



LEUPHANA
UNIVERSITÄT LÜNEBURG

Ausarbeitung
Privacy Marketplace
IT-Trends

Semester: 4. Semester (SoSe 2021)
Major: Wirtschaftsinformatik
Prüfer: Dr. Barbian

Sascha Majewsky
Böcklerstr. 4
22119 Hamburg
Matrikelnr.: 3038957

Inhaltsverzeichnis

1. Einleitung	1
2. Einordnung und Beweggründe des Trends	1
3. Privatsphäre in Gegenüberstellung zu Sicherheit	2
4. Relevanz der Privatsphäre	3
5. Private Daten vor welchen Akteuren schützen?	3
6. Privatsphäre Features in Instant-Messenger	4
6.1. Ende-zu-Ende-Verschlüsselung.....	4
6.2. Selbstzerstörende Nachrichten	5
6.3. Steganographie	5
6.4. PGP	5
6.5. Off-The-Record (OTR)	5
7. Gegenüberstellung verschiedener Instant-Messenger	5
8. Fazit	6
9. Quellenverzeichnis	6
10. Eigenständigkeitserklärung	9

1. Einleitung

Privacy Marketplace ist ein Begriff, der vermutlich nur selten beim ersten Hören mit einem konkreten Sachverhalt in Verbindung gebracht werden kann. Doch dass Privatsphäre im Allgemeinen immer mehr in den Fokus des alltäglichen Lebens rückt, zeigt eine steigende mediale Berichterstattung. Im Januar dieses Jahres sorgten veränderte Datenschutzrichtlinien bei dem Nachrichtendienstleister WhatsApp für Diskussionen. Als Folge wechselten viele Benutzer zum Konkurrenz-Anbieter Signal, dessen Server auf Grund des Andrangs kurzzeitig für weitere Registrierungen überlastet waren (vgl. Schräer, 2021). Diese mediale Aufmerksamkeit und eine spürbar steigende Nachfrage nach Privatsphäre bleiben nicht unbemerkt. Es bildet sich vermehrt ein Marktangebot an Software, welches ganz gezielt Funktionen zum Schutz der Privatsphäre als Kerneigenschaft anbietet. Diese Angebote stellen den sogenannten Privacy Marketplace dar. Dabei zeigt sich, dass dieser Trend in den letzten Jahren in vielen Anwendungsarten von Software auftritt. Diese Ausarbeitung beschäftigt sich mit der Einordnung des Trends und einer allgemeinen Einführung zum Thema Privatsphäre. Diese Arbeit mündet in einer Gegenüberstellung, eingegrenzt auf Instant-Messenger mit Privacy-Features.

2. Einordnung und Beweggründe des Trends

Die Thematik der Privatsphäre im Zeitalter der Digitalisierung scheint von Jahr zu Jahr an Bedeutung zu gewinnen. Neben dem Effekt, dass Verbraucher vermehrt ein Interesse daran entwickeln, was mit ihren Daten geschieht, scheinen auch die Unternehmen diese Entwicklung als Chance zu begreifen, um mit Fokus auf Privatsphäre-Funktionen ihre Reputation und Vertrauen im Angesicht der Kunden aufzuwerten. Auch können Unternehmen die gestiegene Bedeutung der Privatsphäre in Software der letzten Jahre nutzen um, gegenüber langsamer agierenden Unternehmen am Markt, einen kompetitiven Vorteil zu erreichen. Da der Staat in der Regulation des Datenschutzes stetig voranschreitet, können solche Anbieter mit der Integration von Privatsphäre-Funktionen in ihre Software als Nebeneffekt der Erfüllung gesetzlicher Voraussetzungen ihre Kunden binden.

Das Unternehmen Gartner Inc. veröffentlichte 2020 einen ausführlichen Bericht über den Hype Cycle für Privacy verschiedener Domänen. Trotz des kostenpflichtigen Zugriffs auf das Dokument, welches mit knapp 2000 € meine finanziellen Kapazitäten überfordert, kann dem Inhaltsverzeichnis entnommen werden, dass der Bereich der Privatsphäre weiterhin als "on the Rise" eingestuft wird und sich damit noch vor dem Höhepunkt der überhöhten Erwartungen befindet (vgl. Gartner, 2020). Es ist daher anzunehmen, dass sich dieser Sektor noch weiter vergrößern und die Erwartungen sowie die Investitionen und der Fortschritt in diesem Bereich über die nächsten Jahre wachsen wird.

