschutzniveau zugeschrieben. Der Transfer personenbezogener Daten aus Europa in die USA wurde damit rechtlich legitim.

Besonders breite Kritik erntete das Abkommen von Datenschützern unter anderem aus dem Grund, dass sich die gesamte Umsetzung und Einhaltung der Prinzipien auf den Behauptungen der Unternehmen stützte. Die Compliance gegenüber den Safe Harbor Richtlinien wurde von keiner externen Stelle überprüft. Hinzu kommt, dass das Abkommen als gegenstandslos betrachtet wurde, da die Gesetzeslage in den USA (US Patriot Act) den staatlichen Zugriff auf sensible Daten erlaubt. Nach den Snowden-Enthüllungen wurde die Kritik an Safe Harbor stetig lauter.

Im Oktober 2015 wurde das Abkommen zwischen den USA und der EU durch den Europäischen Gerichtshof aufgehoben. Ausschlaggebend für das Urteil war eine durch den österreichischen Datenschutzaktivisten Maximilian Schrems eingereichte Klage gegen Facebook, da dieser einen unzureichenden Schutz seiner Daten auf den US-Servern sah. Die zuständige Behörde berief sich jedoch auf das Safe-Harbor-Abkommen, so soll der Datenschutz innerhalb der Unternehmen dem des europäischen Niveaus gleichgestellt sein. Der irische High-Court ließ anschließend vor dem EuGH prüfen, ob das Schutzniveau als unzureichend eingestuft werden kann und behielt recht. Der EuGH erklärte das Abkommen für ungültig, da ein gleichwertiger Grad an Datenschutz nicht gewährleistet werden konnte, weil es in den USA an entsprechenden Rechtsvorschriften und Verpflichtungen mangelte. Zudem kommt, dass es für EU-Bürger keine ausreichenden Rechtsschutzmöglichkeiten gebe, welche einen ordentlichen Zugang zu den personenbezogenen Daten sicherstellen sollten. Einen Auszug, eine Korrektur oder die Löschung der Daten konnte in diesem Fall nicht wirksam angefordert werden. Weiters konnte ein Abkommen nicht die Zuständigkeit der Datenschutzbehörde aushebeln, welche selbst für die Prüfung der Anforderungen verantwortlich war. Das Gericht wies ebenfalls auf die potentielle Gefährdung der Grundrechte europäischer Bürgerinnen und Bürger hin, da aufgrund der Rechtslage in den Vereinigten Staaten eine

Überwachung durch US-Behörden praktiziert wird [94].

3 Privacy Shield

Damit nach der Aushebelung von Safe Harbor durch den EuGH weiterhin eine Rechtssicherheit bei der Übermittlung personenbezogener Daten aus den europäischen Raum gewährleistet werden konnte, wurde von der EU-Kommission eine Nachfolgeregelung ausgehandelt. 2016 trat eine neue Vereinbarung mit dem Namen Privacy Shield in Kraft. Besonders Wert wurde auf die vom EuGH kritisierten Punkte zur Verbesserung des damaligen Safe-Harbor-Abkommens gelegt. So konnten sich EU-Bürgerinnen und Bürger im Falle einer Beschwerde an eine von den Geheimdiensten unabhängige Ombudsstelle, welche vom US-Außenministerium eingerichtet wurde, wenden. Des Weiteren wurden die Kriterien zum Datenschutz im Vergleich zu Safe Harbor erheblich verschärft und die Informationspflichten genauer definiert.

Gleich der Herangehensweise von Safe Harbor mussten sich US-Unternehmen, welche personenbezogene Daten von EU-Bürgern verarbeiten wollten, in die von US-Handelsministerium geführte Liste eintragen. Auch hier galt das Prinzip der Selbstzertifizierung der Unternehmen, da sich diese lediglich dazu verpflichteten, die Grundsätze des Privacy-Shield-Abkommens einzuhalten. Im Kontrast zum Safe-Harbor-Abkommen mussten Unternehmen im Fall von Verstößen nun tatsächlich mit hohen Sanktionen rechnen. Unternehmen konnten sich freiwillig auf die Liste setzten, verpflichteten sich jedoch sämtliche Vorgaben einzuhalten um weiterhin geführt zu werden. Bei Verstößen wurde das Recht auf die Datenübermittlung und Verarbeitung entzogen und das Unternehmen musste sich neu qualifizieren [95].

Sobald eine Firma in die Liste eingetragen wurde, verpflichtete sich diese sämtliche Vorgaben, welche für ein angemessenes Datenschutzniveau sorgten, strikt einzuhalten. Ein wichtiges Kriterium stellte unter anderem der Grundsatz der Datensparsamkeit dar. So durften lediglich nur jene Daten verarbeitet werden, welche tatsächlich für den Betrieb erforderlich waren. Weiters musste das Prinzip der Zweckbindung eingehalten werden. Somit durften die personenbezogenen Daten lediglich für den angegebenen Zweck und nicht in einem anderen Kontext verwendet werden. Zur Überprüfung, ob die Regeln beziehungsweise die Vorgaben tatsächlich eingehalten wurde, mussten die Firmen bei Untersuchungen und Anfragen mit dem US-Außenministerium kooperieren [95].

Wurden Daten von EU-Bürgern an US-Unternehmen übermittelt, so konnten diese gewissen Rechte geltend machen:

- **Recht auf Information**
- **Recht auf Auskunft**
- **Recht auf Berichtigung falscher Daten**
- **Recht auf Löschung**
- **Widerspruchsrecht**
- **Beschwerderecht**

Wurden seitens der EU-Bürgerinnen oder EU-Bürger Anfragen gestellt, um eines dieser Rechte in Anspruch zu nehmen, so mussten die US-Unternehmen diese innerhalb von 45 Tagen bearbeiten [95].

