Masterthesis

Hochschule für Technik, Wirtschaft und Kultur Leipzig
Fakultät Informatik, Mathematik und Naturwissenschaften
Studiengang Medieninformatik

Datenspuren im Netz und digitaler Selbstschutz

Von: Viola Elsenhans
Matrikelnummer: 64075
Eingereicht am: 28. Februar 2018
Gutachter: Prof. Dr. Michael Frank
Zweitgutachter: Prof. Dr. Klaus Hering

Eidesstattliche Erklärung

Ich versichere, dass die Masterarbeit mit dem Titel *Datenspuren im Netz und digitaler Selbstschutz* nicht anderweitig als Prüfungsleistung verwendet wurde und diese Masterarbeit noch nicht veröffentlicht worden ist. Die hier vorgelegte Masterarbeit habe ich selbstständig und ohne fremde Hilfe abgefasst. Ich habe keine anderen Quellen und Hilfsmittel als die angegebenen benutzt. Diesen Werken wörtlich oder sinngemäß entnommene Stellen habe ich als solche gekennzeichnet.

Leipzig, 28. Februar 2018 .....

Unterschrift

Kurzfassung

Gegenstand dieser Arbeit ist die Untersuchung von Methoden zur Erfassung von Nutzerdaten, welche bei der Nutzung des Internets über einen Personal Computer oder ein mobiles Gerät anfallen. In diesem Zusammenhang werden sowohl die grundlegenden rechtlichen Rahmenbedingungen als auch die Datenauswertung im Rahmen der Nutzerprofilierung betrachtet.
Der Schwerpunkt dieser Arbeit liegt in der Ausarbeitung geeigneter Maßnahmen, die zum Schutz der Privatsphäre des Nutzers im Internet beitragen können.

Abstract

This thesis is focused on technologies for collecting user-data, which accumulate by using the internet with a personal computer or a mobile device. In this context the basic legal requirements and the methods of data analysis for user profiling have been taken into consideration.
Main focus of the thesis is in elaboration of potential measures, which can improve the protection of privacy for internet user.

Inhaltsverzeichnis

1 Einführung

Die Nutzung des Internets ist in den vergangenen Jahren immer selbstverständlicher geworden und durchdringt nahezu jeden Bereich unseres Alltags. Fast jeder Lebensbereich des Menschen kann über informationsverarbeitende Systeme abgewickelt werden, die mit dem Internet in Verbindung stehen. Dabei bleiben meist Spuren in Form von Daten zurück, die gesammelt, mit der entsprechenden Person in Verbindung gebracht, ausgewertet und verkauft werden können. [Los15, Str11]
Durch Informationstechnologie und Software-Algorithmen, bei denen persönliche Daten ausgewertet werden, breitet sich sowohl das Social Sorting in Form einer Klassifikation und Sortierung der Bevölkerung, als auch das Risiko des Datenmissbrauchs aus. [Chr14, Sch14a]

Viele Nutzer sind sich weder ihrer Datenspuren bewusst, die bereits bei alltäglichen Tätigkeiten hinterlassen werden, noch der Gefahren, die diese Daten für die Privatsphäre darstellen, sodass oftmals ein nahezu sorgenfreier Umgang mit persönlichen Informationen die Folge ist. Andere Nutzer empfinden die Überwachungsmaßnahmen als nicht störend oder besorgniserregend, sie sagen: „*Ich habe nichts zu verbergen. Warum sollte sich jemand für mich und meine Daten interessieren?*“. Ihrer Meinung nach sei die Überwachung ausschließlich ein Instrument gegen Kriminalität und Terrorismus.
Allerdings werden Aktivitäten – auch immer mehr alltägliche Tätigkeiten – von jedem Internetnutzer weltweit durch Nachrichtendienste oder Internetkonzerne systematisch überwacht und ausgewertet. [Hei15]

Vernetzte Geräte sind allgegenwärtig und erfassen Daten aus allen Lebensbereichen ihrer Nutzer. Sie sind mit einer Vielzahl von Sensoren ausgestattet und vermessen damit den Körper, die Gesundheit, das Verhalten und die Umgebung des Nutzers. In Smartphones gehören Sensoren, wie GPS-Empfänger, Mikrofon, Kamera, Bewegungs-, Lage-, Licht-, Näherungs-, Magnetfeld- oder Fingerabdrucksensoren zum Standard. Fitness-Tracker, Smartwatches und andere Wearable Com-

puter vermessen neben Schrittanzahl, Puls oder Schlafverhalten, auch Atmung, Hautwiderstand, Blutdruck oder Blutzucker und verfügen zudem über Barometer, Temperatur- oder Luftfeuchtigkeitssensoren. Aber auch an das Internet angeschlossene Stromzähler, Thermostate, Brandmelder, Kühlschränke oder Badewannen liefern umfassende Daten über das Alltagsverhalten der Nutzer.
Diese Geräte erleichtern den Alltag ihrer Nutzer enorm und bieten ein hohes Maß an Komfort. Im Rahmen eines Smart Home kann man beispielsweise die Heizung über sein Smartphone steuern. Dazu genügt ein Befehl wie „*Alexa, Heizung auf 21 Grad einstellen*“. Das Zuhause hat so bereits bei der Ankunft des Bewohners die gewünschte Temperatur. Aufgrund der intelligenten Steuerung kann einerseits der Energieverbrauch reduziert, aber auch mögliche Einbrüche durch simulierte Anwesenheit anhand zeitabhängiger Licht- und Rollladensteuerung vorgebeugt werden. [MV16, Sch17c]
Die Geräte in einem Smart Home sind mit dem Internet verbunden, weshalb sie sich nicht mehr in einem abgeschlossenen System befinden. Dadurch besteht die Gefahr, dass Hacker die Kontrolle über das System übernehmen können. Davon abgesehen, gilt es auch den Aspekt des Datenschutzes zu berücksichtigen, denn auf die anfallenden Daten haben i.d.R. die Hersteller der Geräte bzw. die Anbieter der Dienstleistungen Zugriff. Beispielsweise hatte die Firma iRobot, ein Hersteller von Staubsauger-Robotern, erwogen, ihre Daten mit einem Drittunternehmen zu teilen. Die betroffenen Daten beinhalten Karten der gesamten Wohnungen, welche die Roboter abfahren, inklusive aller darin vorkommender Hindernisse. [Beu17]
Bezüglich des Sprachassistenten Amazon Alexa, der in Kombination mit einem Smart Home verwendet werden kann, warnte Andrea Voßhoff, Datenschutzbeauftragte der Bundesregierung, davor, dass nicht hinreichend transparent sei, welche Daten erfasst und zu welchen Zwecken diese verwendet würden. Die Mikrofone von Alexa sind dauerhaft bereit Befehle zu empfangen. Nachdem das Aktivierungswort *Alexa* ausgesprochen wird, werden Sprachbefehle und Fragen der Nutzer auf Server von Amazon übertragen. Neben den Sprachaufzeichnungen übertragen die Assistenten auch Informationen wie IP-Adressen, Daten zu Hard- und Software oder Such- und Shopping-Informationen. [HM17]

Auch beim Autofahren wird eine Vielzahl an Daten erfasst, z. B. anhand von Fahrassistenzsystemen, wie dem eCall-System (für emergency call). Dabei handelt es sich um ein automatisches Notrufsystem für Kraftfahrzeuge, die einen Verkehrsunfall automatisch an eine Notrufzentrale melden. Ab März 2018 müssen alle Neufahr-

zeuge in der EU dieses System unterstützen. Der europaweite Versichererverband Insurance Europe hat bereits Interesse an einem Zugriff auf die Daten des eCall-Systems durch Versicherungsunternehmen geäußert. Die Daten könnten dann für die Erstellung von Risikoprofilen oder für spezifische *Pay as You Drive*-Tarife verwendet werden. Aber auch Behörden könnten Interesse an den Daten haben, um z. B. aus der Kombination von Ort und Zeit zukünftig Falschparker zu ermitteln oder um über die Auswertung der Geschwindigkeit automatisiert festzustellen, wenn ein Tempolimit überschritten wird.
Allerdings werden die Fahrten durch Fahrassistenzsysteme auch sicherer und komfortabler. Aufgrund der schneller eingeleiteten Rettungsmaßnahmen beim eCall-System können Verletzungen früher behandelt und die Zahl der Verkehrstoten reduziert werden. [Mes14, Sis17]

Digitale Informationen entstehen auch bereits anhand technischer Daten, die allein für den Betrieb von Geräten und für den Aufbau von Verbindungen erforderlich sind. Sobald ein Rechner Zugang zum Internet hat, werden Informationen zur Identität bekannt gegeben. So kann jeder Mausklick, jeder Seitenaufruf, jede E-Mail und jede Internet-Bestellung einem einzelnen Gerät und einer Person zugeordnet und damit alle Online-Aktivitäten eines Menschen überwacht werden. [Sch14a]