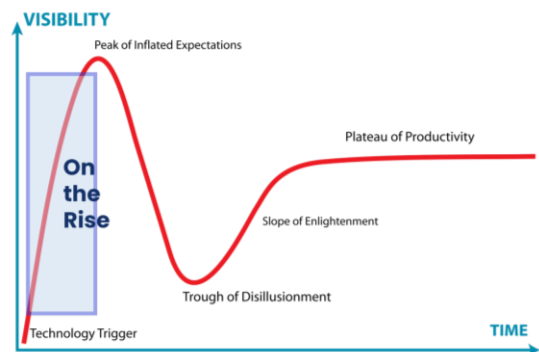


Abbildung 1: Hype Cycle (vgl. Kemp 2007)

Diese Einschätzung deckt sich mit dem über die letzten Jahre gemessenem Wachstum von Anbietern am Markt, welche Software mit Funktionalitäten der Privatsphäre zur Marktreife bringen. Seit mehreren Jahren lässt sich hier ein kontinuierliches Wachstum verzeichnen. So berichtet die International Association of Privacy Professionals (IAPP) in Ihrem Tech Vendor Privacy 2020 Report von knapp 300 verschiedenen Anbietern, welches einem Vorjahreswachstum von annähernd 30 % entspricht (vgl. International Association of Privacy Professionals, 2019a).

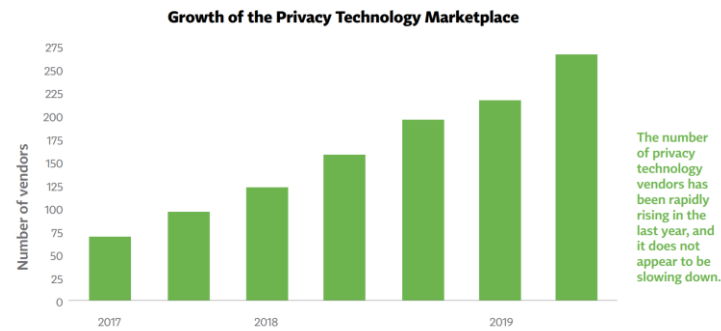


Abbildung 2: Growth of the Privacy Technology Marketplace (vgl. International Association of Privacy Professionals 2019b).

3. Privatsphäre in Gegenüberstellung zu Sicherheit

Um diese gestiegene Bedeutung an der Wichtigkeit von Privatsphäre zu verstehen, muss zunächst der Unterschied zwischen Sicherheit und Privatsphäre genauer beleuchtet werden. Diese beiden Thematiken werden fälschlicherweise oft als das Gleiche angesehen, da die Grenze zwischen der Datensicherheit und Datenprivatsphäre fließend ist. Am offensichtlichsten zeigt sich der Unterschied bei den Auswirkungen eines Verlustes dieser. Ist die Datensicherheit verloren gegangen, so sind beispielsweise sensible Passwörter und Zugänge in fremde Hände gelangt. Dies sollte allerdings nur von temporärer Natur sein, da ein Anbieter Zugangsdaten neu vergeben und somit die Sicherheit wiederherstellen kann. Bei einem Verlust an Daten im Bereich der Privatsphäre sind die Auswirkungen dazu diametral. Auch wenn ein Anbieter die Zugangsdaten dem rechtmäßigen Besitzer zurückgibt, bleiben die entwendeten persönlichen Daten, wie Geburtsdaten, Kontoverbindungen, E-Mail-Adressen oder intime Chatverläufe unumkehrbar für immer in freier Wildbahn.