Wurden Anfragen nicht entsprechend den Vorgaben des Privacy-Shield-Abkommens entgegengenommen und bearbeitet, so hatten die Betroffenen die Möglichkeit, Beschwerde einzureichen. Alle eingetragenen Unternehmen mussten vorab eine unabhängige Stelle angeben, an die die Kunden Beschwerden richten konnten. Alternativ wurde EU-Bürgern die Möglichkeit eingeräumt, sich direkt an die jeweilige nationale Datenschutzbehörde zu wenden. Im Falle einer Verletzung der Rechte stand den Bürgerinnen und Bürgern als letzte Instanz ein Schiedsverfahren offen.

Einer der größten Kritikpunkte beim Vorgängerabkommen Safe Harbor stellte die Gefährdung der Grundrechte europäischer Bürger durch den staatlichen Zugriff auf die gespeicherten Daten dar. Aufgrund der Gesetzgebung in den Vereinigten Staaten, und besonders durch den erlassenen Patriot Act, verfügten US-Geheimdienste über weitreichende Befugnisse personenbezogene Daten einzusehen. Mit dem Privacy-Shield-Abkommen erhielt die Europäische Kommission eine schriftliche Zusicherung seitens der US-Regierung, dass der staatliche Zugriff auf personenbezogene Daten von EU-Bürgern erheblichen Restriktionen und Kontrollen unterliegen würde.

Obgleich durch das Abkommen ein deutlich höheres Schutzniveau erreicht werden konnte, so war es vielfacher Kritik ausgesetzt. Insbesondere der Zugriff auf staatlicher Ebene auf die gespeicherten Daten stellte weiterhin einen massiven Eingriff in die Grundrechte der EU-Bürgerinnen und Bürger dar. Es existierte weiterhin kein ausreichender Schutz der Daten, da die erwähnte schriftliche Zusicherung keine festen Regeln vorschrieb und diese nicht als verbindlicher Vertrag anzusehen war.

Auch gegen dieses Abkommen strengte der Datenschutzaktivist Max Schrems ein neuerliches Verfahren wegen der Übermittlung seiner personenbezogenen Daten von Facebook Ireland in die USA an. So

warf er dem Unternehmen vor, dass aufgrund der Rechtslage in den USA die übermittelten Daten nicht vor staatlicher Überwachung und willkürlichen Zugriffen geschützt seien. Ein gleichwertiges Datenschutzniveau konnte aufgrund des Patriot Acts nicht erreicht werden. Der EuGH kam letztendlich zum Entschluss, dass die in den Vereinigten Staaten eingesetzten Überwachungsprogramme einen Eingriff in die Grundrechte der Betroffenen Personen darstellte. Ebenso entschied der EuGH, dass mangelnde Schutzmechanismen oder Garantien gegen solche Eingriffe keinesfalls dem Datenschutzniveau der Europäischen Union entsprach. Weiters gewährleistete der Ombudsmannmechanismus nicht, dass die Rechte der Betroffenen effektiv durchgesetzt werden konnten. Am 16. Juli 2020 erklärte der Europäische Gerichtshof das EU-US-Privacy-Shield-Abkommen mit sofortiger Wirkung für ungültig (Urteil in der Rechtssache C-311/18 Data Protection Commissioner / Maximillian Schrems und Facebook Ireland) [96] [94] [92].

4 Standard Contractual Clauses

Seit Mitte des Jahres 2020 herrscht rechtliche Unsicherheit bei Unternehmen, welche US-Produkte nutzen. Neue Datenschutzabkommen mit den Vereinigten Staaten kommen nur sehr schwer voran und die Datenschutzbehörden prüfen verstärkt den Einsatz von US-Diensten. Nachdem der EuGH den Datentransfer in die USA auf Grundlage des Privacy Shield für unzulässig erklärte, müssen nun Unternehmen die Tätigkeiten der EU-Kommission übernehmen und jegliche Übermittlung personenbezogener Daten selbst prüfen. Mit dem Wegfallen des Privacy-Shield-Abkommens bedarf es nun anderer Mittel, um ein gleichwertiges Datenschutzniveau zu erreichen und den Transfer rechtlich zu legitimieren. Ein solches Mittel stellen die Standard Contractual Clauses (SCC), welche zu der wichtigsten Rechtsgrundlage für US-Transfers zählt, dar. Bei diesen Standardvertragsklauseln handelt es sich um Musterverträge, welche im Falle von Datentransfers personenbezogener Daten durch Datenexporteure an Datenimporteure in Drittländer verbindlich sind. In diesen Verträgen verpflichten sich die US-Anbieter beziehungsweise die Unternehmen dazu, das EU-Datenschutzniveau bei der Verarbeitung der Daten einzuhalten [97].