Die gesammelten Daten werden verwendet, um Nutzerprofile zu erstellen und daraus persönliche Charaktereigenschaften abzuleiten. Ziel dabei ist, umfassende Kommunikations-, Verhaltens- und Bewegungsprofile von jedem Nutzer zu erstellen. Angestrebt wird die Datengewinnung *from anyone, anytime, anywhere*. [Fri15]

1.1 Motivation und Zielsetzung

Der Schutz der Privatsphäre ist ein internationales Menschenrecht, das auch und gerade im Zeitalter der globalen Kommunikation weltweit garantiert werden muss.
(Resolution „Das Recht auf Privatheit im digitalen Zeitalter“, [Sch14a], S.216)

Durch Edward Snowden wurden Teile der weltweiten Überwachungsmaßnahmen von Geheimdiensten öffentlich und Bedenken über den Datenschutz sind spätestens seit diesem Zeitpunkt berechtigt und belegbar. Durch die Veröffentlichungen wurde deutlich, dass der Mensch des Internetzeitalters im Tausch für mehr Komfort einen Großteil seines Lebens preis gibt und so Gefahr läuft, zum gläsernen Bürger zu werden.

Die Privatsphäre jedes Menschen leidet unter den Methoden der Internetkonzerne und Nachrichtendienste.
Daher werden in dieser Arbeit sowohl eingesetzte Überwachungsmethoden als auch Maßnahmen zum digitalen Selbstschutz untersucht. Der Fokus liegt dabei auf der Internet-Nutzung über einen Browser, aber auch die Verwendung wesentlicher Funktionen über ein Smartphone, wie die des Instant Messagings, wird berücksichtigt.
Das Ziel dieser Arbeit besteht darin, Handlungsempfehlungen zusammenzutragen, mit denen Nutzer sowohl ihre Privatsphäre als auch ihre Daten schützen können.

1.2 Aufbau der Arbeit

Zunächst werden in *Kapitel 2* wesentliche Rechtsgrundlagen in Deutschland, der Europäischen Union und den Vereinigten Staaten von Amerika betrachtet. Im Anschluss daran werden in *Kapitel 3* unterschiedliche Methoden untersucht, bei denen Nutzerdaten erfasst und einem Anwender zugeordnet werden können. Daraufhin folgen Betrachtungen zur Nutzerprofilierung in *Kapitel 4*, worin beispielhaft beschrieben wird, zu welchem Zweck die gesammelten Daten genutzt werden und welche Informationen aus ihnen entnommen werden können. Den Kern dieser Arbeit stellen die Maßnahmen zum Schutz der persönlichen Daten in *Kapitel 5* dar. Dabei werden Methoden und Handlungsempfehlungen genannt, die vor dem Zugriff auf Daten durch Dritte schützen können. Abschließend werden die Ergebnisse im *Fazit* zusammengefasst und Möglichkeiten der weiteren Entwicklungen im *Ausblick* betrachtet.

1.3 Abgrenzung

Im Rahmen dieser Arbeit werden nur solche Überwachungsmaßnahmen betrachtet, die bei der Nutzung des Internets über einen Personal Computer oder ein mobiles Endgerät zum Tragen kommen und die von staatlichen Einrichtungen und Internetkonzernen eingesetzt werden. Die Überwachung oder Manipulation durch Kriminelle wird nicht berücksichtigt, ebenso nicht der physische Zugriff auf die Geräte, beispielsweise durch Familienangehörige. Auch werden keine Schutzmaßnahmen untersucht, die bei einem Verlust von mobilen Geräten hilfreich sein können. Es werden

zudem keine Dienstleistungen betrachtet, bei denen Daten bewusst und freiwillig veröffentlicht oder zur Verfügung gestellt werden, etwa bei der Nutzung sozialer Netzwerke oder Smart Devices wie Amazon Echo oder Google Home im Haus.

Die Inhalte aus *Kapitel 5 Empfehlungen zum digitalen Selbstschutz* dienen lediglich dem Schutz der Privatsphäre, und sollen nicht dem Ziel dienen, kriminelle Aktivitäten im Internet zu verschleiern.

2 Rechtsgrundlagen

Die **Allgemeine Erklärung der Menschenrechte** (die Menschenrechtscharta) wurde von der Generalversammlung der Vereinten Nationen (zu denen inzwischen 193 Mitgliedsstaaten zählen) angenommen. Die Menschenrechtscharta ist eine Absichtserklärung, welche die darin enthaltenen Menschenrechte in möglichst allen Staaten durchsetzen und schützen will. Zwar ist an ihr keine rechtliche Verbindlichkeit für die Mitgliedsstaaten geknüpft, aber die Staaten haben sich auf diese Rechte als Grundlage für ihr Handeln verpflichtet. In Artikel 12 der Menschenrechtscharta heißt es: „*Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.*“ [Praa]
Das bedeutet, dass sich alle UN-Mitgliedsstaaten dazu verpflichtet haben, die Privatsphäre und den Schriftverkehr vor willkürlicher Überwachung zu schützen. Dazu gehört auch elektronische Kommunikation, wie Telefon und E-Mail. [Praa, Prac]

Statt der Menschenrechtscharta ist die Gesetzgebung des jeweiligen Landes, in dem sich das Unternehmen bzw. der Server befindet, rechtlich verbindlich. Dabei ist primär die Rechtsgebung des Landes ausschlaggebend, in dem sich der Unternehmenssitz bzw. die Niederlassung befindet, aber auch der Serverstandort ist für geltende Eingriffsrechte, wie Überwachungsmaßnahmen oder Anordnungen von Behörden zur Herausgabe von Daten, entscheidend. [Sch14a]

In der Europäischen Union gibt es bereits entsprechende Regelungen zum Datenschutz, die für alle EU-Mitgliedsstaaten verbindlich sind. Daher werden in den folgenden Kapiteln sowohl deutsche als auch europäische Regelungen exemplarisch betrachtet. Da viele große und beliebte Internet-Dienstleister aus den USA stammen und damit der US-amerikanischen Gesetzgebung unterliegen, wird auch auf wesentliche Aspekte dieser eingegangen.

2.1 Deutschland

Alle deutschen Nachrichtenagenturen sind an Rechte und Gesetzte gebunden, die auf das **Grundgesetz (GG)** zurückgehen. Das Grundrecht auf informationelle Selbstbestimmung definiert den „*Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten*“ und das Recht jedes Menschen, „*grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*“. [Pet17, Prab]
Zwar ist das Recht auf informationelle Selbstbestimmung im Grundgesetz nicht explizit geregelt, jedoch wurde es beim Volkszählungsurteil durch das Bundesverfassungsgericht als Spezialfall des Allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG, Art. 1 Abs. 1 GG) definiert. Solange „*nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz*“ verstoßen wird, sollte dieses Recht gelten. Zulässig sind Einschränkungen dann, wenn eine gesetzliche Grundlage vorhanden ist und ein überwiegendes Allgemeininteresse vorliegt. Solange also nicht gegen die Verfassung verstoßen wird, gewährleistet das Grundrecht auf informationelle Selbstbestimmung jedem Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. [Pet17, Prab]
In Artikel 10 Grundgesetz steht, dass das „*Briefgeheimnis sowie das Post- und Fernmeldegeheimnis [...] unverletzlich*“ sind. Das bedeutet, dass schriftliche Mitteilungen jeder Art grundsätzlich frei von Überwachung stattfinden sollen. Zum „*Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes*“ könne Artikel 10 auch eingeschränkt werden, ohne dass dies „*dem Betroffenen [...] mitgeteilt wird*“, der Kern des Grundgesetzes müsse jedoch gewahrt bleiben. Personen dürfen nur überwacht werden, wenn von ihnen verfassungsfeindliche Gefährdungen ausgehen. [Bun, Chr14]