Es lassen sich daher die Eigenschaften wie folgt differenzieren:

Tabelle 1: Vergleich der Haupteigenschaften von Sicherheit und Privatsphäre

Eigenschaften Sicherheit	Eigenschaften Privatsphäre
<ul style="list-style-type: none"> • Sicherheit schützt Daten jeglicher Art • Sicherheit ist nicht an Privatsphäre gebunden • Daten der Sicherheit sorgen für Vertraulichkeit • Daten der Sicherheit sorgen für Zugriff und sind erneuerbar 	<ul style="list-style-type: none"> • Privatsphäre schützt persönliche Daten • Privatsphäre kann ohne Sicherheit nicht existieren und ist ein Teil dessen • Daten der Privatsphäre erzeugen eine Nachverfolgbarkeit • Daten der Privatsphäre sind identifizierende Merkmale, viele fix für ein Leben lang

Folgende Tabelle gibt einen Überblick mit exemplarischen Szenarien der Abgrenzung zwischen einem Verlust der Privatsphäre und der Sicherheit:

Tabelle 2: Gegenüberstellung von Beispielen für einen Verlust von Privatsphäre oder Sicherheit

	Verletzte Privatsphäre	Keine verletzte Privatsphäre
Verletzte Sicherheit	Das Prüfungsamt der Leuphana wird gehackt und alle Namen und Noten der Prüfungsleistungen werden abgegriffen und öffentlich.	Das Prüfungsamt der Leuphana wird gehackt und nur das unveröffentlichte neue Curriculum des Folgejahres wird abgegriffen.
Keine verletzte Sicherheit	Die Leuphana veröffentlicht ungefragt die Namen, Alter und Studiengänge der Gewinner des alljährlichen Salzkristalls.	Du schickst deinem Freund eine Instant-Messenger Nachricht zur Einladung zu deinem Geburtstag.

4. Relevanz der Privatsphäre

Neben der Einordnung von Privatsphäre im Kontext der Sicherheit ergibt sich die bekannte Frage nach dessen Relevanz, "man habe doch nichts zu verbergen". Diese Gedankenhaltung scheint obsolet, betrachtet man, dass das Recht auf Privatsphäre fest in den demokratischen Grundsätzen verankert und durch die Allgemeine Erklärung der Menschenrechte gemäß Artikel 12, den europäischen Menschenrechtskonventionen gemäß Artikel 8 und den Europäischen Charta der Grundrechte in Artikel 7 für einen jeden definiert ist (vgl. European Data Protection Supervisor). Abseits der Rechtsprechung sorgt erst die Privatsphäre für eine freie Entfaltung der eigenen Persönlichkeit. Studien zeigen, dass Menschen eine Veränderung in ihrem Verhalten aufweisen, wenn sie wissen, dass sie überwacht werden (vgl. Kokolakis, 2017). Somit ist erkennbar, dass die Fähigkeit freie Entscheidungen zu treffen mindestens eingeschränkt und es kann angezweifelt werden, ob eine freie Meinungsbildung noch möglich ist.

Zudem ist hinzuzufügen, dass sich der öffentliche Raum der Realität und das Internet in seinen Eigenschaften stark unterscheiden. Bewegt sich der alltägliche Nutzer im Internet, befindet sich dieser nicht in einem geschützten Raum, sondern eher in einem Dschungel aus verschiedenen Marktplätzen und überwachten Plattformen, welche im Privatbesitz einzelner Individuen oder Unternehmen sind. Aufgrund der digitalen Natur ist es in diesem Umfeld besonders einfach durch Daten und Metadaten tiefergehende Informationen über einzelne Nutzer zu gewinnen, welches der Betroffene nicht mit sofortiger Wirkung spürt, sondern anschließend mit den vielfältigen Konsequenzen der Datenauswertung, wie durch personalisierte Werbung oder individuelle Preise, konfrontiert wird. Da im Internet das Umfeld und die Auswirkungen bei der Nutzung sich stark von der realen Öffentlichkeit abweichen ist es im Interesse eines jeden, dass die individuelle Privatsphäre auch im Internet gewahrt wird.

5. Private Daten vor welchen Akteuren schützen?

Neben der Bedeutsamkeit, persönliche Daten nur in einem nötigen Mindestmaß für die Betreiber verschiedener Internetangebote zur Verfügung stellen, gibt es auch weitere Akteure welche an den persönlichen Informationen interessiert sind und zu einem Verlust der Privatsphäre führen können.

