Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 102 (2022)

Heft: 1093

Artikel: Der Kampf um die Datenhoheit auf dem Handy

Autor: Belser, Jannik

DOI: https://doi.org/10.5169/seals-1035428

Der Kampf um die Datenhoheit auf dem Handy

Messengerdienste wie WhatsApp verschlüsseln Nachrichten standardmässig. Doch wirklich geschützt sind private Daten erst, wenn der Anbieter seine Nutzer nicht kennt.

von Jannik Belser

Im Frühjahr 2020 ereignete sich Erstaunliches: In der ganzen Welt machten sich selbst technisch wenig bewanderte Nutzer plötzlich ernsthafte Sorgen um ihre Privatsphäre. Was war geschehen? Der beliebte Kurznachrichtendienst WhatsApp, der seit 2014 Facebook gehört, revidierte seine Nutzungsrichtlinien. Und obwohl sich kaum jemand die Lektüre der neuen Vorgaben zu Gemüte führte und sich erkundigte, was bei der App überhaupt anders werde, kehrten zahlreiche wütende Nutzer dem Messengerdienst den Rücken. Alternativen wie Telegram und Signal profitierten.

Deutlich mehr Nutzer verzeichnete auch der Schweizer Messengerdienst Threema: Vergangenes Jahr hat er erstmals die Grenze von zehn Millionen Downloads weltweit geknackt. «Eigentlich können wir Facebook dankbar sein: Sie trampeln von einem Fettnäpfchen ins nächste und bescheren uns so Zulauf», sagt CEO Martin Blatter.

Entstanden ist Threema am Küchentisch: Vor rund zehn Jahren entwickelt Blatter mit zwei Freunden eine App, die eine Alternative zu den gängigen Kurznachrichtenanbietern sein soll. Die drei Informatiker nennen sie anfänglich EEEMA – kurz für «End-to-End Encrypted Messaging Application». Mit dem Taufnamen verdeutlichen die Entwickler ihre Vision: Sie wollen eine Kommunikation ermöglichen, bei welcher die Nachrichten des Absenders nur vom Empfänger gelesen werden können – ohne Möglichkeiten zur Einsehbarkeit durch Dritte, auch nicht durch den Anbieter. In der Fachsprache nennt man diesen sicheren Kanal eine Ende-zu-Ende-Verschlüsselung. «2012 gab es so was eigentlich noch nicht», sagt Blatter.

Was Zuckerberg über Sie wissen will

2013 erhält die Debatte um den Schutz der privaten Kommunikation neue Dynamik: Edward Snowdens Enthüllungen zu den umfänglichen Überwachungstätigkeiten der amerikanischen Behörden sorgen dafür, dass immer mehr Nutzer auf Sicherheit vor Überwachung pochen. Zahlreiche Kurznachrichtenanbieter reagieren und satteln auf die Ende-zu-Ende-Verschlüsselung um. Auch WhatsApp erhält seit 2016 standardmässig keine Einsicht in den Inhalt Ihrer Privatnachrichten mehr – es sei denn, Sie speichern Ihre Chats mit einem Back-up auf der Cloud. Eine Ausnahme stellt bis heute der russische Anbieter Telegram dar, der letztes Jahr besonders unter Kritikern der Coronamassnahmen grossen Zulauf erhielt und paradoxerweise zu einem grossen Nutzniesser der neuen Nutzungsrichtlinien auf WhatsApp wurde: Hier muss die Verschlüsselung privater Konversationen optional aktiviert werden. In den beliebten Telegram-Gruppenchats ist die Kommunikation nach wie vor nur unverschlüsselt möglich.