Mit 04.06.2021 hat die EU-Kommission die neuen Standardvertragsklauseln für den internationalen Datentransfer angenommen und veröffentlicht. Die neuen Klauseln sollen die alten Regelungen, welche über 10 Jahre alt sind und somit weder die DSGVO noch das Schrems-II-Urteil berücksichtigen, zeitgemäß ergänzt werden. Vor allem neu ist der Aufbau der Standard Contractual Clauses, so sind die verschiedenen Varianten der Datenübermittlung nicht auf zwei SCC-Muster verteilt, sondern zu einem Dokument zusammengefasst und in 4 verschiedene Module zur flexibleren Vertragsgestaltung geglie-

dert:

- **Modul 1:** Übermittlung von personenbezogenen Daten zwischen zwei Verantwortlichen
- **Modul 2:** Übermittlung von personenbezogenen Daten vom Verantwortlichen an den Auftragsverarbeiter
- **Modul 3:** Übermittlung von personenbezogenen Daten zwischen zwei Auftragsverarbeitern
- **Modul 4:** Übermittlung von personenbezogenen Daten vom Auftragsverarbeiter an den Verantwortlichen

Zu den aktualisierten Standardvertragsklauseln kommt die Pflicht zur Datentransfer-Folgenabschätzung. Das bedeutet, dass nachgewiesen werden muss, ob der Vertragspartner aus dem Drittstaat dazu in der Lage ist, den Verpflichtungen aus dem SCC nachzukommen. Ein weiterer Kernpunkt besteht in der Pflicht zur Abwehr von Regierungsanfragen, so besteht nun eine Benachrichtigungspflicht gegenüber den betroffenen Personen und dem Datenexporteur [98].

Die wesentlichen Regelungsinhalte sind wie folgt:

- **Baukastenprinzip:** Die neuen Standardklauseln sind so konzipiert, dass mehr Optionen zur Vertragsgestaltung zur Verfügung stehen. Für die Übermittlung personenbezogener Daten sind die oben genannten Module vorgesehen.
- **Schrems-II-Klausel:** Vor der Datenübermittlung in Drittländer, muss hinsichtlich der Rechtsvorschriften und Gepflogenheiten im Bereich Datenschutz im Empfängerland eine Risikobewertung durchgeführt werden. Die neuen SCCs beinhalten detaillierte Hinweise zur Durchführung der Risikobewertungen. So wird erreicht, dass die Rechtssicherheit an Granularität gewinnt.
- **Pflichten bei staatlichen Zugriffen:** Neu hinzu kommen die Pflichten des Datenimporteurs im Falle staatlicher Zugriffe auf die Daten. Dazu gehört die Benachrichtigungspflicht gegenüber den betroffenen Personen und dem Importeur. Diese Informationspflicht gilt auch dann, wenn rechtliche Bestimmungen eine Benachrichtigung untersagen. Der Datenimporteur muss sich nach besten Kräften um die Aufhebung des Verbots bemühen, damit die Informationen schnell kommuniziert werden können. Ebenfalls muss der Datenimporteur dafür sorgen, dass die Rechtmäßigkeit staatlicher Zugriffe gegeben ist. Dies gilt besonders für die Überprüfung der einhergehenden Befugnisse und ob gegebenenfalls rechtliche Schritte dagegen eingeleitet werden können.

- **Koppelungsklausel:** Aufgrund der steigenden Komplexität bei der internationalen Datenverarbeitung berücksichtigen die neuen SCCs, dass nachträgliche Änderungen im Bezug auf die Parteien eintreten können. So sieht die optionale Klausel 7 vor, dass zu jeder Zeit neue Beteiligte als Partei den SCCs beitreten können.

Jedoch muss berücksichtigt werden, dass auch bei der Verwendung der neuen SCC eine Einzelfallprüfung des Datenschutzniveaus unumgänglich ist, da die neuen Klauseln alleine unzureichend sind, um den Anforderungen des EuGH gerecht zu werden. Vor allem der Vertragstext und das tatsächliche Schutzniveau sind Gegenstand dieser Überprüfungen. Letzteres wird dabei mittels einem speziell dafür ausgearbeiteten Fragenkatalog, welcher vom Verarbeiter im Drittstaat ausgefüllt werden muss, überprüft. Somit wird sichergestellt, dass die neuen Standard Contractual Clauses nicht einfach nur unterschrieben werden, sondern der Verantwortliche muss selbst aktiv werden, damit der sichere Datentransfer in das entsprechende Drittland rechtlich legitim ist [98].

4.1 Alternativen zu den SCC

Die Verarbeitung personenbezogener Daten außerhalb der Europäischen Union darf laut DSGVO (Art. 44 bis 49 DSGVO) nicht stattfinden, sollte im Drittland kein angemessenes Datenschutzniveau herrschen. Vor allem die Vereinigten Staaten zählen zu diesen Ländern außerhalb des EWR. Um die Angemessenheit des Schutzniveaus zu überprüfen, stehen neben den bereits erwähnten Standard Contractual Clauses auch Alternativen zur Verfügung.

Die EU-Kommission kann mittels so genannten *Angemessenheitsbeschlüssen* [99] das im Drittland herrschende Datenschutzniveau bestimmen und den Datentransfer genehmigen. Derartige Beschlüsse regeln die Übermittlung in die Schweiz, Neuseeland, Andorra, Argentinien, die Färöer Inseln, Guernsey, Japan und im wesentlichen für Kanada, Israel und seit Juni 2021 auf für Großbritannien.

Über *Binding Corporate Rules* können sich Unternehmen auch eigene Datenschutzregeln selbst auferlegen. Die Alternative ist jedoch recht selten, da eine externe Zertifizierung oder interne Prüfung auf Compliance erforderliche ist, um Daten in Drittländer zu übermitteln.

Fällt die Übermittlung unter erforderliche Datentransfers, zum Beispiel wird eine Reise gebucht oder müssen E-Mails in die USA verschickt werden, so ist die Datenverarbeitung im Drittland unter der Vor-

aussetzung, dass dies für die Betroffenen erkennbar ist, erlaubt.

Als letzte Möglichkeit um einen Datentransfer in ein Drittland zu legitimieren, müssen die Betroffenen der Verarbeitung personenbezogener Daten explizite einwilligen. Diese Einwilligungen sind jedoch einerseits relativ umständlich und andererseits fehlt des Öfteren die Transparenz. Oftmals scheitert die Einwilligung auch an der fehlenden Freiwilligkeit beziehungsweise der fehlenden Einwilligungsfähigkeit (in Österreich ab 14 Jahren, s. Art. 8 Abs. 3 DSGVO) [100].