Die lassen sich wie folgt zusammenfassend darstellen:

Tabelle 3: Zwei Akteure die an persönlichen Informationen interessiert sein können

Angreifer eines Internetangebotes	Staatliche Intervention
<ul style="list-style-type: none"> • Nutzen Schwachstellen aus, um an massenweise Daten von Nutzern zu gelangen • Verkaufen Daten in Hehlerei an den Meistbietenden weiter oder nutzen diese selber für kriminelle Machenschaften aus • Geschieht täglich, wird meist öffentlich 	<ul style="list-style-type: none"> • Nutzen durch internationale Spionage Schwachstellen aus, um gezielte Datengewinnung zu erreichen • Verpflichten Unternehmen durch die Gesetzgebung teilweise dazu Nutzerdaten freiwillig zu teilen, oftmals in Geheimhaltung • Geschieht permanent und geheim

Das Hackerangriffe tägliche Realität sind und auch weltführende Technologie-Konzerne die Privatsphäre ihrer Nutzer nicht ausreichend absichern können, zeigen historisch wiederkehrende und umfassende Datenlecks. Alleine im März diesen Jahres wurden Datensätze von über einer halben Milliarde Personen veröffentlicht. Diese umfassten E-Mail-Adressen, Anschriften, biografischen Informationen und Telefonnummern und wurden von der Plattform Facebook entwendet (vgl. Holmes, 2021). Ob auch die eigenen Daten bereits Teil solcher Datenlecks waren, kann auf der Internetseite <https://haveibeenpwned.com> überprüft werden, indem die eigene E-Mail oder Handynummer dort eingegeben und mit angegriffenen Datensätzen abgeglichen werden kann (vgl. Hunt).

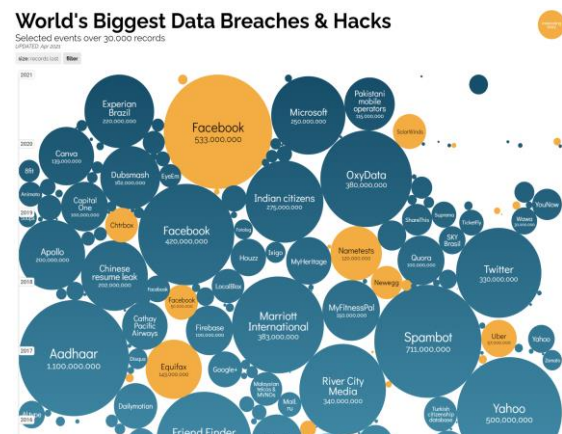


Abbildung 3: World's Biggest Data Breaches & Hacks (vgl. Information is beautiful, 2021)

Was jedoch nicht ohne weiteres geprüft werden kann, ist der eigene Schutz vor dem Ausspähen durch staatliche Akteure. So ist mindestens mit dem PRISM-Programm 2013 bekannt geworden, dass die Geheimdienste der USA fast alle digitale Kommunikation belauschen. Mit sogenannten Gagging Orders bringt sie Großkonzerne sogar gezielt dazu, die Daten freiwillig selber herauszugeben und gleichermaßen zu unterschreiben, dass niemals darüber gesprochen werden darf (vgl. Rossi, 2013). Auch in Deutschland finden offiziell einige Arten der Speicherung von Metadaten statt (vgl. Handelsblatt, 2015). Welche internationale Spionage auf unsere privaten Daten so stattfindet, lässt sich wohl nur erahnen.

6. Privatsphäre Features in Instant-Messenger

Heutzutage sind Implementationen für Privatsphäre-Features auch in dem meistgenutzten Instant-Messenger WhatsApp angekommen. Als guter Schritt in Richtung für mehr Privatsphäre der Milliarden Nutzer gestartet, sind auch diese nicht frei von jeglicher Kritik. So kritisieren Experten das weitere Speichern von Metadaten, keiner Quelloffenheit und andere Instant-Messenger bieten mit einer Vielzahl an alternativen Privatsphäre-Funktionen einen Mehrwert.

Die wichtigsten sollen hier kurz erläutert werden:

6.1. Ende-zu-Ende-Verschlüsselung

Die Ende-zu-Ende-Verschlüsselung sorgt dafür, dass Daten zwischen zwei Endpunkten abhörsicher und unveränderbar übertragen werden können. Dazu wird auf dem einem Gerät der Datensatz mit

einem kryptografischen Schlüssel verschlüsselt, dann in diesem Zustand übertragen und auf dem Endgerät erst wieder entschlüsselt. Somit ist eine Nachricht für den Transportweg gegen das Mitlesen oder das Verändern geschützt. Allerdings ist diese auch nur auf diesem Weg geschützt und nicht auf den Endpunkten der Geräte selbst. Auch fallen weiterhin alle Metadaten über Datum, Uhrzeit, Empfänger und Lesezeitpunkt der Nachricht an und es lassen sich Informationen ableiten.