Für eine Überwachung von Telefonaten und Internetverbindungen ist die Genehmigung der **G10-Kommission** erforderlich. Die G10-Kommission ist ein unabhängiges Gremium des Bundestags, das eingeschaltet wird, wenn der Geheimdienst in Artikel 10 des Grundgesetzes eingreifen will – daher auch die Bezeichnung G10. Bei dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (**G10-Gesetz**) wird zwischen der Überwachung einer bestimmten Person (Beschränkung im Einzelfall) und der strategischen Überwachung unterschieden. Bei der zuletzt genannten darf jegliche internationale Telekommunikation erfasst, gespeichert und ausgewertet werden. Zwar ist die inländische Kommunikation davon grundsätzlich

nicht betroffen, wird diese jedoch über ausländische Server geleitet (beispielsweise aufgrund eines ausländischen Anbieters), ist auch inländische Kommunikation Teil der strategischen Überwachung. Im Rahmen des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes wurde im Dezember 2016 die mengenmäßige Begrenzung der strategischen Telekommunikationsüberwachung aufgehoben. [Bun, Kau15, Sch14a]
Amnesty International Deutschland hat mit der Gesellschaft für Freiheitsrechte (GFF) im November 2016 gegen das G10-Gesetz vor dem Bundesverfassungsgericht Klage eingereicht. Dadurch soll primär aufgearbeitet werden, ob eine anlasslose Überwachung mit dem Grundgesetz vereinbar sei, da nach Andrea Berg, Amnesty International Deutschland, das Gesetz „*nicht mit dem universellen Recht auf Privatsphäre vereinbar*“ sei. [Wei16a]

Aufbauend auf dem Grundgesetz regelt das **Bundesdatenschutzgesetz (BDSG)** den Umgang mit personenbezogenen Daten. Nach §4 BDSG ist die „*Erhebung, Verarbeitung und Nutzung personenbezogener Daten [...] nur zulässig*“, wenn das BDSG „*oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat*“.
Zudem hat die verantwortliche Stelle dem Betroffenen nach §34 Abs. 1 BDSG auf Verlangen darüber Auskunft zu erteilen, welche Daten zu seiner Person gespeichert werden, an welche Empfänger oder Kategorien von Empfängern die Daten weitergegeben werden und zu welchem Zweck die Daten gespeichert werden.
§35 BDSG regelt die Berichtigung, Löschung und Sperrung von personenbezogenen Daten. So müssen Daten beispielsweise gelöscht werden, wenn ihre Richtigkeit nicht nachweisbar ist oder wenn sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind. Letzteres gilt jedoch nur, wenn der Löschung keine „*gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen*“. [Bun]

Das Telemediengesetz und das Telekommunikationsgesetz enthalten Regelungen, die verschiedene Teledienste betreffen. Das **Telemediengesetz (TMG)** ist für die Erbringung eines Informations- bzw. Kommunikationsdienstes über ein Telekommunikationsnetz relevant. Hier stehen die übertragenen Inhalte im Vordergrund, wie z. B. bei der Bereitstellung von Webspeicherplatz für fremde Inhalte oder der Veröffentlichung redaktioneller Beiträge. [Bun, For16]
Dagegen betrifft das **Telekommunikationsgesetz (TKG)** im Wesentlichen die Telekommunikationsinfrastruktur: das Leitungsnetz und die darüber erbrachten Dienstleistungen, sowie den technischen Vorgang des Sendens, Übermittelns und Empfangs

von Signalen. Dazu gehören z. B. die Vermittlung des Internetzugangs durch einen Provider oder die Bereitstellung eines E-Mail-Accounts. [For16]
Das TKG enthält Regelungen zum Fernmeldegeheimnis und spezifische Datenschutzregelungen. So dürfen beispielsweise Verkehrsdaten (also Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden) nach §96 im Wesentlichen lediglich für die Erbringung und die Abrechnung der Dienstleistung verwendet werden. Sobald die Daten nicht mehr erforderlich sind, hat nach Verbindungsende deren Löschung zu erfolgen.
In §98 TKG wird die Verwendung der Standortdaten von einem Endgerät eines Nutzers definiert. Diese „*dürfen nur im zur Bereitstellung von Diensten [...] erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes [...] seine Einwilligung erteilt hat*“. [Bun]

Die Wiedereinführung der **Vorratsdatenspeicherung** wurde im Oktober 2015 durch den Bundestag beschlossen. Sie beinhaltet, dass Telekommunikationsanbieter die Verkehrsdaten ihrer Kunden (also wann und mit wem ein Nutzer telefoniert hat und mit welcher IP-Adresse er sich verbunden hat) für zehn Wochen und die Standortdaten der Handynutzer für vier Wochen zu speichern und bereitzuhalten sind. Deutsche Internetanbieter hatten bis zum 1. Juli 2017 Zeit, diese Vorgaben umzusetzen. [BB16]
Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen erklärte im 22. Juni 2017 die verpflichtende Speicherung von Verbindungs- und Standortdaten der Kommunikationsteilnehmer für unzulässig, da diese „*mit dem Recht der Europäischen Union nicht vereinbar*“ (siehe *Abschnitt 2.2*) sei. Das Urteil gilt zunächst jedoch nur für das Eilverfahren und ausschließlich für den Kläger, den Münchner Provider SpaceNet. Ein Urteil im Hauptverfahren ist zur Zeit noch nicht absehbar, allerdings hat die Bundesnetzagentur daraufhin beschlossen, die Vorratsdatenspeicherung vorerst nicht durchzusetzen. Bis zu einem Urteil werden also „*keine Bußgeldverfahren wegen einer nicht erfolgten Umsetzung gegen die verpflichteten Unternehmen eingeleitet*“. [Gre17a, Gre17b]

Ein Gesetz ganz anderer Art ist das Gesetz zur effektiveren und praxistaugliche-ren Ausgestaltung des Strafverfahrens, welches unter dem Namen *Staatstrojaner* bekannt ist. Der Änderungsantrag dazu wurde am 22. Juni 2017 verabschiedet und soll die Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die heimliche Online-Durchsuchung in der Strafprozessordnung bilden.

„*Die **Online-Durchsuchung** erlaubt es Sicherheitsbehörden, Computer und andere informationstechnische Systeme mit Spähsoftware zu infiltrieren, um alle gespeicherten Informationen zu durchsuchen*“ (Andrea Voßhoff, [Kur17a]). Bislang gibt es bei der Online-Untersuchung keine Beschränkung für die Inhalte, auf die zugegriffen werden darf. [Kur17a]
Durch die **Quellen-TKÜ** dürfen Strafverfolger Inhaltsdaten von laufender Kommunikation an der Quelle abgreifen, also bevor sie ver- oder nachdem sie entschlüsselt worden sind. Dazu gehört z. B. die Kommunikation über E-Mails, Internet-Telefonie wie Skype oder Instant-Messenger wie WhatsApp, Signal, Telegram oder Threema. Nach Einschätzung der Bundesdatenschutzbeauftragten, Andrea Voßhoff, führe die Regelung zur Quellen-TKÜ „*zu erheblichen datenschutzrechtlichen Risiken und zu einem klaren Verfassungsverstoß*“. [BB17, Kre17c, Kur17a]
Bei laufenden Verfahren werden vom Bundeskriminalamt bereits Trojaner eingesetzt, um verschlüsselte Nachrichten auf Smartphones mitlesen zu können. Um verwendete Verschlüsselungsverfahren zu umgehen, werden Sicherheitslücken ausgenutzt. Aussagen zur Häufigkeit des eingesetzten Staatstrojaners für Smartphones machte das BKA nicht. [PT18]

Weitere Einschnitte bezüglich des Datenschutzes gab es im Juli 2017 durch das Gesetz zur Förderung des elektronischen Identitätsnachweises. Dadurch haben neben der Polizei, auch Geheimdienste ohne Kontrollinstanz Zugriff auf die biometrischen Daten, die im Rahmen des Personalausweises gespeichert werden.
Die Erhebung bzw. Speicherung von Daten wird auch durch das Fluggastdatengesetz (bei dem EU-Recht umgesetzt wird), das Videoüberwachungsverbesserungsgesetz oder das Gesetz zur besseren Durchsetzung der Ausreisepflicht erweitert, wodurch der Datenschutz in Deutschland weiter eingeschränkt wird. [Mü17a]

2.2 Europäische Union

Die **EU-Menschenrechtskonvention** enthält in Artikel 8 ein explizites Grundrecht auf Datenschutz. Die Menschenrechtskonvention trat 1953 in Kraft und wurde von allen Mitgliedsstaaten des Europarats unterzeichnet. Bereits 1981 nahm der Europarat die Konvention Nr. 108 mit dem Titel „*Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*“ an. Durch diese steht jeder Person das Recht „*auf Achtung ihres Privat- und Familienlebens,*

ihrer Wohnung und ihrer Korrespondenz“ zu. In Europa stehen auch Metadaten unter dem Schutz des Fernmeldegeheimnisses. [Bun16, Pet17]

Die **Charta der Grundrechte** der EU wurde 1999/2000 erarbeitet und ist seit 2009 rechtlich bindend. Darin ist in Artikel 8 ein Datenschutz-Grundrecht enthalten, welches personenbezogene Daten schützt. Daraus ergibt sich, dass personenbezogene Daten nur „*mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden*“ dürfen. Darüber hinaus hat die betroffene Person das Recht „*Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken*“. [Eur00, Pet17]