6 Conclusio

Die Privatsphäre gilt in der westlichen Gesellschaft als besonders schützenswertes Gut und wurde von den Vereinigten Nationen als geltendes Menschenrecht beschrieben. Aufgrund der fortschreitenden Digitalisierung ergeben sich besonders im Online-Kontext neue Herausforderungen im Bereich Datenschutz und Anonymisierung. Obgleich es sich hierbei um ein zweischneidiges Schwert handelt, und Anonymisierungstechnologien für strafbare Handlungen missbrauch werden können, so überwiegt das Interesse der Allgemeinheit, sich einer totalitären Überwachung zu entziehen. Die fehlende Sensibilisierung der Nutzerinnen und Nutzer stellt dabei eines des größten Risiken dar, da vorrangig die Meinung nichts zu verbergen zu haben, die Sammlung, Speicherung und Verarbeitung personenbezogener Daten zu rechtfertigen scheint. Dieses Problem manifestiert sich besonders im Bereich Instant-Messaging, da Datenschutzerklärungen entweder nur teilweise oder überhaupt nicht von den Userinnen und Usern gelesen werden. Somit können sie nicht nachvollziehen, welche Daten über sie gesammelt, wohin diese transferiert und zu welchem Zweck sie verarbeitet werden.

Im Zuge dieser Masterarbeit wurden 6 der populärsten Messaging-Applikationen in den Bereichen Privatsphäre/Anonymität, Sicherheit und Benutzerfreundlichkeit auf vorab definierte Eigenschaften untersucht. Die Ergebnisse zeigen, dass es bei der Benutzerfreundlichkeit kaum unterschiede zwischen den einzelnen Messenger gibt. Lediglich Telegram erntet Kritik, da die Ende-zu-Ende-Verschlüsselung nicht standardmäßig aktiviert ist, und Nutzerinnen und Nutzer sich dadurch in falscher Sicherheit wiegen können, da die Nachrichten lediglich mittels Client-Server-Verschlüsselung geschützt werden. Eine besonders hohe Nutzerfreundlichkeit bietet der Kurznachrichtendienst Wickr Me, da diese Applikation sämtliche Anforderungen erfüllt. Im Bereich der Sicherheit bieten die Messenger Signal, Wick rMe und WhatsApp die stärksten Security-Eigenschaften. Telegram wurde aufgrund der fehlenden Default-E2E-Encryption und der Nichterfüllung der Secure-Group-Chat-Eigenschaft schlechter bewertet. Auch der Messenger Threema ist aufgrund mangelhafter Forward-Secrecy und fehlender Backward-Secrecy negativer eingestuft. In der Domäne Privatsphäre und Anonymität konnten die größten Gaps zwischen den Applikationen ermittelt werden. Es zeigt sich, dass vor allem WhatsApp und Viber enorme Da-

ten über ihre Userinnen und User sammeln und zu Werbezwecken an Partnerunternehmen weitergeben. Einen anonyme Verwendung kann weiters nur durch Wickr Me und Threema erreicht werden, da diese Applikationen keine Angabe personenbezogener Daten voraussetzen. Daten verlassen lediglich bei den Messengern Telegram und Threema nicht den EWR, da die Rechenzentren in den Niederlanden beziehungsweise in der Schweiz gehostet werden. Somit können US-Geheimdienste nicht auf die Daten der Nutzerinnen und Nutzer auf Grundlage des US-Patriot-Acts zugreifen. Eine allgemeine Empfehlung kann an dieser Stelle nicht ausgesprochen werden, da die Präferenzen und das zu erreichende Schutzniveau am Ende des Tages den Userinnen und Usern obliegt. Die tabellarische Gegenüberstellung in Kombination mit der Gliederung in die verschiedenen Domänen unterstützen jedoch die Entscheidungsfindung.

Neben der Bewertung der einzelnen Messaging-Applikationen konnten im Zuge dieser Arbeit die rechtlichen Vereinbarungen zwischen der Europäischen Union und den Vereinigten Staaten, welche einen Transfer personenbezogener Daten legitimieren, ermittelt werden. Da die Abkommen Safe Harbor und Privacy Shield durch den Europäischen Gerichtshof für rechtswidrig erklärt wurden, mussten neue rechtliche Grundlagen beschlossen werden. Die Standardvertragsklauseln substituieren die damaligen Abkommen und sichern die Legitimität der Transfers personenbezogener Daten aus dem Europäischen Wirtschaftsraum. Gleichzeitig wird mit diesen SCCs sichergestellt, dass das Datenschutzniveau im Drittland gleichgesetzt mit dem der Europäischen Union ist. Da jedoch der US-Patriot-Act den Geheimdiensten weiterhin den Zugriff auf Daten, welche auf US-Servern gespeichert sind, erlaubt, bestehen Zweifel über die Konformität gegenüber den Datenschutzbestimmungen der Europäischen Union. Die neuen und durchaus strikteren Anforderungen, welche aus den Standardvertragsklausel hervorgehen, geben zumindest die richtige Richtung vor und es bleibt abzuwarten, ob dieser Trend seitens der Union weiterhin so fortgesetzt wird. Denn auch beim Datenschutz handelt es sich um einen stetig zu verbessernden Prozess, welcher einen Schritt voraus, jedoch im selben Zug zwei Schritte zurück gehen kann.