6.2. Selbstzerstörende Nachrichten

Selbstzerstörende Nachrichten oder Konversationen liegen nur für einen vom Nutzer definierten Zeitraum vor. Damit sind diese vor späterer Auswertung geschützt. Allerdings könnte die Nachricht bereits initial belauscht oder festgehalten worden sein und stellt somit eine ergänzende Funktion dar.

6.3. Steganographie

Mittels Steganografie können Nachrichten geheim in Trägermedien, wie Bildern, versteckt versendet werden. Dabei muss ein Mitleser gezielt gewöhnliche Konversationen mit technischem Wissen über das Verfahren durchsuchen, um die Nachrichten zu entschlüsseln. Ist in Kombination mit selbstzerstörenden Nachrichten sinnvoll, um das Zeitfenster der Durchsuchung zu minimieren.

6.4. PGP

Durch PGP können Nachrichten mit festen Public-Private-Schlüsselpaaren verschlüsselt und entschlüsselt werden. Allerdings bieten die Schlüssel auch eine Art unbestreitbare Identifikation mit einer Nachricht und bei einem Verlust des geheimen Schlüssels kann ein Angreifer fortan alles Vergangene und Zukünftige mitlesen.

6.5. Off-The-Record (OTR)

OTR nutzt Ende-zu-Ende-Verschlüsselung für Nachrichten, um diese für den Transportweg abzusichern. Dabei gibt es keine Signaturen, wodurch eine Konversation stets glaubhaft abgestritten werden kann. Der Gesprächspartner muss authentifiziert werden und sämtlicher Datenverkehr wird nach dem Gespräch vernichtet. Daher sind beide Partner gezwungen zeitgleich online zu sein und die Klartext-Nachrichten müssen auf den Endgeräten weiterhin ausreichend geschützt werden.

7. Gegenüberstellung verschiedener Instant-Messenger

Tabelle 4: Gegenüberstellung Privacy-Feature verschiedener Instant-Messenger

	WhatsApp	Telegram	Threema	Signal	Wickr	Wire	Matrix	XMPP	Pixel-knot
E2E	Ja	Optional	Ja	Ja	Ja	Ja	Ja	Ja	Nein
Selbstzerstörung	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Nein
Stego	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja
PGP	Nein	Nein	Nein	Signal-	Nein	Nein	Ja	Ja	Nein

				Protocol					
OTR	Nein	Nein	Nein	Signal-Protocol	Nein	Nein	OMEMO-Protocol	Ja	Nein
Open-Source	Nein	Nein	Ja	Ja	Nein	Ja	Ja	Ja	Ja
Konzern	FANG	Global	Schweiz	Foundation	USA	USA	Community	Community	Community
Staatsnah	Kooperativ	Kooperativ	Ungewiss	USA-Finanzierung	Ungewiss	Ungewiss	Nein	Nein	Nein

8. Fazit

Privatsphäre ist ein im Grundgesetz verankertes Gut, welches jedem Menschen zusteht und für jeden Menschen von Bedeutung sein sollte. Gerade deshalb ist die Entwicklung des Trends Privacy-Marketplace mit seinem Mehrangebot für die Endverbraucher im Generellen zu begrüßen. Allerdings stellt sich die Frage inwiefern die Versprechen und Angebote in der Realität wirklich umgesetzt werden können und die Nutzer nicht in falscher Sicherheit wiegen. Gerade aufgrund der Natur der Sache, dass verlorene Privatsphäre nur selten wieder erlangt werden kann ist ein guter Schutz mit intrinsischer Motivation des anbietenden Unternehmens nötig. Die Realität zeigt, dass gerade aus regulatorischer Sicht Ländern zwar die Unternehmen verpflichten sich vermehrt um das Thema Privatsphäre zu kümmern, jedoch diese gleichermaßen befehlen Ihre Hintertüren der Daten für die staatlichen Akteure zu öffnen.

Betrachtet man die Gegenüberstellung der wichtigsten Instant-Messenger scheint es so, als würde Signal eines der besten Ergebnisse liefern. Es bietet viele gut umgesetzte Funktionen der Privatsphäre und ist leicht zugänglich. Allerdings wird auch hier ein Großteil der Finanzierung durch die US-Regierung gestellt, welche Fragwürdigkeiten bietet.

