

Freie Messenger – Sichere Kommunikation

**Warum es sinnvoll ist, darüber
nachzudenken**

PETER
LÖBBECKE

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



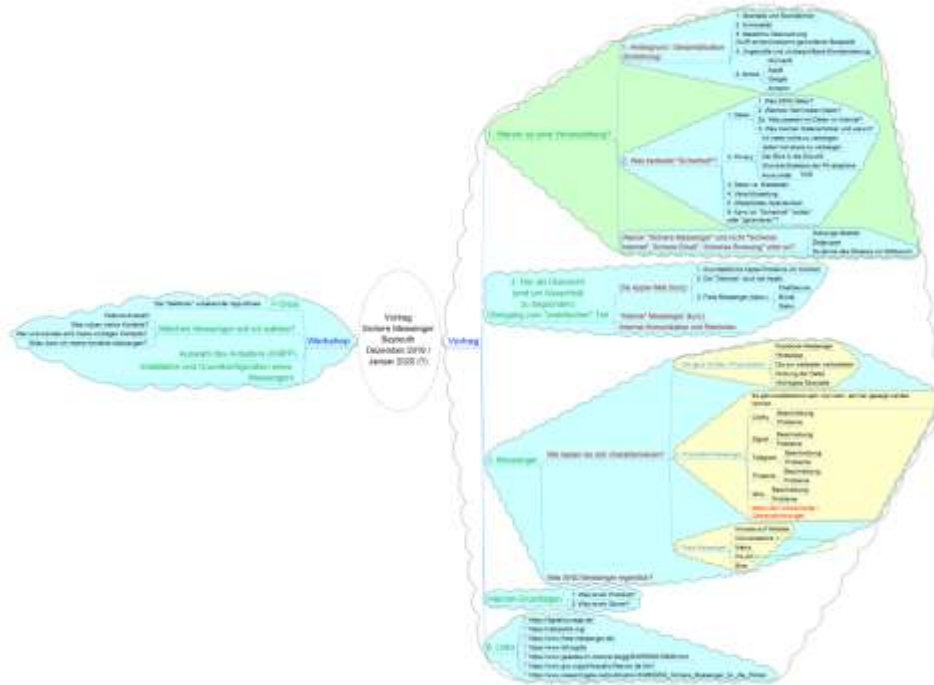
Ein wichtiger Hinweis:

Verwendete Logos, Namen etc.

**stehen entweder unter einer freien Lizenz
oder sind Eigentum der bezeichneten Firmen.**

**Ich beziehe außer meinem Gehalt
keine Zuwendungen von irgendwem!**

Was haben wir heute vor?



Was haben wir heute wirklich vor?

- ▶ Wozu so eine Veranstaltung?
 - ▶ Gesamtsituation / Hintergrund
 - ▶ Was bedeutet „Sicherheit“ in unserem Kontext?
- ▶ Messenger
 - ▶ „Proprietäre“ Messenger
 - ▶ Die ganz Großen
 - ▶ Die kleineren Großen
 - ▶ „Freie“ Messenger

F
R
A
G
E
N

u
n
d

W
O
R
K
S
H
O
P

Skandale, Skandälchen: Alle sind betroffen

- ▶ Sind Sie bei [Facebook](#)?
- ▶ Sind Sie bei WhatsApp? (dann sind Sie auch bei Facebook)
- ▶ Googlen Sie viel?
- ▶ Gehen Sie gern Einkaufen?
- ▶ Nutzen Sie gern Ihr Smartphone?

Skandale, Skandälchen: Alle sind betroffen

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

Skandale, Skandälchen: Alle sind betroffen

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

Skandale, Skandälchen: Alle sind betroffen

- ▶ Tracking ist allgegenwärtig
 - ▶ Firmen verfolgen uns durch's Internet
 - ▶ Gegenwärtige und zukünftige Nachteile
 - ▶ Wahl-/Politikbeeinflussung
- ▶ Der Staat verfolgt uns durch's Internet
 - ▶ Bewegungsprofile (Vorratsdatenspeicherung!)
 - ▶ Predictive Policing ...