Literatur

[1] Amir Herzberg und Hemi Leibowitz, “Can Johnny finally encrypt?: Evaluating E2E-encryption in popular IM applications”, en, in *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*, Los Angeles California: ACM, Dez. 2016, S. 17–28, ISBN: 978-1-4503-4826-3. DOI: 10.1145/3046055.3046059. Adresse: https://dl.acm.org/doi/10.1145/3046055.3046059 (besucht am 20. 04. 2021).

[2] J Botha und C Van, “A Comparison of Chat Applications in Terms of Security and Privacy”, en, S. 8,

[3] Murat Demirciog, “Security Analysis of the Encrypted Mobile Communication Applications”, en, S. 5,

[4] Mujaj Aulon, *A Comparison of Secure Messaging Protocols and Implementations*, 2017.

[5] Hsiao-Ying Huang und Masooda Bashir, “Is privacy a human right? An empirical examination in a global context”, in *2015 13th Annual Conference on Privacy, Security and Trust (PST)*, Izmir, Turkey: IEEE, Juli 2015, S. 77–84, ISBN: 978-1-4673-7828-4. DOI: 10.1109/PST.2015.7232957. Adresse: http://ieeexplore.ieee.org/document/7232957/ (besucht am 06. 02. 2021).

[6] Samuel D. Warren und Louis D. Brandeis, *The Right To Privacy*. Adresse: https://www.stetson.edu/law/studyabroad/spain/media/Wk3.Stuart.Day1-1-THE-RIGHT-TO-PRIVACY-(excerpt).pdf.

[7] Rebecca H. Rutherfoord und James K. Rutherfoord, “Privacy and ethical concerns in internet security”, en, in *Proceedings of the 2010 ACM conference on Information technology education - SIGITE ’10*, Midland, Michigan, USA: ACM Press, 2010, S. 131, ISBN: 978-1-4503-0343-9. DOI: 10.1145/1867651.1867686. Adresse: http://portal.acm.org/citation.cfm?doid=1867651.1867686 (besucht am 06. 02. 2021).

[8] Alen F. Westin, *Social and Political Dimensions of Privacy*, 2003. Adresse: https://spssi.onlinelibrary.wiley.com/doi/full/10.1111/1540-4560.00072.

[9] Daniel J Solove, “Nothing to Hide: The False Tradeoff between Privacy and Security (Introduction)”, en, S. 30,

[10] Roba Abbas, Katina Michael und M G. Michael, *Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World*, 2014. Adresse: https://scholars.uow.edu.au/display/publication135839.

[11] Lewis P., “I was shocked it was so easy’:
meet the professor who says facial recognition can tell if you’re gay”, 2018. Adresse: https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis.

[12] M. Michael, K. Michael und C. Perakslis, *Ueberveillance, the Web of Things, and People: What is the culmination of all this surveillance?*, 2015. Adresse: https://www.researchgate.net/publication/275055698_Uberveillance_the_Web_of_Things_and_People_What_is_the_culmination_of_all_this_surveillance.

[13] Jospeh Migga Kizza, *Ethical and Social Issues in the Information Age*. Springer, 2007, ISBN: 978-1-84628-659-9.

[14] Martin Rost und Kirsten Bock, “Privacy By Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen”, de, *Datenschutz und Datensicherheit - DuD*, Jg. 35, Nr. 1, S. 30–35, Jan. 2011, ISSN: 1614-0702, 1862-2607. DOI: 10.1007/s11623-011-0009-y. Adresse: http://link.springer.com/10.1007/s11623-011-0009-y (besucht am 06. 02. 2021).

[15] Marie Caroline Oetzel und Tijana Gonja, “The online privacy paradox: A social representations perspective”, en, in *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems - CHI EA ’11*, Vancouver, BC, Canada: ACM Press, 2011, S. 2107, ISBN: 978-1-4503-0268-5. DOI: 10.1145/1979742.1979887. Adresse: http://portal.acm.org/citation.cfm?doid=1979742.1979887 (besucht am 06. 02. 2021).

[16] D.N. Jutla und P. Bodorik, “Sociotechnical Architecture for Online Privacy”, en, *IEEE Security and Privacy Magazine*, Jg. 3, Nr. 2, S. 29–39, März 2005, ISSN: 1540-7993. DOI: 10.1109/MSP.2005.50. Adresse: http://ieeexplore.ieee.org/document/1423958/ (besucht am 06. 02. 2021).

[17] Mark S. Ackerman, Lorrie Faith Cranor und Joseph Reagle, “Privacy in e-commerce: Examining user scenarios and privacy preferences”, en, in *Proceedings of the 1st ACM conference on Electronic commerce - EC ’99*, Denver, Colorado, United States: ACM Press, 1999, S. 1–8, ISBN: 978-1-58113-176-5. DOI: 10.1145/336992.336995. Adresse: http://portal.acm.org/citation.cfm?doid=336992.336995 (besucht am 17. 02. 2021).

[18] Eric C. Turner und Subhasish Dasgupta, “Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals”, en, *Information Systems Management*, Jg. 20, Nr. 1, S. 8–18, Jan. 2003, ISSN: 1058-0530, 1934-8703. DOI: 10.1201/1078/43203.20.1.20031201/40079.2. Adresse: http://www.tandfonline.com/doi/abs/10.1201/1078/43203.20.1.20031201/40079.2 (besucht am 17. 02. 2021).

[19] Ruogu Kang, Stephanie Brown und Sara Kiesler, “Why do people seek anonymity on the internet?: Informing policy and design”, en, S. 10,

[20] Gary T. Marx, “What’s in a Name? Some Reflections on the Sociology of Anonymity”, en, *The Information Society*, Jg. 15, Nr. 2, S. 99–112, Mai 1999, ISSN: 0197-2243, 1087-6537. DOI: 10.1080/019722499128565. Adresse: http://www.tandfonline.com/doi/abs/10.1080/019722499128565 (besucht am 17. 02. 2021).