Wenn selbst Facebook auf Ende-zu-Ende-Verschlüsselung setzt, darf man getrost bilanzieren: Kryptografie ist endgültig im Mainstream angekommen. Wo liegt also überhaupt Threemas Existenzberechtigung? Im Kern kann man diese Frage mit einem einzigen Wort beantworten: Metadaten. WhatsApp mag zwar die genauen Inhalte Ihrer Textnachrichten nicht mitlesen können. Das heisst aber noch lange nicht, dass WhatsApp mit Ihren Handlungen auf der App keine Aussagen über Sie tätigen kann. WhatsApp weiss zwar nicht, was Sie Ihren Bekanntschaften schreiben – WhatsApp weiss aber, wer Ihre Freunde sind und wie regelmässig Sie sich mit ihnen austauschen. Diese Kenntnis über Ihr Netzwerk lässt Rückschlüsse über Ihr Naturell zu: Wenn Ihr Cousin beispielsweise ein bekennender Anhänger der Fussballnationalmannschaft ist und Ihnen nach jedem Spiel eine minutenlange Sprachnachricht hinterlässt – wäre es dann nicht vielversprechend, Ihnen bei Facebook eine Werbung des neuen Nati-Trikots zu zeigen? Auf WhatsApp mögen Ihre Nachrichten noch so verschlüsselt und unlesbar sein – Ihre Daten tragen trotzdem zu Mark Zuckerbergs Reichtum bei. In den Metadaten liegt übrigens auch der Ursprung der letztjährigen Kontroverse um die Revision der Nutzungsrichtlinien von WhatsApp: Mit der neuen Datenschutzverordnung wollte WhatsApp die Weitergabe von Metadaten an private Unternehmen, allen voran an den Mutterkonzern Facebook, ausbauen. Die Option, die Datenweitergabe zu blockieren, wurde deaktiviert.

Threema geht mit den Metadaten deutlich sparsamer als seine Konkurrenz um: Das Schweizer Unternehmen erhebt keine Daten darüber, wie häufig Sie mit wem kommunizieren. Als einziger Anbieter lässt sich der Dienst zudem komplett anonym und ohne Hinterlegung einer Mobiltele-