Ein Beschluss von 2006 verpflichtet alle Mitgliedsstaaten der EU dazu, die Verkehrsdaten der Telekommunikation auf **Vorrat zu speichern**. Davon sind Daten der Internetnutzung (IP-Adressen, E-Mail-Verkehr) und Telefondaten betroffen. Die Mindestspeicherungsfrist soll zwischen 6 Monaten und 2 Jahren liegen. [Sch14a]

Im Mai 2018 werden alle Regelungen der **EU-Datenschutz-Grundverordnung (EU-DSGVO)** für die EU-Mitgliedsstaaten in Kraft treten, wodurch die Verarbeitung personenbezogener Daten europaweit geregelt werden wird. Viele Bestimmungen entsprechen denen, die bisher im Bundesdatenschutzgesetz geregelt sind. Änderungen, die sich dadurch ergeben, betreffen z. B. die Erhöhung der Bußgelder bei Verstößen gegen die DSGVO, aber auch die Erweiterung der Aufgaben von Datenschutzbeauftragten um umfassende Überwachungspflichten. Zudem wird die Dokumentations- und Nachweispflichten bei der Verarbeitung personenbezogener Daten erweitert, ebenso wie die Transparenzvorschriften, durch die betroffene Personen von der Verarbeitung ihrer personenbezogenen Daten „*in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache*“ unterrichtet werden müssen (Art. 12 Abs. 1 DSGVO). Darüber hinaus müssen personenbezogene Daten gelöscht werden, wenn beispielsweise die betroffene Person einen Widerspruch gegen deren Verarbeitung einlegt (§35 BDSG. Art. 17 DSGVO). Ausnahmen von der Löschpflicht sind z. B. durch die Erfüllung einer rechtlichen Verpflichtung, das Recht auf freie Meinungsäußerung oder Gründe des öffentlichen Interesses gegeben. [Ble16, Mei16]

Die Änderungen der DSGVO haben auch Auswirkungen auf die E-Privacy-Verordnung. Diese regelt das Speichern und Auslesen von Daten auf Endgeräten von Nutzern durch Dritte und wird im Mai 2018 alle Regelungen, die auf der E-Privacy-Richtlinie 2002/58 basieren, aufheben. In Artikel 4 Abs. 3 kommen zu dem Schutz-

umfang der neuen Verordnung die Metadaten hinzu.
Auch jede Form des Webtrackings, zu denen Cookies, Fingerprinting oder ähnliche Technologien zählen, werden von der E-Privacy-Verordnung umfasst. Sofern der Webseitenbetreiber das Tracking selbst zur Besuchermessung durchführt, ist es generell zulässig. Auch wenn der Webseitenbetreiber einen Vertrag zur Auftragsdatenverarbeitung mit einem Tracking-Unternehmen abgeschlossen hat, wird das Webtracking dem Webseitenbetreiber zugeordnet und bleibt damit zulässig.
Die für Cookies relevanten Regelungen finden sich in Artikel 8 und 9, sowie den der Verordnung vorangestellten Erwägungsgründen 21 bis 24. Beispielsweise sollen Cookies, die beim Ausfüllen eines Formulars oder zur Messung des Webseiten-Traffics erforderlich sind, ohne gesonderte Einwilligung durch den Nutzer gesetzt werden dürfen. Wird eine Einwilligung eingeholt, muss der Nutzer die Wahl haben, dieser zuzustimmen oder sie abzulehnen. Bei einer Ablehnung darf für den Nutzer jedoch kein Nachteil entstehen und die Webseite darf nicht gesperrt werden. [Eur17, Mez17]

2.3 Vereinigte Staaten

Der **Foreign Intelligence Surveillance Act (FISA)** wurde vom US-Kongress 1978 beschlossen und sollte Bürger vor verfassungswidriger Ausspähung schützen, indem die Überwachung einer gerichtlichen und parlamentarischen Kontrolle untersteht. So müssen Überwachungsmaßnahmen innerhalb der USA durch den **FISA-Court (FISC)** genehmigt werden. Den US-Behörden wurde über den **Patriot Act** ein weitreichendes Kontrollrecht zur Überwachung der in den USA übertragenen Daten eingeräumt. Im Juni 2015 wurden diese abgelaufenen Bestimmungen durch die des **Freedom Act** ersetzt. Dabei werden Telekommunikationsdaten bei Telekommunikationsanbietern gespeichert und müssen an amerikanische Behörden wie dem FBI, der NSA oder der CIA weitergegeben werden, sofern ein begründeter Terrorverdacht und ein entsprechender Beschluss des Geheimgerichts FISC vorliegt. Bei Überwachungsmaßnahmen außerhalb der Vereinigten Staaten ist der FISC-Schutzmechanismus nicht erforderlich. [Sch14a, ZEI15]

Ein Instrument, um ohne FISC-Beschluss an Metadaten zu gelangen, ist der **National Security Letter (NSL)**. Dabei können US-Behörden die Datenherausgabe von Telekommunikationsunternehmen, Bibliotheken, Banken und anderen Finanzunternehmen verlangen. Im Jahr 2012 gab es 21.000 solcher Anfragen. [Sch14a]

Das Gesetz **Communications Assistance for Law Enforcement Act (CALEA)** schreibt US-Unternehmen bereits seit 1994 vor, Maßnahmen zu treffen, über die sowohl auf Gesprächsinhalte als auch auf Verkehrsdaten zugegriffen werden kann. Zunächst galt es ausschließlich für Telefonnetze und wurde 2007 auf Anbieter von Breitband-Internetzugängen und auf Unternehmen, die mit Internet-Telefondiensten zu tun haben, erweitert. 2012 wurde bekannt, dass eine Ausweitung auf CALEA II geplant sei, wobei die Vorgabe auf alle Internetunternehmen ausgeweitet werden sollte. Ob diese Pläne weiter verfolgt werden, ist nicht bekannt, zumal eine Verpflichtung der Unternehmen nicht mehr erforderlich ist, da die Schnittstellen im Rahmen von PRISM (siehe *Abschnitt 3.1*) bereits auf freiwilliger Basis eingerichtet wurden. [Sch14a]

2.4 Zusammenfassung

Nahezu alle Staaten der Welt haben sich durch die Unterzeichnung der Allgemeinen Erklärung der Menschenrechte damit einverstanden erklärt, dass es keine willkürlichen Eingriffe in das Privatleben oder den Schriftverkehr geben und dass jeder Mensch einen Schutzanspruch gegen solche Eingriffe haben soll.

Wie in *Abschnitt 2.1* dargelegt, sind in Deutschland für den Datenschutz relevante Regelungen im Grundgesetz, sowohl durch das Recht auf informationelle Selbstbestimmung, als auch das Brief-, Post- und Fernmeldegeheimnis enthalten. Darüber hinaus ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Bundesdatenschutzgesetz geregelt. Allerdings gibt es neben Datenschutzregelungen auch solche, die mit diesen in Konflikt stehen. So ist beispielsweise in Deutschland umstritten, ob die Quellen-TKÜ oder das G10-Gesetz gegen das Grundgesetz bzw. die Menschenrechte verstoßen.
Besonders seit 2015 wurden in Deutschland Gesetze beschlossen, die das bis dahin als sehr hoch eingestufte Datenschutzniveau deutlich abgesenkt haben. Dazu beigetragen haben unter anderem die in *Abschnitt 2.1* genannten Beschlüsse zur Quellen-TKÜ und Online-Durchsuchung, die formale Wiedereinführung der Vorratsdatenspeicherung, aber auch das Gesetz zur Förderung des elektronischen Identitätsnachweises.

Die in der EU geltenden Datenschutzregelungen werden von den einzelnen Mitgliedsstaaten in nationales Recht umgesetzt. Durch die EU-Menschenrechtskonvention,

sowie das Grundrecht auf Datenschutz kann in den EU-Staaten ein relativ hohes Datenschutzniveau garantiert werden. Europaweit gesehen werden auch die Beschlüsse der EU-Datenschutz-Grundverordnung, die ab Mai 2018 in Kraft treten werden, dazu beitragen, dieses Niveau nochmals anzuheben.

