



POSITIONSPAPIER

OSB Alliance fordert: Der Staat muss auf drei Ebenen das Messenger-Dilemma beenden!

Hintergrund: Das Messenger-Dilemma

Die Nutzung von sogenannten Messengerdiensten nimmt stetig zu. Nach einer Statistik von Facebook aus dem Jahre 2017 nutzen 80% der 19 bis 64-jährigen Nutzer täglich Messenger Apps. Die große Akzeptanz ist nachvollziehbar. Messenger erlauben es gerade mit Mobilgeräten völlig unkompliziert Bilder, Videos und Textnachrichten mit anderen Nutzern auszutauschen. Sie ermöglichen teilweise sogar Video- und Sprachtelefonate. Geld muss man dafür meist nicht oder nur sehr wenig zahlen. Das ist verlockend und deshalb verwundert die [Untersuchung](#) [1] des Bitkom aus 2018 nicht, dass 9 von 10 Internetnutzern in Deutschland Messengerdienste nutzen.

81% von ihnen nutzen dabei WhatsApp. 46% den Facebook-Messenger, iMessage und Telegram sind abgeschlagen mit 10 bzw. 7 %. Das Dilemma an dieser Situation ist, dass die marktbeherrschende Stellung von WhatsApp sich selbst verstärkt, denn um möglichst viele zu erreichen und selber möglichst umfassend erreichbar zu sein treten immer mehr Nutzer dieser einen, siloartigen Lösung bei. Andere Lösungen haben kaum eine Chance, relevante Nutzeranteile zu gewinnen.

Das ist auch insoweit interessant, weil WhatsApp inzwischen zu Facebook gehört. Im Mai 2018 wurde [bekannt](#) [2], dass die Daten aus WhatsApp direkt an Facebook weitergereicht werden. Darüber hinaus wurde auch publik, dass Mark Zuckerberg Überlegungen anstellt, ein sogenanntes „Whatsabook“ zu schaffen durch die Zusammenlegung von Messenger-Profilen und -Daten aus WhatsApp, Facebook und Instagram, also sogar die Zusammenlegung von drei proprietären Datensilos zu einem.

Die marktbeherrschende Stellung von Facebook mit den zwei klassischen Text-Messengern sowie der Foto/Video-MicroBlogging-Plattform Instagram, die gleichfalls persönliche Daten sammelt, erfordert zwingend ein Einschreiten des Staates, um die digitale Souveränität der Mehrheit seiner Bürger*innen und Unternehmen sowie seiner selbst zu schützen und die Einhaltung des Datenschutzrechts durchzusetzen.

Die Open Source Business Alliance fordert das Handeln des Staates auf drei Ebenen.



POSITIONSPAPIER

Der Staat als Regulierer und Rechtsverfolger (Handlungsebene 1)

Das Vorgehen von Facebook wird von vielen Datenschützern als rechtswidrig angesehen, als Verstoß gegen die DSGVO und die ständige Rechtsprechung deutscher Gerichte. Ob die Aktionen von Facebook rechtswidrig sind oder nicht, werden wir vielleicht irgendwann durch das ein oder andere Urteil beleuchten können. Wahrscheinlich ist, dass es im Zweifel bis dahin diesen Datenfluss gibt. Auch der Bundesdatenschutzbeauftragte Ulrich Kelber hat jüngst WhatsApp für europarechtswidrig erklärt. Es geht hier aber für die Nutzer weniger um die Frage, ob das vielleicht gerade noch rechtlich zulässig ist. Viel mehr geht es darum, dass es nicht zuzulassen ist, dass auf diese Weise Daten abgeschöpft werden. Gibt es hier Lücken in der DSGVO, sind sie sofort zu schließen.

Rechtswidriger Datenmissbrauch muss gestoppt werden und Lücken in der DSGVO sind sofort zu schließen.