[21] Andreas Pfitzmann und Marit Köhntopp, “Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology”, en, in *Designing Privacy Enhancing Technologies*, Gerhard Goos, Juris Hartmanis, Jan van Leeuwen und Hannes Federrath, Hrsg., Bd. 2009, Series Title: Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, S. 1–9, ISBN: 978-3-540-41724-8 978-3-540-44702-3. DOI: 10.1007/3-540-44702-4_1. Adresse: http://link.springer.com/10.1007/3-540-44702-4_1 (besucht am 18. 02. 2021).

[22] Michael S Bernstein, “4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community”, en, S. 9,

[23] Helen Nissenbaum, “The Meaning of Anonymity in an Information Age”, en, *The Information Society*, Jg. 15, Nr. 2, S. 141–144, Mai 1999, ISSN: 0197-2243, 1087-6537. DOI: 10.1080/019722499128592. Adresse: http://www.tandfonline.com/doi/abs/10.1080/019722499128592 (besucht am 19. 02. 2021).

[24] Robert Bodle, “The ethics of online anonymity or Zuckerberg vs. "moot

", en, *ACM SIGCAS Computers and Society*, Jg. 43, Nr. 1, S. 22–35, Mai 2013, ISSN: 0095-2737. DOI: 10.1145/2505414.2505417. Adresse: https://dl.acm.org/doi/10.1145/2505414.2505417 (besucht am 06. 02. 2021).

[25] Marcel Rosenbach und Hilmar Schmundt, "The War on Web Anonymity", 2011. Adresse: https://www.spiegel.de/international/spiegel/internet-evolution-the-war-on-web-anonymity-a-778138.html.

[26] Daegon Cho, "Real Name Verification Law on the Internet: A Poison or Cure for Privacy?", en, in *Economics of Information Security and Privacy III*, Bruce Schneier, Hrsg., New York, NY: Springer New York, 2013, S. 239–261, ISBN: 978-1-4614-1980-8 978-1-4614-1981-5. DOI: 10.1007/978-1-4614-1981-5_11. Adresse: http://link.springer.com/10.1007/978-1-4614-1981-5_11 (besucht am 19. 02. 2021).

[27] Rodrigo Ferrada Stoehrel und Simon Lindgren, "For the Lulz: Anonymous, Aesthetics and Affect", en, *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, Jg. 12, Nr. 1, S. 238–264, März 2014, ISSN: 1726-670X, 1726-670X. DOI: 10.31269/triplec.v12i1.503. Adresse: https://www.triple-c.at/index.php/tripleC/article/view/503 (besucht am 19. 02. 2021).

[28] Chris Smith, "Visualized: The terrifying amount of data Facebook Messenger collects compared to Signal, iMessage, and WhatsApp", Mai 2021. Adresse: https://bgr.com/2021/01/05/app-privacy-labels-facebook-messenger-vs-imessge-signal-whatsapp/.

[29] Threema, "The new EU General Data Protection Regulation", 2018. Adresse: https://threema.ch/en/blog/posts/new-gdpr.

[30] Orcas, "Der große Messenger-Vergleich", 2017. Adresse: https://www.orcas.de/whatsapp-facebook-skype-telegram-signal-threema-wire-viber-hangouts-icq-jabber-simsme-hoccer-yooyuu-discord-vergleich/.

[31] Tole Sutikno, Lina Handayani, Deris Stiawan, Munawar Agus Riyadi und Imam Much Ibnu Subroto, "WhatsApp, Viber and Telegram which is Best for Instant Messaging?", en, *International Journal of Electrical and Computer Engineering (IJECE)*, Jg. 6, Nr. 3, S. 909, Juni 2016, ISSN: 2088-8708, 2088-8708. DOI: 10.11591/ijece.v6i3.10271. Adresse: http://www.iaescore.com/journals/index.php/IJECE/article/view/443 (besucht am 08. 04. 2021).

[32] Viber, *Connect A Proxy To Viber*, 2021. Adresse: https://help.viber.com/en/article/connect-a-proxy-to-viber.

[33] Rakuten Viber, *Privacy-Policy-Update-Nov-2019.pdf*, 2019. Adresse: https://www.viber.com/app/uploads/Privacy-Policy-Update-Nov-2019.pdf.

[34] ——, *Viber Terms of Use*, 2018. Adresse: https://www.viber.com/app/uploads/Viber-Terms-of-Use-2018-PDF-version.pdf.

[35] ——, *Viber Richtlinie zu Technologien für Werbung, Cookies & Tracking*, 2021. Adresse: https://www.viber.com/de/terms/cookies-and-tracking/.

[36] ——, *GDPR Privacy Rights*, 2021. Adresse: https://www.viber.com/de/terms/gdpr-privacy-rights/.

[37] Nathalie Cohen-Sheffer, *Viber's Delete Messages Feature Hits 5 Billion Usage Milestone!*, 2017. Adresse: https://www.viber.com/en/blog/2017-09-25/vibers-delete-messages-feature/.

[38] Rakuten Viber, *Disappearing Messages for Extra Privacy*, 2020. Adresse: https://www.viber.com/en/blog/2020-06-23/disappearing-messages-for-extra-privacy/.

[39] ——, *Viber-encryption-overview.pdf*, 2021. Adresse: https://www.viber.com/app/uploads/viber-encryption-overview.pdf.