Wie in *Abschnitt 2.3* aufgeführt, sind die rechtlich geschützten Kontrollmöglichkeiten in den USA relativ weitreichend. So ist bei Überwachungsmaßnahmen innerhalb der USA zwar eine Genehmigung durch den FISA-Court erforderlich, jedoch nicht bei denen außerhalb der USA. Im Inland können Behörden durch den National Security Letter dafür ohne FISC-Beschluss von Telekommunikationsunternehmen die Herausgabe von Metadaten fordern. Darüber hinaus wird US-Unternehmen bereits seit 1994 durch den Communications Assistance for Law Enforcement Act (CALEA) vorgeschrieben, dass Maßnahmen getroffen werden müssen, damit Behörden auf Inhalts- und Metadaten zugreifen können.
Aufgrund dieser weitreichenden Kontrollrechte, aber auch, weil keine Datenschutzregelungen auf Bundesebene bestehen, die mit denen in Deutschland oder der EU vergleichbar wären, ist in den USA ein niedriges Datenschutzniveau gegeben.

Die rechtlich verbindlichen Gesetze zum Datenschutz sind, wie in diesem Kapitel gezeigt wurde, in jedem Staat unterschiedlich geregelt. Noch komplizierter ist die Rechtslage in Anbetracht der Tatsache, dass die Nutzung des Internets Staatsgrenzen überschreitet und damit meist mehrere Rechtslagen relevant sind.
Generell gilt das Datenschutzniveau innerhalb der EU, der Schweiz, Kanadas, Argentiniens, Guernseys und auf der Isle of Man als angemessen.

3 Methoden der Datenerhebung

Gegenstand dieses Kapitels ist es, den technischen Hintergrund ausgesuchter Methoden zur Datenerhebung im Detail zu betrachten, die von staatlichen Behörden oder Internetkonzernen zur Datenerhebung genutzt werden. In der Regel werden die hier beschriebenen Methoden in Kombination eingesetzt. Die dabei erfassten Daten dienen als Grundlage für die in *Kapitel 4* thematisierte Nutzerprofilierung.

Beim Aufruf einer Webseite wird die IP-Adresse des Nutzerrechners an den Betreiber der Webseite übermittelt. Abhängig davon, welche weiteren Elemente auf der Webseite eingebettet sind, werden neben der IP-Adresse auch weitere Informationen an den Webseiten-Betreiber oder auch an Dritte übertragen. Mit solchen - aber auch anderen Verfahren - befasst sich dieses Kapitel, wobei nur eine kleine Auswahl der tatsächlich existierenden Methoden betrachtet werden kann.

3.1 Hintertüren, Schwachstellen

Eine **Hintertür** (Backdoor) ermöglicht es, den eigentlichen Zugang zu einem Computer oder einer gesicherten Funktion eines Computerprogramms über einen geheimen Zugang zu umgehen. Häufig wird diese vom Entwickler des Programms vorsätzlich eingebaut. [Spr]
Eine **Schwachstelle** entsteht bei der Entwicklung eines Programms. Dabei handelt es sich in der Regel um Sicherheitslücken oder Fehlfunktionen von Programmen, die beispielsweise genutzt werden können, um in Computersysteme einzudringen oder diese zu manipulieren. [Bun13]

Wie bereits in *Abschnitt 2.3* dargelegt, sind US-Telekommunikationsunternehmen seit 1994 unter Androhung hoher Strafzahlungen dazu verpflichtet, ihre Systeme (wie Telefonnetze, Breitband-Internetzugänge und Internet-Telefondienste) so zu gestalten, dass sie einfach zu überwachen sind. Das bedeutet, die Unternehmen sind

dazu aufgefordert, Schnittstellen in ihre Systeme zu integrieren, über die in Echtzeit ein Zugriff auf Inhalts- und Metadaten möglich ist. Dazu müssen die Unternehmen beispielsweise bestimmte Netzwerkkomponenten (z. B. Router) verwenden, die mit entsprechenden Schnittstellen ausgestattet sind und über die Fähigkeit zur detaillierten Datenanalyse, der *Deep Packet Inspection*, verfügen. [Sch14a]
Wenn eine Person und deren Kommunikation von besonderem Interesse ist, können deren Daten so separiert und analysiert werden. Zudem kann ein Trojaner auf dem Zielsystem der betroffenen Person installiert werden, über den das System kontrolliert und manipuliert werden kann. Darüber hinaus können alle Daten, die sich auf dem System befinden, durchsucht und kopiert werden. [Sch14a]

Seit dem Anschlag vom 11.09.2001 auf das World Trade Center wurden die Befugnisse der US-Behörden drastisch ausgeweitet. Im Kampf gegen den Terrorismus werden tiefe Einschnitte bei den Bürgerrechten in Kauf genommen. 2013 sagte ein Washingtoner Bundesrichter, man könne sich „*keine rücksichtsloseren und willkürlicheren Eingriffe als diese Speicherung persönlicher Daten von praktisch jedem einzelnen Bürger [...] ohne vorherige richterliche Erlaubnis vorstellen.*“ [Sch14a, S.90-110]

Bei den Überwachungsprogrammen, die 2013 durch Edward Snowden öffentlich bekannt wurde, wurden allein 20 Programme von der *National Security Agency* (NSA) betrieben. Dabei wurden auch die Zusammenhänge zwischen den verschiedenen Komponenten des Überwachungssystems deutlich: Das Abfangen von Metadaten wurde über das Programm Mainway realisiert, die Erfassung und Filterung von Kommunikationsinhalten über Tempora. Die Auswertung der Kommunikationsinhalte aufgrund bestimmter Muster, Kommunikationspartner oder verwendeter Begriffe war Aufgabe von X-Keyscore (siehe *Abschnitt 4.2*). Das Anfordern von Daten bei Internet- und Kommunikationsunternehmen war Teil von PRISM. [Sch14a]

Das Projekt **PRISM** (Planning tool for Resource Integration, Synchronization, and Management) basiert auf der Zusammenarbeit der NSA mit neun Anbietern von Internetdiensten, darunter Google, Microsoft, Facebook, Yahoo, Apple, AOL und Paltalk. [Los15]
Es ermöglicht eine umfassende, weltweite Überwachung von Personen, die digital kommunizieren. Mit PRISM können individuelle Zielpersonen ausgewählt und deren Kommunikation direkt mitgeschnitten bzw. von den Servern abgerufen werden. Das heißt, dass sowohl auf die gespeicherte als auch auf live stattfindende Kommunikation über Dienste der beteiligten Unternehmen zugegriffen werden kann. Die NSA

kann somit Verbindungsprotokolle, Fotos, Musik, Videos, E-Mails, Chats (in Form von Text, Audio oder Video), aber auch andere Dokumente mitlesen, speichern und durchsuchen. [Fri15]

Die NSA überwacht nicht nur Bürger, sondern auch Regierungsmitglieder und politische Einrichtungen. So hat das Programm **DROPMIRE** zur Aufgabe, die verschlüsselte Faxkommunikation zwischen der EU-Vertretung in Washington und der EU-Zentrale in Brüssel zu überwachen. So wurden beispielsweise geschützte Netzwerke von EU-Institutionen und die Telefonanlage des Europäischen Rates ausgespäht. [Sch14a]

Der britische Geheimdienst *Government Communications Headquarters* (GCHQ) überwacht mit **Tempora** den weltweiten Internet- und Telekommunikationsdatenverkehr. Die Datenübertragung zwischen Europa, den Vereinigten Staaten und anderen Regionen findet über Unterseekabel statt. Für diese Übertragung müssen die Signale in Relaisstationen verstärkt werden. Über diese Stationen hat der britische Geheimdienst Zugriff auf 200 Glasfaserkabel, jedes mit einer Übertragungskapazität von 10 Gigabits pro Sekunde. An einem Tag ergibt sich somit eine Datenmenge von 21 Petabytes, die dem GCHQ zu Verfügung steht. Darin sind Telefonate, E-Mails und Daten der Internetnutzung enthalten. Laut Edward Snowden handle es sich bei Tempora „*um das größte Programm zur verdachtslosen Überwachung in der menschlichen Geschichte*“. [Sch14a, S.29]
Diese Daten teilt die GCHQ für mehr als 100 Millionen britische Pfund jährlich mit der NSA. [Sch14a]

Analog zu den Behörden in den USA und Großbritannien existieren auch in Deutschland entsprechende Organe. In Deutschland gibt es insgesamt 19 Nachrichtendienste: den Bundesnachrichtendienst (BND), den Militärischen Abschirmdienst (MAD), das Bundesamt für Verfassungsschutz (BfV) und 16 Landesämter für Verfassungsschutz (LfV). Dabei ist der BND direkt dem Bundeskanzleramt unterstellt und befasst sich mit der wirtschaftlichen, politischen und militärischen Auslandsaufklärung. Die Arbeit des BfV ist dagegen auf das deutsche Inland beschränkt. Für den BfV sind all jene Informationen relevant, die gegen die freiheitliche demokratische Grundordnung und gegen die Sicherheit der Bundesrepublik gerichtet sind. Fernmeldeüberwachungen des BfV müssen durch einen parlamentarischen Ausschuss, die G10-Kommission, genehmigt werden. [Sch14a]