Der Staat als Förderer für sichere Lösungen (Handlungsebene 2)

Eigentlich sollte das Grund genug für Nutzer sein, WhatsApp den Rücken zu kehren und sich eines anderen Dienstes zu bedienen. Auch Zeitschriften geben Tipps zu alternativen Messengern. Aber ein Kernproblem ist, dass die Masse eben WhatsApp nutzt und man einen WhatsApp-Nutzer eben nicht mit einem anderen Messenger erreichen kann (und umgekehrt). Das System ist geschlossen, es gibt keine standardisierten Schnittstellen und Protokolle, der Code ist nicht veröffentlicht. Hiermit zementiert Facebook seine marktbeherrschende Stellung. Gäbe es solche proprietären Systeme in der Telefonie, könnte man wohl aus dem Telekom-Netz nicht in das Vodafone-Netz telefonieren oder mit einem Siemens-Endgerät kein Panasonic anrufen. Ginge es um Fotos, die auf einem Apple erstellt würden, könnte man die auf einem Windows-PC vielleicht nicht sehen. Das wäre ein unhaltbarer Zustand. Und bei über 50 Millionen deutschen Messenger-Usern ist es auch für Messenger-Dienste ein unhaltbarer Zustand. Der Staat muss deshalb die Aufstellung normativer Kriterien für einen diskriminierungsfreien Gebrauch eines Messengers fördern und die Beherrschung des Marktes durch ein einzelnes Unternehmen verhindern.



POSITIONSPAPIER

Die Problematik trifft natürlich auch Gesellschaft und Staat selbst, z.B. bei der Frage der WhatsApp-Nutzung in allen öffentlichen Bereichen wie Parlamenten, Behörden, Schulen und sonstige öffentlich geförderte Einrichtungen. In Teilen der Schweiz hat man sich z.B. grundsätzlich gegen WhatsApp [ausgesprochen](#) [3]. Der Staat hat bei der Beschaffung und der Nutzung durch eigene Institutionen auf die Kriterien eines „guten“ Messengers zu achten bzw. als Voraussetzung zu definieren.

Über alle Parteien hinweg kommen in der Politik zu Recht Forderungen auf, die Interoperabilität und eine mögliche Föderation (verschiedene Systeme kommunizieren aufgrund gemeinsamer Standards miteinander, bleiben aber vollständig autark) solcher Dienste sicherzustellen, notfalls durch einen noch zu definierenden Rechtsrahmen. In diesem Zusammenhang wird immer wieder auch auf die Verfügbarkeit europäischer oder auch deutscher Dienste verwiesen. Letzteres hilft als alleiniges Kriterium wenig weiter. Entscheidend ist, dass sich ein Dienst - auch überprüfbar - deutschen und europäischen Datenschutzbestimmungen unterwirft; es kann nicht per se darum gehen, nicht-europäische Anbieter auszuschließen bzw. europäische deshalb zu bevorzugen.

Es gibt bereits unternehmensübergreifende Ansätze für ein standardisiertes Protokoll, z.B. [Matrix](#) [4]. Auf Basis dieser Entwicklung will der [französische Staat](#) [5] flächendeckend seine Messenger-Kommunikation ausrichten und WhatsApp im öffentlichen Sektor vollständig abschaffen. Dabei fördert Frankreich nicht nur den Einsatz dieses Protokolls als Alternative zu WhatsApp, sondern unterstützt durch Implementierungsbeiträge und damit verbundene Investitionen eine Open Source Lösung, die dann jedermann zum Nutzen dient. Ein weiterer neuer Ansatz zur Entwicklung und Umsetzung ist das [Chat-over-IMAP Protokoll](#) [6]. „Chat-over-IMAP“ (CoI) kann theoretisch auf jedem IMAP-Server genutzt werden und wäre damit als "Erweiterung für E-Mail" für alle E-Mail-Nutzer verfügbar.

Welche technischen Eigenschaften einer solchen Umsetzung des offenen Standards sind es wert, durch den Staat gefördert zu werden? Die technischen Voraussetzungen für einen „guten“ Messenger sind überschaubar, können sich aber gegenüber der Marktmacht von Facebook-Messengern nicht durchsetzen.

Politik und Staat müssen der Beherrschung des "Messenger-Marktes" durch einen Anbieter entschlossen entgegenreten. Zudem müssen Messenger-Dienste durch offenen Quellcode überprüfbar sein und über offene Standards miteinander kommunizieren können, ohne ihre Autarkie dabei aufgeben zu müssen.