Mani-
pula-
tion
??

Kon-
trol-
le
??

Skandale, Skandälchen: Die Politik

- ▶ Polizei- und andere Gesetze (SOG) werden mit Blick auf Privatsphäre aufgeweicht
- ▶ Videoüberwachung
- ▶ Vorratsdatenspeicherung
- ▶ Staatstrojaner
- ▶ Sicherheit oder Freiheit?

Skandale, Skandälchen: Kriminalität, Abzocke

- ▶ Phishing / Drive-by downloads / Schadsoftware allg.
- ▶ Internet-Abmahnungen
- ▶ Digitale Erpressung / Ransomware
- ▶ Dox(x)ing
- ▶ Der Kühlschrank schlägt zu
- ▶ . . .
- ▶ Statistik: [Anzahl](#) / [Schaden](#)

Was sind Daten?

- ▶ Daten sind Informationen in jeder Form:
 - ▶ Aussagen und Infos aller Art, über mich oder anderes
 - ▶ Bilder / Selfies / Videos / Musik / Playlisten
 - ▶ [Suchanfragen](#)
 - ▶ Was ich in der Cloud speichere
 - ▶ . . .



Was sind Daten?

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

Ausschnitt „[Nackt im Netz](#)“

Metadaten

- ▶ Das Experiment von Ton Siedsma:
 - ▶ 15.000 Datensätze innerhalb nur einer Woche
 - ▶ Ton Siedmas [Gerätenutzung](#)
 - ▶ So sieht ein [Tag](#) von Ton Siedsma aus
 - ▶ Tons [Freunde](#) und [Kollegen](#)

[Pentagon](#)

[White House](#)

[NPS, Florida](#)

[Bushwick,
Brooklyn](#)

Metadaten sind [tödlich!](#)

[Qasem](#)

Wen interessieren unsere Daten und Metadaten?

- ▶ Die Werbeindustrie: Targeted advertising
 - ▶ Die Politik: Wählerbeeinflussung
 - ▶ Den Staat: Überwachung
 - ▶ „Daten sind das Öl des 21. Jahrhunderts“
-
- ▶ „Daten sind das Wasser des 21. Jahrhunderts“

„Ich habe doch nichts zu verbergen“

WIRKLICH NICHT?

- ▶ Machen Sie die Klotür hinter sich zu?
- ▶ Stehen Sie doch zu Ihren Verbrechen! Oder?
- ▶ Wollen Sie erpressbar sein?
- ▶ Wollen Sie in der Zukunft leiden?
- ▶ Wollen Sie, dass jemand alles über Ihre Kinder weiß?

Das Problem mit der „Sicherheit“

- ▶ Es gibt keine absolute Sicherheit!
- ▶ Sicherheit ist ein Prozess!
- ▶ Sicherheit kann im Internet Verschiedenes bedeuten
- ▶ „Sicherheit“ vs. „Privacy“
- ▶ Verschlüsselung gibt nur teilweise „Sicherheit“
- ▶ Es gibt verschiedene **Schutzbedürfnisse** – sind Sie:

Einfacher
„Normalo“?

Politischer
Dissident?

Elternteil?

Wissenschaftler?

Ingenieur/Erfinder?

...

Warum also „Sichere Messenger“ ...

- ▶ ... und nicht „*Sicheres Internet*“, „*Sichere Email*“, „*Sicheres Browsing*“ ..?
 - ▶ Emails gewinnen zwar immer noch hinzu ...
 - ▶ ... aber die Reaktion auf Nachrichten ist eindeutig ...
 - ▶ ... und Messengernutzung hat sie im Alltag schon überholt
 - ▶ SMS werden immer mehr abgelöst

Hurra – die Überleitung zum „praktischen“ Teil!