In der im November 2016 beschlossenen *Cyberstrategie für Deutschland* wird der Ansatz *Sicherheit trotz Verschlüsselung* verfolgt, wodurch die finanziellen Mittel für Überwachungsmaßnahmen in Deutschland ausgebaut werden.
Das Budget für den BfV betrug im Jahr 2017 307 Millionen Euro, was einer Steigerung von 18% zum Vorjahr entspricht. Die Erhöhung beim BND beträgt 12%, insgesamt sind das 808 Millionen Euro. Davon wird auch das BND-Projekt *Panos* finanziert, bei dem Schwachstellen in der Verschlüsselung von Instant-Messengern aufgespürt werden sollen. [BB16, Reu16]

Die **Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)**, welche unabhängig von der Aufstockung finanziert wird und 2017 ihren Dienst aufgenommen hat, soll verschlüsselte Kommunikation dechiffrieren und dadurch sowohl die Polizei als auch den Verfassungsschutz unterstützen. ZITiS nutzt Schwachstellen in Hard- und Software, um Trojaner auf Smartphones zu installieren. Darüber hinaus werden Mechanismen zur Verschlüsselung umgangen. Ziel dabei ist es, die verschlüsselte Kommunikation von Instant-Messengern mitlesen zu können. [BB16, Tan17]

Leistungsstarke und fehlerfreie Verschlüsselungsverfahren sind kaum zu entschlüsseln, weshalb immer mehr Geld in Maßnahmen investiert wird, um die Verschlüsselung zu unterlaufen. Die NSA und die GCHQ haben dazu die Projekte BULLRUN, Edgehill und Muscular gestartet, bei denen IT-Unternehmen, die Produkte zur kommerziellen Datenverschlüsselung anbieten, Geld erhalten haben. Als Gegenleistung wurden Wissen und Technik zur Verfügung gestellt, wie sich der von diesen Unternehmen entwickelte Schutzmechanismus umgehen lässt. So hat RSA, einer der wichtigsten Hersteller von Verschlüsselungstechnik, mit der NSA zusammengearbeitet. Dabei konnte die NSA die Verwendung eines schwachen Verschlüsselungsalgorithmus als Standardeinstellung in den von RSA angebotenen Produkten durchsetzen. Das Mitlesen verschlüsselter Daten wurde in diesem Fall mit einer Einschränkung der Verschlüsselungsstärke ermöglicht. Auch die Standards zur Erzeugung von Schlüsseln sei manipuliert worden, indem der Zufallsgenerator auf bestimmte Wertebereiche beschränkt wurde. [Sch14a]
Microsoft habe ebenfalls dabei geholfen die Verschlüsselung von Daten seiner Nutzer zu umgehen. Skype galt bis zur Übernahme von Microsoft als nahezu abhörsicher. Danach wurden Abhörschnittstellen in den Dienst eingebaut. [Sch14a]

Aufgrund einer Sicherheitslücke bei Microsoft konnte der Trojaner *WannaCry* weltweit innerhalb von drei Tagen mehr als 220.000 Computer in 150 Ländern infizieren. Es wird vermutet, dass der NSA die dabei genutzte Sicherheitslücke bekannt gewesen ist, diese jedoch nicht an Microsoft zur Behebung weitergeleitet, sondern stattdessen geheim gehalten und für eigene Zwecke genutzt wurde. Stichhaltige Beweise dafür gibt es jedoch nicht. [Bri17, Ste17]

3.2 Cookies

Eine weit verbreitete Möglichkeit, Nutzerdaten zu sammeln, sind Cookies. Dabei handelt es sich um kleine Textdateien, in denen Informationen über den Nutzer auf dessen Rechner gespeichert werden. Sie können mit geringem Aufwand gesetzt, geändert, gelesen und gelöscht werden und werden darüber hinaus von jedem Browser unterstützt.

Cookies werden entweder clientseitig über ein Skript, das z. B. in der Sprache JavaScript verfasst sein kann, erzeugt oder von Webservern generiert und in einer *HTTP-Response* an den Client übermittelt. Wird eine Webseite erneut aufgerufen, für die bereits ein Cookie vorliegt, wird das Cookie ausgelesen bzw. beim *HTTP-Request* wieder vom Client an den Webserver übermittelt. Cookies sind an eine Internetadresse (Domain) gebunden, das heißt, sie werden immer nur an die Domäne übermittelt, von der sie stammen. [LoI, Mau15, Pet17]
Ein Cookie muss serverseitig mindestens über einen eindeutigen Namen verfügen. Wichtige optionale Attribute sind der Wert (also die Information des Cookies), der Pfad auf dem Server, für den das Cookie verfügbar ist und das Ablaufdatum. Darüber hinaus können Cookies einen eindeutigen Identifikator enthalten, wodurch sie vom Webserver einem Nutzer zugeordnet und in einen zeitlichen Bezug gebracht werden können. Damit wird die Zustandslosigkeit des HTTP-Protokolls – also die Eigenschaft des Protokolls, mehrere Anfragen grundsätzlich als voneinander unabhängige Transaktionen zu behandeln – umgangen und die Wiedererkennung eines Nutzers ermöglicht. [LoI, Mau15, Pet17]
Cookies kommen beispielsweise beim Login auf einer Webseite, bei Warenkorbsystemen oder Online-Banking zum Einsatz. Sie können jedoch auch verwendet werden, um das Surf-Verhalten eines Nutzers zu erfassen und ihm z. B. personalisierte Werbung einblenden zu können. Begrifflichkeiten, verschiedene Arten von Cookies

und deren Einsatzzweck werden beispielhaft im Folgenden betrachtet. [Hei15, LoI, Pet17]

Session Cookies dienen dazu die Internetnutzung einfacher und komfortabler zu gestalten. Sie werden zum Zwecke der Verwaltung von Sitzungsinformationen erstellt und verlieren ihre Gültigkeit und Existenz mit dem Sitzungsende bzw. spätestens mit dem Schließen des Browsers. [LoI]

Persistent Cookies haben eine Gültigkeitsdauer von mehreren Monaten bis hin zu Jahrzehnten. Sie werden über mehrere Sitzungen verwendet und können so die Aktivitäten des Nutzers sitzungsübergreifend verknüpfen. Dadurch wird das gewonnene Bild über die Nutzer erweitert und detaillierter. [LoI]

HTML5-Cookies beruhen auf der Einführung einer neuen Speichertechnologie mit dem HTML5-Standard. Dabei wird zwischen *Session-Storage* und *Local-Storage* unterschieden. Sie unterscheiden sich insbesondere dadurch, dass bei einem *Session-Storage*-Objekt die Daten lediglich für eine Session gespeichert werden und beim Schließen des entsprechenden Browser-Tabs wieder gelöscht werden. Bei einem *Local-Storage*-Objekt dagegen wird das Cookie nicht mit dem Schließen des Browser-Tabs gelöscht, sondern ist über die Session hinaus verfügbar.
Beim HTML5-Standard stehen darüber hinaus die Speicherbereiche *Global Storage*, *Database Storage* via SQLite und *HTML5 IndexedDB* zu Verfügung, welche ebenfalls zur Speicherung von Cookies genutzt werden können. [Kam10, Mau15, W3S17]

Flash-Cookies oder *Local Shared Objects* (LSOs) basieren auf der Skriptsprache ActionScript, mit der unter anderem Programme für Adobe Flash entwickelt werden können. Beim Besuch einer Webseite können Webserver auch Flash-Inhalte übertragen, welche dann Flash-Cookies setzen. Für deren Verwaltung ist nicht der Browser, sondern die Flash-Player-Anwendung des Nutzers, bspw. in Form eines Browser-Plugins zuständig. Daher sind diese Cookies browserunabhängig und können nicht über die Löschfunktion im Browser entfernt werden. Flash-Cookies haben kein Verfallsdatum und keine Größenbegrenzung. Zudem haben Flash-Cookies den Vorteil, dass sie Browser-übergreifend verfügbar sind, zumindest bei allen Browsern, die das Adobe Flash Plugin verwenden. [AEE+14, LoI, Pet17]

Evercookies werden auch *Zombiecookies* genannt, weil sie unmittelbar nach dem Löschen erneut erzeugt werden. Dabei werden unterschiedliche Cookie-Verfahren miteinander kombiniert. Nach Angaben des Sicherheitsforschers Samy Kamkar nutzt

ein Evercookie bis zu 13 verschiedene Technologien, um sich redundant auf dem Rechner des Nutzers zu speichern, beispielsweise HTTP-Cookies, Flash-Cookies, HTML5-Cookies, ETags und Silverlight-Cookies. Darüber hinaus werden Cookie-Inhalte auch als Bilddatei oder als Teil des Browserverlaufs gespeichert. [Kam10, Mau15, Sch16]