POSITIONSPAPIER

Im Kern geht es der OSB Alliance um folgende Voraussetzungen, die eine solche Lösung erfüllen muß:

Die Kommunikationslösungen müssen ...

... genau wie die dabei anfallenden Daten- und Metadatensammlungen dezentralisiert/lokal sein, um Unabhängigkeit zu garantieren.

... über normierte, offene Standards mit Alternativlösungen kommunizieren können (Föderation), sowie den Wechsel zwischen Messengerlösungen durch Benutzer*innen durch die Mitnahme der Profil und Kommunikationsdaten ermöglichen.

... in Bezug auf Implementierungen der Messengerfunktionalität sowie ihrer Schnittstellen und APIs im Source Code offen zugänglich sein und einer freien Lizenz unterliegen.

... die Möglichkeit zur Ende-zu-Ende Verschlüsselung der Kommunikationsdaten und verschlüsselter Ablage von Benutzerdaten bieten.

... Transparenz und Steuerungsmöglichkeit/Administrationsmöglichkeit durch Benutzer*innen im Hinblick auf Compliance Aspekte und Messenger-übergreifenden „Daten Grabblings“ (z.B. Zugriff auf Kontakte, Standortnutzung, Surfverhalten vom Browser, usw.) sicherstellen.

... der Maxime einer Datensparsamkeit folgen: keine (Daten-)Kommunikation oder Weitergabe an eine zentrale Auswertestelle.



POSITIONSPAPIER

... sollen über unterschiedlichste Plattformen hinweg (verschiedene Endgeräte, verschiedene Betriebssysteme, verschiedene Kommunikations-Provider) nutzbar sein und diesbezüglich Anwender*innen keinen Beschränkungen unterwerfen.

... müssen in Bezug auf die geforderten Eigenschaften analysier- und nach-vollziehbar durch Dritte sein.

... die Möglichkeit alternativer aber dennoch in der Kommunikation kompatibler Implementierungen eröffnen (kompatible Implementierung anhand von Standards, APIs und Beschreibung möglich).

Diese Entwicklungen sind sowohl im Sinne des offenen Standards als auch einer nutzbaren Referenzimplementierung mit diesen technischen Eigenschaften voranzubringen. Sie sind auch mit Fördermitteln zu unterstützen bis hin zur Produktreife. Das halten wir nicht nur für geboten, sondern für zwingend. Der Staat muss hier eingreifen, um das Markteintrittsrisiko gegen die übermächtigen Messenger von Facebook zu senken und die Entwicklung datenschutzkonformer Angebote zu beschleunigen.

Es geht auch nicht darum, WhatsApp „nachzubauen“, sondern Innovation anzureizen und neue Dienste zu entwickeln. Dazu ist die Definition eines offenen Standards als Norm für Messengerdienste vom Staat zu fördern und fordern. Unter dem Gesichtspunkt des Public Money - Public Code-Gedankens ist der in der freien Wirtschaft zu entwickelnde Code nach einer durch den Staat geförderten Referenzimplementierung unter einer Open Source Lizenz öffentlich zur Verfügung zu stellen.

Die Innovation von datenschutzkonformen Messenger muss durch Fördermittel vom Staat unterstützt und die entwickelten Codes gemäß dem Grundsatz Public Money - Public Code unter einer Open Source Lizenz öffentlich zu Verfügung gestellt werden.



POSITIONSPAPIER

Der Staat als Überwacher und Aufklärer (Handlungsebene 3)

Er hat darüber hinaus die Bürger aufzuklären, wie er sich gegen den Datenmißbrauch schützen kann. Eine Messenger-Zertifizierung halten wir dabei nicht nur für eine geeignete Kommunikationsoption an Nutzer, sondern auch für einen Garanten, angebotene Dienste auf ihre Konformität mit den Datenschutzvorschriften wie auch auf die Nutzung und Einhaltung der offenen Standards und ihrer Unabhängigkeit von anderen Diensten zu überprüfen. Kernvoraussetzung für die Prüfung ist Open Source und die Einhaltung des oben geforderten offenen Standards als Norm durch den Messengerdienst.