- ▶ Privatsphäre und Berufsleben überlappen sich zunehmend
 - ▶ Home Office
 - ▶ Der öffentliche Dienst tut sich ganz schwer mit der neuen Technologie:
 - ▶ Beispiel Polizei: Verbote, geschlossene und eigene Entwicklungen
- ▶ Die Apple-Welt
 - ▶ Strukturen sind dieselben
 - ▶ Apples eigene Probleme – und die Lösungen im Kontext

Und jetzt endlich:

Instant Messaging

Was sind „Sichere“ Messenger?

- ▶ Individuelle **Schutzziele** beachten / eigene Risikoanalyse erstellen!
- ▶ Standardmerkmale:
 - ▶ Quelloffenheit
 - ▶ Vermeidung von Metadaten
 - ▶ Dezentralisierung
 - ▶ Mobile Endsysteme
 - ▶ Alternative Bezugsquellen
 - ▶ Alternativer Identifier
- ▶ Kryptografie:
 - ▶ Ende-zu-Ende-Verschlüsselung
 - ▶ Verbindlichkeit
 - ▶ Abstreitbarkeit
 - ▶ Folgenlosigkeit bzw.
 - ▶ Perfect Forward Secrecy

Zwei Kategorien von Messengern

- ▶ **„Proprietäre“** Messenger
 - ▶ Bilden eine „Marke“, sind „unfrei“
 - ▶ Brauchen daher das Vertrauen der NutzerInnen
 - ▶ Können nur untereinander kommunizieren (eigenes „*Protokoll*“, abgeschlossene „Server“, „Zentralisierung“)

- ▶ **„Freie“** Messenger
 - ▶ Sind quelloffen
 - ▶ Unterliegen auch sonst keinen Beschränkungen
 - ▶ Können auch mit anderen kommunizieren („öffentliches“/„freies“ *Protokoll*, „Föderation“)

Proprietäre Messenger: Die ganz Großen

► WhatsApp

Jede/r ist bei
WhatsApp!!!



► Facebook-Messenger



WhatsApp

- ▶ [Beliebtester](#) Messenger weltweit
- ▶ Baut ursprünglich auf dem (freien) XMPP auf
- ▶ Teil der Facebook-Gruppe (USA; seit 2014)
- ▶ Abgeschottetes Inselsystem
- ▶ Finanzierung durch Handel mit Nutzerdaten und
- ▶ Eigene [Auswertung](#) von Nutzerdaten, auch mit Dritten
- ▶ Keine Kontrolle der Funktionalität durch Nutzer möglich
- ▶ Mindestalter 16 Jahre

WhatsApp-Merkmale

- ▶ Ende-zu-Ende-Verschlüsselung automatisch
- ▶ Ein und dieselbe App bei allen Partnern erforderlich
- ▶ Nur ein Konto möglich
- ▶ Zentrale Infrastruktur
- ▶ Telefonie / Videotelefonie, Voice-Messages möglich
- ▶ Stickers, GIFs, Emojis, ...
- ▶ Chatgruppen möglich
- ▶ Kostenlose Nutzung

WhatsApp-Issues

- ▶ Telefonnummer als Identifier – Klarnamenpflicht
- ▶ Lädt [Adressbuch](#) zur [Mutterfirma](#) hoch
- ▶ Legale WhatsApp-Nutzung in EU nicht möglich; Datenschützer der Länder warnen ausdrücklich vor WhatsApp
- ▶ Sicherheit der Ende-zu-Ende Verschlüsselung nur zum Teil gegeben
- ▶ WhatsApp-Nutzer können von außen [nachverfolgt werden](#)
- ▶ Dokumente und Nachrichten werden ungeschützt gespeichert
- ▶ Serverstandort: USA

Facebook-Messenger

- ▶ Zweit-beliebtester Messenger
- ▶ Integriert in Facebook (USA), an Account gebunden
- ▶ Eigenes, geschlossenes Protokoll
- ▶ Abgeschottetes Protokoll
- ▶ Finanzierung durch die Mutterfirma (lebt vom Handel mit Nutzerdaten)
- ▶ Keine Kontrolle der Funktionalität durch Nutzer möglich