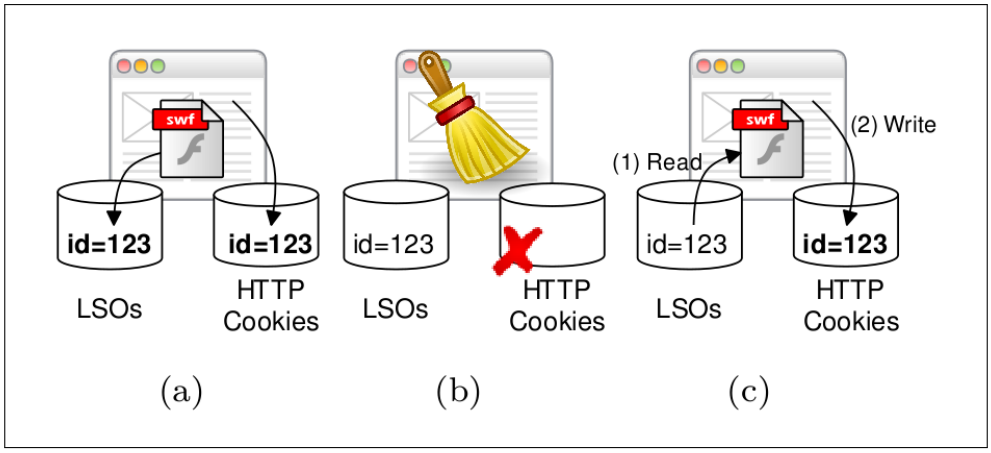

Abbildung 1: Wieder-Erstellung eines HTTP-Cookies [AEE+14]

Das Prinzip einer erneuten Erstellung eines HTTP-Cookies mit Hilfe eines Flash-Cookies (LSOs) zeigt *Abb. 1.* Beim Besuch einer Webseite, die Evercookies verwendet, wird eine Nutzer-ID (id=*123*) und andere Informationen sowohl in einem HTTP-Cookie als auch in einem Flash-Cookie gespeichert (a). Entfernt der Nutzer zwar das HTTP-Cookie, jedoch nicht das Flash-Cookie (b), wird nach dem Löschvorgang aufgrund des Flash-Cookies ein neues HTTP-Cookie erzeugt. Diesem werden die identischen Informationen (auch die ID mit dem Wert *123*) zugewiesen, indem die Werte aus dem Flash-Cookie ausgelesen werden (c).
Da Flash-Cookies Browser-übergreifend verfügbar sind, können bei der Verwendung mehrerer Browser Cookies, die bereits aus dem Speicherbereich eines Browsers gelöscht wurden, durch den Einsatz eines anderen Browsers erneut erzeugt werden. [AEE+14]

Bei **Third-Party Cookies** handelt es sich um Session Cookies oder Persistent Cookies von Dritten, die das Surf-Verhalten von Nutzern über mehrere Webseiten mitverfolgen können. Wie in *Abb. 2* beispielhaft dargestellt ist, werden dazu externe Inhalte von Dritten (z. B. von Werbedienstleistern) in Webseiten eingebunden. Auch diese externen Inhalte der Werbedienstleister können Cookies setzen und lesen. Im Folgenden wird dieser Vorgang beispielhaft im Detail beschrieben.

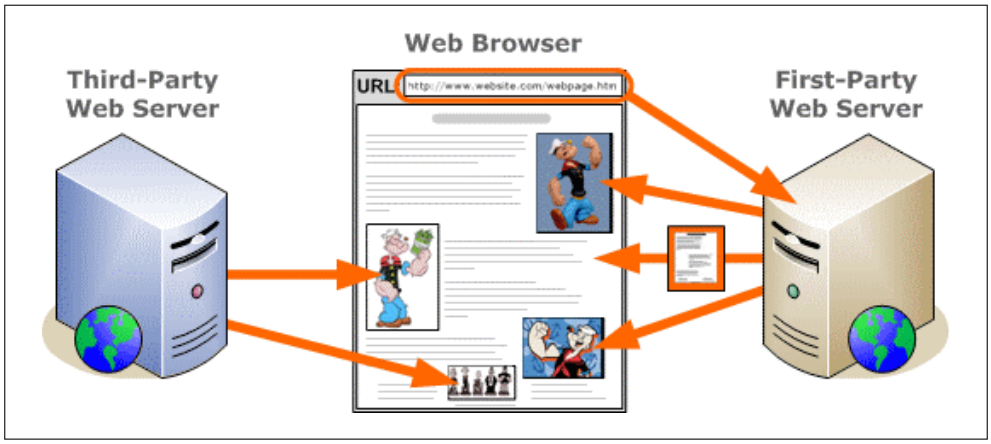

Abbildung 2: Externe Inhalte von Dritten [Gib16]

Grundsätzlich werden Cookies zwar immer nur an die Domäne übermittelt, von der sie stammen. Ruft aber ein Nutzer beispielsweise die Internetseite *www.spiegel.de* auf, in welcher der Drittanbieter *www.krux.com* externe Inhalte (beispielsweise ein Bild, ein Werbebanner, eine Schaltfläche von sozialen Netzwerken oder auch ein einziges unsichtbares Pixel, das auch Bacon genannt wird) eingebunden hat und darüber ein Third-Party Cookie gesetzt wird, so stammt das Cookies nicht von der Domäne *www.spiegel.de*, sondern von *www.krux.com*. Die Informationen des Nutzers werden daher auch an diese Domäne übermittelt.
Cookies oder andere Technologien von Werbedienstleistern, die Nutzer über unterschiedliche Webseiten hinweg erkennen können, werden als Tracker bezeichnet. Wird z. B. eine Suche bei einem Anbieter für Flüge durchgeführt, deren Webseite einen Tracker integriert hat, mit dem auch ein Online-Buchhändler in einer Geschäftsbeziehung steht, kann die angezeigte Werbung beim Aufruf der Webseite des Buchhändlers entsprechend an die durchgeführte Suchanfrage für Flüge angepasst werden. Je mehr Cookies eines Werbedienstleisters verbreitet sind, desto vollständiger ist das Bild der getrackten Nutzer. Da Werbedienstleister mit vielen verschiedenen Webseitenbetreibern Verträge haben, können sie dadurch das Nutzerverhalten über viele Webseiten-Aufrufe und Domänen hinweg verfolgen. [LoI, Pet17]

Beim sogenannten **Cookie Syncing** bzw. **Cookie Matching** tauschen z. B. Werbedienstleister ihre Informationen untereinander aus, indem sie ihre Datenbanken vereinen bzw. die eindeutigen Kennungen der verschiedenen Domains austauschen. Für das Mapping der IDs werden sogenannte Cookie-Matching-Tabellen zu Hilfe genommen. Beim Aufruf einer Webseite kann der Inhaber der Seite bzw. von In-

halten im Rahmen des Mappings die Nutzer-ID an ein weiteres System (z. B. einen Adserver) weitergeben. Dadurch kann das Drittsystem kurzzeitig auf den Nutzer-Browser zugreifen und eine eigene ID setzen. Beide IDs werden daraufhin in der Cookie-Matching-Tabelle gespeichert. Nach einem Matching kann in der Tabelle nachgeschlagen werden, ob weitere IDs zu einem Nutzer existieren. Die verfügbaren Informationen zu den Nutzer-IDs können die Beteiligen dann untereinander austauschen.
Einen Einblick in die Verflechtungen von Third-Party-Trackern erhält man über die Webseite *webcookies.org* oder das Firefox-AddOn Lightbeam. In *Abschnitt 5.5* ist die Anwendung von Lightbeam illustriert. [LoI, Sch17b]

3.3 eTags

Neben Cookies wird auch der Cache des Browsers genutzt, um Nutzer wiederzuerkennen. Eine grundlegende Methode stellt dabei das eTag dar. ETag steht für *entity tag* und ist ein Header-Feld, welches verhindern soll, dass identische Ressourcen mehrfach angefordert und geladen werden. Wird beispielsweise eine Webseite mit dem Bild *pic.png* aufgerufen, so wird das Bild im Cache des Browsers gespeichert und zusätzlich eine eindeutige Zeichenkette (eTag) vom Server gesendet. Anhand des eTags kann bei einem erneuten Aufruf des Bildes *pic.png* festgestellt werden, ob sich das Bild bereits im Cache des Browsers befindet und wird nicht erneut geladen, sofern der identische eTag vorliegt. Um diese Methode zur Identifikation eines Nutzers zu verwenden, wird jedem Anwender eine eindeutige Zeichenkette zugeordnet. Das gleiche Prinzip wird auch bei Cookies angewendet, jedoch werden eTags auch dann gesendet, wenn das Setzen von Cookies oder die Verwendung von JavaScript blockiert wurde. [Sch13, SES14]

3.4 Fingerprinting

Das Akzeptieren von Cookies kann im Browser schnell und vergleichsweise einfach verweigert werden. Aufgrund der dadurch etwaig resultierenden Nichtverfügbarkeit von Cookies wurden Werbetreibende dazu motiviert eine Alternative zu finden, Nutzer zu identifizieren und deren Aktivität über mehrere Webseiten hinweg verfolgen

zu können. Dies ist gelungen, indem der Nutzer anhand von Merkmalen seines Browsers (*Browser Fingerprinting*), bzw. aufgrund der Art und Weise wie Schrift oder Bilder dargestellt werden (*Canvas Fingerprinting*) identifiziert wird.