Es ist aus unserer Sicht sinnvoll, an die Etablierung entsprechender Prüforganisationen diversifiziert und dezentral heranzugehen. Dies erachten wir deshalb als erforderlich, weil der Nutzer die Wahl des Prüforgans seines Vertrauens haben sollte. Es bedarf hier voraussichtlich nicht einmal neuer Strukturen, da es hinreichend Prüforganisationen gibt, die das leisten können. Der Bedarf dieser zertifizierenden Prüforganisationen rechtfertigt sich auch durch andere Teilbereiche der aktuellen Digitalisierungsfortschritte in Staat und Gesellschaft (Stichwort KI und Algorithmen).

Das Fernmeldegeheimnis des Grundgesetzes und des TKG und dessen staatliche Überwachung muss endlich auch für Messenger in der Politik gedacht und durchgesetzt werden. Anderenfalls bleibt die DSGVO ein zahnloser Tiger und der Bürger bleibt monopolistischen Anbietern ausgeliefert, die den Datenschutz nach eigenen Interessen interpretieren.

**Datenschutzvorschriften müssen auch für Messenger-Dienste und deren Anbieter gelten und durchgesetzt werden.
Darüber hinaus sollte der Staat den Nutzer*innen im Wege der Zertifizierung datenschutzkonforme Messenger-Dienste aufzeigen.**



POSITIONSPAPIER

Unsere Forderungen im Überblick:

- Der Staat muss konsequent jeden Verstoß gegen die Datenschutzgrundverordnung durch Messenger-Dienste unterbinden.
- Er hat sofort jede Lücke im Datenschutz zu schließen, die zur Abschöpfung persönlicher Daten führt.
- Er hat sich dafür einzusetzen, dass dieser sensible Kommunikationsbereich durch Open Source überprüfbar wird und offene Standards zur Interoperabilität aller Dienste führen.
- Hierfür hat er durch ein Marktentwicklungsprogramm finanzielle Mittel zur Verfügung zu stellen, die die Entwicklung solcher Dienste und die offene Standardisierung vorantreiben (die Prinzipien von Public Money - Public Code sind einzuhalten).
- Er hat Bürger*innen darauf hinzuweisen, dass geschlossene Messenger-Dienste zu erheblichen Integritäts- und Souveränitätsverlusten führen können.
- Der Staat hat selbst diese Kriterien bei sich anzulegen (z.B. in Schulen oder Behörden und allen von ihm geförderten Einrichtungen).
- Hierzu fordern wir auch eine Messenger-Zertifizierung, die ausschließlich Tools zulässt, die sich offener Standards bedienen und aufgrund offener Codes durch ihn überprüfbar sind.



POSITIONSPAPIER

Autoren: Lothar K. Becker (.riess applications GmbH), Vorstand OSB Alliance
und Sprecher Working Group Public Affairs
RA Karl Krüger, Bereichsleiter Public Sector
März 2019

Linkliste: [1] <https://www.messengerpeople.com/de/whatsapp-nutzerzahlen-deutschland-2018/#Messenger>
[2] <https://www.techbook.de/easylife/whatsapp-daten-facebook-dsgvo>
[3] <https://www.inside-it.ch/articles/53634>
[4] <https://matrix.org/docs/spec/>
[5] <https://www.golem.de/news/statt-whatsapp-frankreich-wandert-in-die-matrix-1902-139167.html>
[6] <https://github.com/coi-dev/coi-specs>

Das Positionspapier kann unter den Lizenzbedingungen der Creative Commons Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 Deutschland (CC BY SA 4.0 International)“ wie folgt genutzt werden:

Herausgeber: © 2019 Open Source Business Alliance e.V.

Autoren: Dipl.-Inform. Lothar K. Becker, RA Karl Krüger

Titel: Positionspapier der OSBA: Beendigung des Messenger-Dilemmas

Lizenz: CC BY SA 4.0 International

(<https://creativecommons.org/licenses/by-sa/4.0/>)