Facebook-Messenger-Merkmale

- ▶ Nutzung ist kostenlos
- ▶ Kein Mindestalter, aber Mindestalter für Facebook: 13 Jahre
- ▶ Keine Ende-zu-Ende-Verschlüsselung – Facebook kann Nachrichten lesen und speichert sie im Klartext
- ▶ Stickers, GIFs, Emojis,
- ▶ Bilder und Videos übermitteln
- ▶ Chatgruppen möglich
- ▶ Telefonate und Videotelefonate, Voice-Messages
- ▶ Spiele-Integration

Facebook-Messenger-Issues

- ▶ ... sind Facebook-Issues:
 - ▶ FB ist der zweitgrößte Datensammler im Netz
 - ▶ FB erstellt umfangreiche Profile von Nutzern und verbindet die in FB eingegebenen Daten mit „getrackten“ Daten
 - ▶ FB sammelt und speichert Metadaten und wertet sie aus
 - ▶ FB lädt das komplette Adressbuch von Nutzern hoch
 - ▶ FB gibt Daten an Behörden und andere Stellen weiter
 - ▶ FB wirbt im Namen von Nutzern ohne deren Wissen
 - ▶ FB gibt Firmen Zugriff auf Nutzerdaten

Proprietäre Messenger: Die größeren Kleinen

Signal



Chiffry



Threema



Telegram



Wire



Signal

- ▶ Produziert von der Firma Open Whisper Systems / USA
- ▶ Quelloffene Software (App und Server), offenes Protokoll
- ▶ Finanzierung durch Spenden, Zuwendungen, Stiftungen
- ▶ Kaum Sammlung von Kundendaten durch die Firma
- ▶ Sehr starkes, offenes Verschlüsselungsprotokoll
- ▶ Zentralisiert, „Walled Garden“

Signal-Merkmale

- ▶ Text-, Gruppen-, Sprach-, Video-, Dokument- und Bildnachrichten
- ▶ Sprach- und Videotelefonate
- ▶ Standardmäßige Ende-zu-Ende-Verschlüsselung
- ▶ Selbstzerstörende Nachrichten einstellbar
- ▶ Partner müssen nicht gleichzeitig online sein
- ▶ Kostenfrei

Signal-Issues

- ▶ Minimale Kundendatensammlung
- ▶ Keine anonyme Anmeldung möglich, Identifizierbarkeit
- ▶ Serverstandort: USA
- ▶ Unter Umständen eingebundene Tracker
- ▶ Abhängigkeit vom Firmenserver

Telegram

- ▶ Russischer Messenger; Entwicklungsteam derzeit in Dubai
- ▶ Die App ist open source, der Server nicht
- ▶ Läuft auf vielen Plattformen
- ▶ Verschlüsselung muss manuell für jede Kommunikation eingeschaltet werden
- ▶ Finanzierung durch eine Person (Spende); zukünftig ggf. kostenpflichtige Zusatzfunktionen; daher für Nutzer kostenfrei
- ▶ Zentralisierter „Walled Garden“

Telegram-Merkmale

- ▶ Einzel- und Gruppenchats
- ▶ Synchronisation über Gerätegrenzen hinweg
- ▶ Dokumentenübermittlung
- ▶ Keine Größenbeschränkung
- ▶ Speicherung von Dokumenten in der Cloud
- ▶ Selbstzerstörende Nachrichten einstellbar

Telegram-Issues

- ▶ Sicherheitsniveau von Experten kritisch eingeschätzt
- ▶ Registrierung mit Telefonnummer
- ▶ Eingebundene Android-Tracker
- ▶ Keine Kontrolle darüber, was auf dem Server passiert;
Abhängigkeit vom Firmenserver