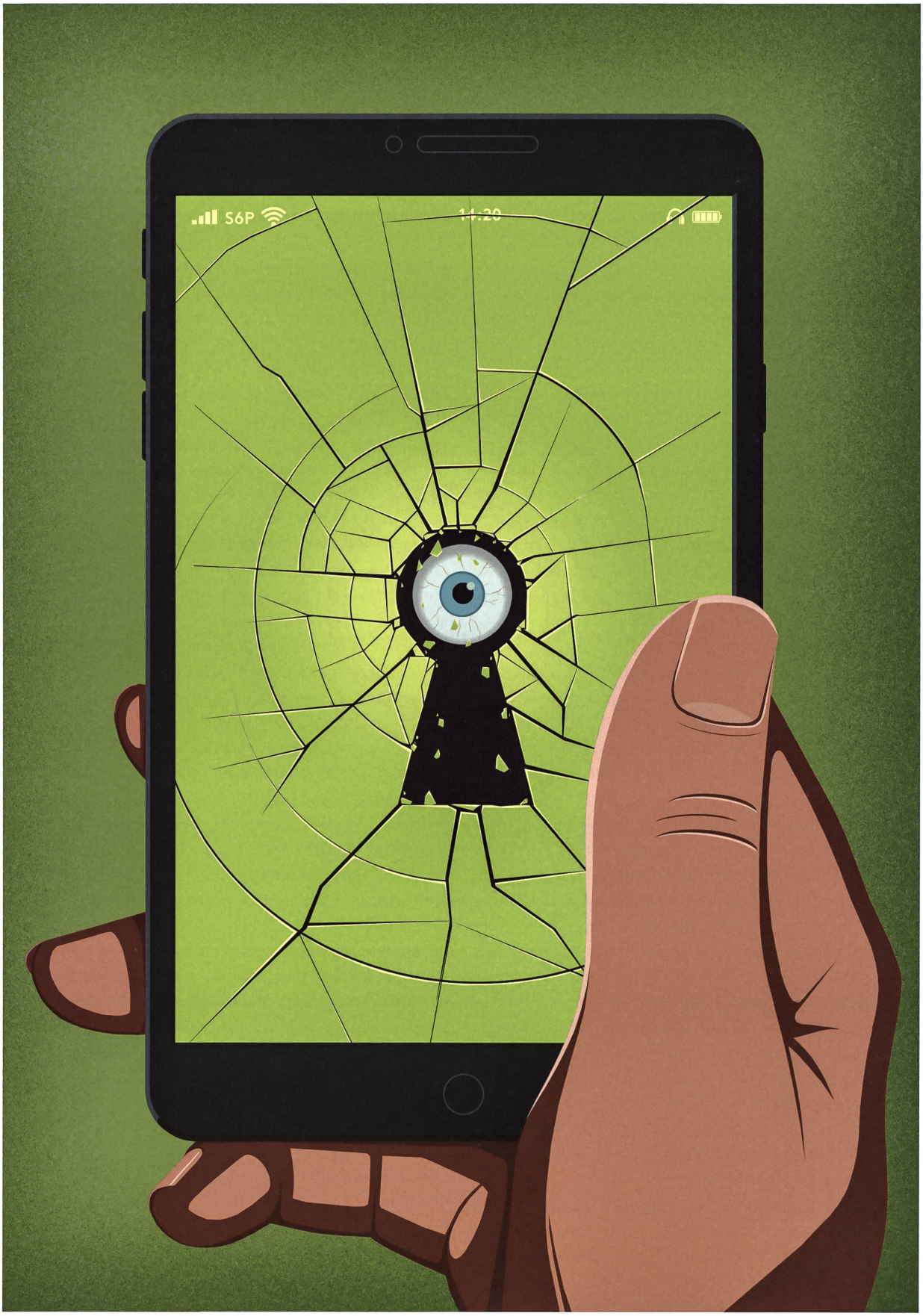

Illustration von Stephan Schmitz.

fonnummer nutzen. Diese sei in der modernen Welt beinahe schon zu einem Teil der eigenen Identität geworden, erzählt Blatter: «Überall, auch auf behördlichen Dokumenten, muss man mittlerweile seine Handynummer darlegen. In europäischen Staaten unterstehen SIM-Karten sogar einer Registrationspflicht, womit der Staat den Inhaber einer Telefonnummer sehr einfach ermitteln kann. Damit ist sie zu einem Primärschlüssel geworden, mit dem man eine Person ziemlich genau identifizieren und zahlreiche Daten aus verschiedenen Quellen zusammenführen kann.»

Wenn der Staat anklopft

Auch der Staat hat übrigens durchaus ein Interesse an einer Erhebung der Metadaten: Mittels einer Analyse der Kontaktfrequenz erhoffen sich Strafverfolgungsbehörden beispielsweise Hinweise auf Terrornetzwerke oder die Lieferketten von Drogendealern. Auch Threema wäre beinahe eine einschneidende Anpassung ihrer Datenpolitik aufgebrummt geworden: Kürzlich musste der Messengerdienst gegen das Eidgenössische Justiz- und Polizeidepartement (EJPD) vor Bundesgericht ziehen, weil dieses Threema zu einer Echtzeitüberwachung der Metadaten und einer Aufhebung der Transportverschlüsselung verpflichten wollte. Threema bekam im Mai 2021 Recht zugesprochen – das Unternehmen darf seine App weiterhin auf den maximalen Schutz der Privatsphäre ausrichten.