Nach Abwägung würde ich daher drei verschiedene Empfehlungs-Szenarien aussprechen:

- Signal für die unverfängliche Alltagskommunikation
- Matrix mit eigenem Server für sensible Kommunikation
- XMPP mit OTR auf Spezialhardware zur Besprechung von Geschäftsgeheimnissen

Es ist somit erkennbar, dass im Teilbereich des Instant-Messagings durchaus Möglichkeiten vorhanden sind proaktive Schritte zur Wahrung der eigenen Privatsphäre vorzunehmen. Allerdings befinden sich diese oftmals hinter einer Mauer aus benutzerfreundlichen technischen Hürden und enden meist dank mangelndem Netzwerkeffekt in einem leeren Kontaktbuch. Dies lässt einerseits ein dürftiges Résumé für den jungen Trend des Privacy Marketplaces ziehen, öffnet allerdings auch Türen für zukünftige Marktteilnehmer, um durch technische Innovation und regulatorische Spitzfindigkeit, Angebote für noch bessere Privatsphäre im Bereich des Instant-Messagings bereitstellen zu können.

9. Quellenverzeichnis

Literaturquellen:

Gartner. (2020, 23. Juli). *Hype Cycle for Privacy, 2020*. Gartner.

<https://www.gartner.com/en/documents/3987903/hype-cycle-for-privacy-2020>

International Association of Privacy Professionals. (2019a). *2019 Privacy Tech VENDOR REPORT*

(V.3.2). https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf

S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Computers & Security*, Volume 64, 2017, Pages 122-134, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2015.07.002>.

Internetquellen:

European Data Protection Supervisor. (o. D.). *Datenschutz*. Abgerufen am 19. Mai 2021, von

https://edps.europa.eu/data-protection/data-protection_de

Holmes, A. (2021, 3. April). *533 million Facebook users' phone numbers and personal data have been*

leaked online. Business Insider. <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T>

Handelsblatt. (2015, 30. Januar). *Überwachung in Deutschland: BND soll täglich Millionen Telefondaten*

speichern. <https://www.handelsblatt.com/politik/deutschland/ueberwachung-in-deutschland-bnd-soll-taeglich-millionen-telefondaten-speichern/11305682.html?ticket=ST-3050398-zOgVwejix94sEISKu33v-ap3>

Hunt, T. (o. D.). *'--have i been pwned? Haveibeenpwned*. Abgerufen am 19. Mai 2021, von <https://haveibeenpwned.com/>

Rossi, B. (2013, 12. Juni). *US tech giants demand end to PRISM gagging order*. Information Age.

<https://www.information-age.com/us-tech-giants-demand-end-to-prism-gagging-order-123457123/>

Schräer, F. (2021, 8. Januar). *Signal Messenger: Ansturm neuer Nutzer überlastet Signals Anmelde-*

system. heise online. <https://www.heise.de/news/Signal-Messenger-Ansturm-neuer-Nutzer-ueberlastet-Signals-Anmeldesystem-5018215.html>

Bildquellen:

Information is beautiful. (2021, April). *World's Biggest Data Breaches & Hacks* [Illustration]. information-isbeautiful. <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

International Association of Privacy Professionals. (2019b). *Growth of the Privacy Technology Marketplace* [Diagramm]. iapp. https://iapp.org/media/pdf/resource_center/2019Tech-VendorReport.pdf

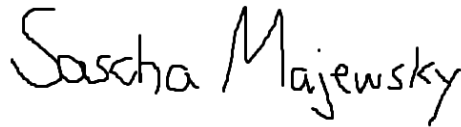
Kemp, J. (2007, 27. Dezember). *Hype cycle* [Diagramm]. wikipedia. https://en.wikipedia.org/wiki/Hype_cycle#/media/File:Gartner_Hype_Cycle.svg

10. Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Stellen der Arbeit, die wortwörtlich oder sinngemäß aus anderen Quellen übernommen wurden, habe ich als solche kenntlich gemacht. Die Arbeit habe ich in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt.

Matrikel Nr.: 3038957

Hamburg, den 22.05.2021

A handwritten signature in black ink that reads "Sascha Majewsky". The signature is written in a cursive style with a large 'M'.

Sascha Majewsky