Threema

- ▶ Schweizer Entwicklung, Firmenstandort ist die Schweiz
- ▶ Vollständig Ende-zu-Ende-verschlüsselt
- ▶ Der Quellcode ist nicht öffentlich, wird aber auditiert
- ▶ Einmalige Kosten von 2,99 Euro
- ▶ Keine Sammlung von Kundendaten
- ▶ Zentralisierter „Walled Garden“

Threema-Merkmale

- ▶ Text- und Sprachnachrichten
- ▶ Teilen von Bildern, Videos, animierten GIFs, Standorten
- ▶ Sprachanrufe
- ▶ Umfragen und Abstimmungen
- ▶ Keine Telefonnummer erforderlich, anonyme Anmeldung möglich
- ▶ Verschiedene Stufen zur Kontakt-Verifizierung möglich
- ▶ Unterstützt Smartwatches

Threema-Issues

- ▶ Nicht open source
- ▶ Abhängigkeit vom Firmenserver
- ▶ Keine Testversion (bei Kosten)
- ▶ Relativ geringe Verbreitung
- ▶ Keine Tracker eingebaut
- ▶ Selbstzerstörende Nachrichten möglich

Wire

- ▶ Ursprünglicher Standort: Schweiz
- ▶ Kürzlich an US-Firma verkauft
- ▶ Für Privatanwender kostenfrei; Finanzierung über Firmenleistungen
- ▶ Offenes Protokoll
- ▶ Quelloffene Software
- ▶ Standardmäßig starke Ende-zu-Ende-Verschlüsselung
- ▶ Plattformübergreifende Synchronisation
- ▶ Unbekannte Verbreitung

Wire

- ▶ Text- und Bildnachrichten
- ▶ Sprach- und Videotelefonate
- ▶ Bildmedien können bearbeitet und markiert werden
- ▶ Bearbeiten von Nachrichten möglich
- ▶ Anmeldung über Telefonnummer *oder* (Trash-) Mailadresse möglich
- ▶ Daten können für alle Geräte gelöscht werden
- ▶ Selbstzerstörende Nachrichten möglich

Wire-Issues

- ▶ Zentralisiertes System, (noch) keine Föderation möglich
 - ▶ (jedoch self-hosting)
- ▶ Abhängigkeit vom Firmenserver
- ▶ Daten werden auf dem Firmenserver gespeichert
- ▶ Jurisdiktion derzeit unklar
- ▶ Keine Tracker eingebunden

Chiffry

- ▶ Entwickelt in Deutschland, Firmensitz in Teutschenthal
- ▶ Für Privatanwender kostenfrei; kostenpflichtige Version für Behörden und Firmen
- ▶ Programmcode und Verschlüsselungsprotokoll nicht offen
- ▶ Siegel “IT-Security made in Germany”
- ▶ Empfohlen vom LDSB LSA
- ▶ Registrierung mittels Telefonnummer **und** Geräteinformationen

Chiffry-Merkmale

- ▶ Verschlüsselter Chat und Gruppenchat mit bis zu 10 Mitgliedern
- ▶ Sprach- und Kurznachrichten
- ▶ Verschlüsselt und kostenlos telefonieren (Internet)
- ▶ Bilder, Videos, Kontakte, Standorte teilen

Chiffry-Issues

- ▶ Abhängigkeit vom Firmenserver einer kleinen Firma
- ▶ Der Nutzer muß der Firma in jeder Hinsicht vertrauen
- ▶ Google-Tracker eingebunden
- ▶ Alle Nutzer müssen dieselbe App nutzen

Freie Messenger: Die wichtigsten Protokolle



Slack



Email-Chat
/ChatSecure



Die wichtigsten (?) „Freien Messenger“ ...

- ▶ Windows / Linux:
 - ▶ Gajim / Dino
- ▶ iPhone / (Mac):
 - ▶ Monal / ChatSecure
- ▶ Android:
 - ▶ Conversations / Pix-Art / Quicksy

www.Freie-Messenger.de

Herzlichen Dank!!!