Gesetzlich ist Threema lediglich dazu verpflichtet, bei der Aufklärung von schweren Straftaten mit den Behörden zusammenzuarbeiten: Über den Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF) erreicht das Unternehmen in einem solchen Fall eine Anfrage zur Aushändigung aller vorhandenen Daten über eine ausgewählte Threema-ID, eine achtstellige Ziffernfolge, die dem Benutzernamen eines Users auf der Applikation gleichkommt. Der Staat erhält von Threema jedoch nur wenige Informationen, weil Threema selber gar nicht viel über seine Nutzer weiss: Zum einen lässt sich das Datum der Erstellung der Threema-ID sowie das letzte Log-in ermitteln. Bei einem Nutzer, der Threema anonym und ohne Verknüpfung verwendet, wäre das schon alles. Falls vorhanden, übergibt Threema den Behörden zum anderen die Handynummer oder E-Mail-Adresse des Nutzers – allerdings nur in verschlüsselter Form. Wirklich viel könne der Staat damit wohl nicht anfangen, mutmasst Blatter. Am ergiebigsten sei wahrscheinlich die letzte Auskunft: der sogenannte Push-Token, welcher der Aktivierung der Push-Benachrichtigungen des Betriebssystems dient. Mit dem anonymisierten Token kann der Staat die Identität des Nutzers zwar noch nicht erschliessen. Der Token kann allerdings die Basis für eine Anfrage beim Anbieter des Betriebssystems bilden – er ist gewissermassen ein Krümel, der gegebenenfalls zum Keks führt.

Blatter findet, dass Threema mit der einigermassen schlanken Rechtsbestimmung der Schweiz nicht allzu schlecht fahre. Als Negativbeispiel verweist er auf den Cloud Act in den USA, der Unternehmen einer Zugriffspflicht für Behörden unterstellt – selbst dann, wenn die Datenspeicherung nicht in den USA erfolgt. In einem geleakten Dokument schwärmte das amerikanische FBI jüngst, wie zügig und zuverlässig WhatsApp verfügbare Metadaten mit der Strafverfolgungsbehörde teile.

Ohne Privatsphäre keine Freiheit

Nichtsdestotrotz konstatiert Martin Blatter, dass die staatlichen Gelüste auf den Zugriff privater Daten in der jüngeren Vergangenheit auch in der Schweiz zugenommen hätten. Dies habe wohl primär damit zu tun, dass eine Datenabfrage den Behörden fast keinen Aufwand beschere: «Mit einer einfachen Ausgestaltung des Zugriffs auf persönliche Daten steigt auch die Versuchung. Plötzlich überwacht der Staat nicht nur potentielle Täter von Kapitalverbrechen, sondern auch den 18jährigen Grasdealer von nebenan», sagt Blatter. Er bezweifelt, dass Staaten mit mehr Daten Verbrechen wirklich erfolgreicher verhindern können: «Die jüngste Kampagne gegen Verschlüsselungsdienste wird sehr populistisch geführt. Kein Mensch hätte ernsthaft etwas gegen eine Bekämpfung von Kinderpornografie oder Terrorismus. Doch nur weil man den Heuhaufen grösser macht, heisst das nicht, dass man die Nadel auch findet – im Gegenteil. Bei zahlreichen Terroranschlägen in der jüngeren Vergangenheit waren die späteren Täter den Strafverfolgungsbehörden bereits bekannt.»

Blatter bereitet der Ausbau staatlicher Überwachung grosse Sorgen: «Mir graut vor einer Welt, in welcher das Vertrauen der Obrigkeit in den Bürger so gering ist, dass man ihn auf Schritt und Tritt überwacht. In einer Demokratie ist die Privatsphäre etwas, auf das man sich verlassen können muss.» Die Leute müssten sich allerdings bewusst sein, dass sie für den Schutz ihrer Privatsphäre auch etwas leisten müssten: Zahlreiche Nutzer hätten sich beispielsweise an den Zustand gewöhnt, dass man gelöschte Daten ganz bequem aus einer Cloud wiederherstellen könne. Dass man damit die Herrschaft über die eigenen Daten abgebe, sei vielen gar nicht bewusst. «Freiheit ist immer mit Eigenverantwortung verbunden», meint Blatter. ‹

Jannik Belser
ist Redaktor dieser Zeitschrift.