[40] Amir Herzberg und Hemi Leibowitz, "Can Johnny finally encrypt?: Evaluating E2E-encryption in popular IM applications", en, in *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*, Los Angeles California: ACM, Dez. 2016, S. 17–28, ISBN: 978-1-4503-4826-3. DOI: 10.1145/3046055.3046059. Adresse: https://dl.acm.org/doi/10.1145/3046055.3046059 (besucht am 22. 06. 2021).

[41] Christian Johansen, Aulon Mujaj, Hamed Arshad und Josef Noll, "The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications", en, *arXiv:1807.07952 [cs]*, Juli 2019, arXiv: 1807.07952. Adresse: http://arxiv.org/abs/1807.07952 (besucht am 20. 04. 2021).

[42] VK, "VK", 2021. Adresse: https://vk.com/.

[43] IQBAL Mansoor, "Telegram Revenue and Usage Statistics", 2021. Adresse: https://www.businessofapps.com/data/telegram-statistics/.

[44] Burak Kocuro, “DESIGNING SECURE MOBILE MESSAGING OVER THE INTERNET”, en, S. 94,

[45] T9gram, “Telegram proxy”, Adresse: https://t9gram.com/f/telegram-proxy/.

[46] Telegram, *Telegram API Documentation*, 2021. Adresse: https://core.telegram.org/api/end-to-end.

[47] Elham Vaziripour, Justin Wu, Reza Farahbakhsh, Kent Seamons, Mark O’Neill und Daniel Zappala, “A Survey of the Privacy Preferences and Practices of Iranian Users of Telegram”, en, S. 20,

[48] Wolfgang A. Halang und Rudolf Konakovsky, *Sicherheitsgerichtete Echtzeitsysteme*, de, 3., überarbeitete und erweiterte Auflage, Ser. VDI-Buch. Berlin: Springer Vieweg, 2018, OCLC: 1037939878, ISBN: 978-3-662-56368-7.

[49] Telegram, *Perfect Forward Secrecy*, 2021. Adresse: https://core.telegram.org/api/end-to-end/pfs.

[50] ——, *FAQ for the Technically Inclined*, 2021. Adresse: https://core.telegram.org/techfaq#man-in-the-middle-attacks.

[51] ——, *Channels*, 2021. Adresse: https://core.telegram.org/api/channel.

[52] James Nolan, “Die Messenger-App, die Politiker, Manager und Drogendealer lieben”, 2018. Adresse: https://www.vice.com/de/article/paq88n/die-messenger-app-die-politiker-manager-und-drogendealer-lieben.

[53] Psiphon, *Psiphon*, 2021. Adresse: https://www.psiphon3.com/de/index.html.

[54] Wickr Inc., *Product Feature: Wickr Open Access*, 2020. Adresse: https://wickr.com/product-feature-wickr-open-access/.

[55] ——, *Wickr Product Tiers*, 2021. Adresse: https://wickr.com/product-tiers/.

[56] ——, *Legal Process Guidelines*, 2021. Adresse: https://wickr.com/privacy/?legalprocess.

[57] H. Elena, *Wickr Screenshot Detection*, 2021. Adresse: https://support.wickr.com/hc/en-us/articles/360001710133-Wickr-Screenshot-Detection.

[58] Adam Shostack, Scott Stender und Jesse Burns, “Wickr Messaging Protocol -Technical Paper”, en, S. 15,

[59] Wickr Inc, *Wickr-Customer-Security-Promises-March-2020.pdf*, 2018. Adresse: https://wickr.com/wp-content/uploads/PDFs/misc/WickrCustomerSecurityPromisesJuly201 pdf.

[60] ——, *Security Verification*, 2021. Adresse: https://support.wickr.com/hc/en-us/articles/115005092548-Security-Verification.

[61] ——, *Contact Discovery, ID Policy and Anonymity*. Adresse: https://wickr.com/contact-discovery-id-policy-and-anonymity/.

[62] ——, *Wickr Me Privacy Policy*, 2021. Adresse: https://wickr.com/privacy/me/.

[63] Threema, *Press-Info_threema_de.pdf*, 2020. Adresse: https://threema.ch/press-files/1_press_info/Press-Info_Threema_DE.pdf.

[64] ——, *Threema Multi-Device: Ein technischer überblick*, März 2021. Adresse: https://threema.ch/de/blog/posts/md-architectural-overview-de#main.

[65] ——, *Datenschutzerklärung*, 2021. Adresse: https://threema.ch/de/privacy.

[66] ——, *Sicherheit und Datenschutz*, 2021. Adresse: https://threema.ch/de/security.

[67] Threema GmbH, *Messenger Vergleich - Funktionen*, 2021. Adresse: https://threema.ch/de/messenger-vergleich.

[68] Threema, *Cryptography Whitepaper*, 2021. Adresse: https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf.

[69] Paul Rosler, Christian Mainka und Jorg Schwenk, "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema", en, in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London: IEEE, Apr. 2018, S. 415–429, ISBN: 978-1-5386-4228-3. DOI: 10.1109/EuroSP.2018.00036. Adresse: https://ieeexplore.ieee.org/document/8406614/ (besucht am 17. 06. 2021).

[70] Burak Kocuro, "DESIGNING SECURE MOBILE MESSAGING OVER THE INTERNET", en, S. 94,

[71] Threema, *Threema Multi Device Support*, 2021. Adresse: https://threema.ch/de/faq/multideviceexpl.

[72] Paul Rosler, Christian Mainka und Jorg Schwenk, “More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema”, en, in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London: IEEE, Apr. 2018, S. 415–429, ISBN: 978-1-5386-4228-3. DOI: 10.1109/EuroSP.2018.00036. Adresse: https://ieeexplore.ieee.org/document/8406614/ (besucht am 16. 06. 2021).

[73] Business of Apps, *Signal Revenue & Usage Statistics (2021)*, 2021. Adresse: https://www.businessofapps.com/data/signal-statistics/.

[74] jlund Signal, *Help users in Iran reconnect to Signal*, 2021. Adresse: https://signal.org/blog/help-iran-reconnect/.

[75] Signal, *Proxy Unterstützung*, 2021. Adresse: https://support.signal.org/hc/de/articles/360056052052-Proxy-Unterst%C3%BCtzung.

[76] ——, *Privacy Policy*, 2021. Adresse: https://signal.org/legal/#terms-of-service.

[77] ——, *Signal und die Datenschutz-Grundverordnung (DSGVO)*, 2021. Adresse: https://support.signal.org/hc/de/articles/360007059412-Signal-und-die-Datenschutz-Grundverordnung-DSGVO-.

[78] ——, *Signal Terms of Service*, 2021. Adresse: https://signal.org/legal/#terms-of-service.

[79] Support Signal, *Für jeden löschen*, 2021. Adresse: https://support.signal.org/hc/de/articles/360050426432-F%C3%BCr-jeden-l%C3%B6schen.

[80] ——, *Verschwindende Nachrichten festlegen und verwalten*, 2021. Adresse: https://support.signal.org/hc/de/articles/360007320771-Verschwindende-Nachrichten-festlegen-und-verwalten.

[81] Marius Wagner, “Das Signal-Protokoll”, de, S. 7,

[82] Support Signal, *Gekoppelte Geräte*, 2021. Adresse: https://support.signal.org/hc/de/articles/360007320551-Gekoppelte-Ger%C3%A4te.

[83] moxie0 Signal, *Private contact discovery for Signal*, 2017. Adresse: https://signal.org/blog/private-contact-discovery/.

[84] Statista, *Most popular global mobile messenger apps as of January 2021, based on number of monthly active users*, 2021. Adresse: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

[85] Whatsapp LLC, *Whatsapp Support & FAQ*, 2021. Adresse: https://faq.whatsapp.com/.

[86] Whatsapp Ireland Limited, *WhatsApp Datenschutzrichtlinie*, 2021. Adresse: https://www.whatsapp.com/legal/privacy-policy-eea#5pjKcdLXTVnRjhMZ7.

[87] Amtsblatt der Europäischen Union, *DURCHFÜHRUNGSBESCHLUSS (EU) 2021/914 DER KOMMISSION vom 4. Juni 2021über Standardvertragsklauseln für die übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates*, 2021. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

[88] Whatsapp LLC, *WhatsApp Encryption Overview*, 2020. Adresse: https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=A7oP_9hIoZIAX9-OKRK&_nc_ht=scontent.whatsapp.net&oh=cb0dbf5c36d62730a0886f9a8547b45a&oe=60E2C7D9.

[89] Lijun Zhang, Qingbing Ji und Fei Yu, "The Security Analysis of Popular Instant Messaging Applications", en, in *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, Dalian: IEEE, Dez. 2017, S. 1324–1328, ISBN: 978-1-5386-3573-5. DOI: 10.1109/ICCSEC.2017.8446863. Adresse: https://ieeexplore.ieee.org/document/8446863/ (besucht am 01. 07. 2021).

[90] Whatsapp LLC, *How to use Android fingerprint lock*, 2021. Adresse: https://faq.whatsapp.com/android/security-and-privacy/how-to-use-android-fingerprint-lock/.

[91] Org Datenschutz, *Datenschutz in den USA: Wo steht er im Vergleich zu Europa?*, 2021. Adresse: https://www.datenschutz.org/usa/.

[92] Varonis Varonis, *Complete Guide to Privacy Laws in the US*, 2021. Adresse: https://www.varonis.com/blog/us-privacy-laws/.

[93] Org Datenschutz, *Safe Harbor: Ein sicherer Hafen für europäische Daten?*, 2021. Adresse: https://www.datenschutz.org/safe-harbor/.

[94] Martin A Weiss und Kristin Archick, "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield", en, S. 19,

[95] , *EU-US Privacy Shield: Schutzschild für europäische Daten?*, https://www.datenschutz.org/privacy-shield/, 2021. Adresse: https://www.datenschutz.org/privacy-shield/.

[96] ——, *C-311/18 - Facebook Ireland und Schrems*, 2020. Adresse: https://curia.europa.eu/juris/document/document.jsf;jsessionid=A5D9AC4D64856080E4B33E43D668B3B2?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=2399197.

[97] Lutz Gleis, *Neue EU Standardvertragsklauseln für Datenübermittlungen in Drittstaaten – Was sie bringen und was jetzt zu tun ist.pdf*, 2021. Adresse: https://www.gleisslutz.com/de/node/20854/pdf.

[98] Dr. Hauke Hansen, *Neue Standardvertragsklauseln für internationalen Datentransfer und für Auftragsverarbeitungsverträge*, 2021. Adresse: https://blog.fps-law.de/datenschutz/neue-standardvertragsklauseln-fuer-internationalen-datentransfer-fuer-auftragsverarbeitungsvertraege/.

[99] EU-Kommission EU-Kommission, *Adequacy decisions*, 2021. Adresse: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[100] Thomas Schwenke, *Keine Angst vor US-Datentransfers ohne Privacy Shield – Muster, Ratschläge und Checkliste für Standardvertragsklauseln*, 2021. Adresse: https://datenschutz-generator.de/dsgvo-usa-muster-checkliste-scc/.