Beim **Browser Fingerprinting** können sowohl Hardwareparameter, wie Prozessortyp und Seriennummer, als auch Softwareparameter, wie Betriebssystem, Browser, Browser-Plugins, Sprach- und Farbeinstellungen oder installierte Schriftarten zur eindeutigen Wiedererkennung genutzt werden. Die unterschiedlichen Parameter werden kombiniert und daraus Profile erstellt. [Sch14a]

Das **Canvas Fingerprinting** macht sich den Umstand zu Nutzen, dass verschiedene Rechner, je nach Betriebssystem, Grafikkarte und -treiber, Browser und installierten Schriften, den Text einer Webseite unterschiedlich darstellen. Darüber lässt sich die genutzte Hardware und letztendlich der Nutzer wiedererkennen.
Dazu wird über Javascript ein nicht sichtbares HTML- bzw. Canvas-Element in eine Webseite eingebettet, in dem dann ein bestimmter Text oder ein bestimmtes Bild hinzugefügt wird, woraufhin die gerenderten Pixel, bzw. deren Hash-Werte ausgelesen werden. Anhand dieser Rendering-Merkmale können Fingerprinting-Informationen über den Browser gewonnen werden.
Wie das Bild bzw. der Text aussieht, hängt also vom Betriebssystem, der Bildschirmauflösung, den installierten Schriftarten und der Browser-Version ab. Da fast jede Browser-Computer-Kombination bei der Erstellung dieses Canvas-Elements kleine Unterschiede aufweist, kann so jeweils eine eindeutig identifizierbare Nummernfolge generiert werden, und der Rechner des Nutzers ist durch diesen individuellen Code (Fingerprint) gekennzeichnet. [LoI, Spi14]

Eine Forschungsgruppe der KU Leuven und der University of California haben den Quellcode der drei Fingerprinting-Anbieter *BlueCava*, *Iovation* und *ThreatMetrix* untersucht. Dabei hat sich gezeigt, dass alle drei Anbieter sowohl Flash als auch JavaScript einsetzen, um die Fingerprints zu erstellen.
In Abhängigkeit davon, ob eine Funktion direkt vom Browser oder vom Flash-Plugin ausgeführt wird, werden unterschiedliche Informationen zurückgegeben. So liefert die in Flash reimplementierte Browserfunktion bei der Abfrage der verwendeten Plattform als Antwort die vollständige Kernel-Version, z. B. *Linux 3.2.0-26-generic*; während die gleiche Abfrage unter Firefox dagegen lediglich *Linux x86_64* lautet.
Ebenso enthält der Rückgabewert der Funktion bezüglich der Bildschirmauflösung unterschiedliche Informationen: das Flash-Plugin gibt als Auflösung die Summe der

angeschlossenen Monitore zurück; die Browser-Funktion dagegen liefert die Auflösung des Monitors, in dem sich das Browser-Fenster befindet. Werden beiden Antworten miteinander kombiniert, kann abgeleitet werden, ob zwei Monitore angeschlossen sind und welche Auflösung diese haben. Somit können über Flash- oder JavaScript-Plugins spezifische Informationen gewonnen werden. Dies sind nur zwei Beispiele, welche die diffizilen Abfragemöglichkeiten verdeutlichen sollen. [NKJ+13]

Mittels Flash können ebenso installierte Schriften abgefragt werden. Einer der Anbieter stellt zudem eine Möglichkeit bereit, die Schriften zu ermitteln, selbst wenn das Flash-Plugin nicht vorhanden ist.

Diese Vorgehensweise wird nachfolgend beispielhaft beschrieben:

1. Zunächst wird ein *div*-Element erzeugt, in dem sich ein *span*-Element befindet. In dem *span*-Element wird eine bestimmte Zeichenkette in einer bestimmten Größe und Schriftart generiert.

2. Nun wird die Breite und Höhe der HTML-Elemente über die JavaScript-Eigenschaften *offsetWidth* und *offsetHeight* für die default-Schriftart des Browsers ermittelt. Dazu wird der Methode *get_text_dimensions* als Parameter für die Schriftart der Wert *sans* übergeben. Die default-Schrift verwendet ein Browser immer dann, wenn eine andere angefragte Schrift nicht verfügbar ist.

3. Daraufhin wird die Methode *get_text_dimensions* für eine vordefinierte Liste von Schriftarten ausgeführt. Sind Höhe und Breite identisch mit den Abmessungen der default-Schriftart, ist die abgefragte Schrift auf dem System nicht vorhanden und der Browser hat die Fallback-Schrift gewählt. Um auch geringe Abweichungen zwischen den Schriftgrößen feststellen zu können, erfolgt der Methodenaufruf mit einer besonders großen Schriftgröße.

Mit dieser Methode, die in einem für den Nutzer nicht sichtbaren *iframe* stattfindet, kann bei etlichen Schriftarten abgefragt werden, ob sich diese auf dem Betriebssystem befinden oder nicht. [NKJ+13]

Neben den installierten Schriften kann weiterhin ermittelt werden, ob ein HTTP-Proxy verwendet wird. Das gleiche Forschungsteam hat Hinweise darauf gefunden, dass das Fingerprinting-Skript mittels Flash die Proxy-Einstellungen des Nutzers auf Browser-Ebene umgeht, um so das Resultat der Flash-Anfrage daraufhin mit dem einer JavaScript-Anfrage vergleichen zu können. Obwohl das Team keinen Zugriff auf

den serverseitigen Code der Fingerprinting-Anbieter hatte, vermutet es, dass Identifikatoren dazu verwendet werden, um herauszufinden, ob zwei möglicherweise unterschiedliche IP-Adressen miteinander übereinstimmen. Dazu wird zwischen Flash und JavaScript ein alphanumerisches Token ausgetauscht. Enthält die von JavaScript stammende Antwort das gleiche Token, wie die von Flash stammende Antwort, weicht jedoch die IP-Adressen beider Anfragen voneinander ab, kann daraus abgeleitet werden, dass der Nutzer einen HTTP-Proxy verwendet. [NKJ+13]

Ist die vom Nutzer aufgerufene Webseite diejenige, welche die Eigenschaften für den Fingerprint anfordert, kann der Fingerprint des Nutzers im DOM (Document Object Model) der Seite hinzugefügt werden. Angenommen die Domain *www.spiegel.de* bindet Skripte des Fingerprinting-Anbieters *BlueCava* ein, um dessen Dienste zu nutzen, ist der Ablauf wie folgt: Das Skript liest zunächst die Fingerprinting-Merkmale eines Nutzers aus und kombiniert diese zu einem Fingerprint. Daraufhin wird der Fingerprint verschlüsselt und die resultierende Zeichenkette wird mittels DOM-Manipulation zu der Objektstruktur von *www.spiegel.de* hinzugefügt (ein Browser übersetzt den Text einer Webseite in eine Objekt- oder Baumstruktur, die im Arbeitsspeicher gehalten wird; zu dieser wird die verschlüsselte Fingerprinting-Zeichenkette hinzugefügt). Dadurch wird beispielsweise der verschlüsselte Fingerprint an die Server von Spiegel Online übermittelt, sobald ein Nutzer deren Webseite aufruft. Allerdings kann Spiegel Online den Fingerprint nicht selbst entschlüsseln, sondern muss ihn zurück an *BlueCava* senden, die wiederum mit Informationen über das Gerät des Nutzers antworten.
Diese Architektur erlaubt es *BlueCava* die Implementierungsdetails vor ihren Klienten geheim zu halten und zugleich Nutzerprofile über ihren gesamten Klienten-Kreis hinweg erstellen und zuordnen zu können. [NKJ+13]

Viele Attribute, die zur Berechnung des Fingerprints herangezogen werden können, sind auf der Webseite *browserspy.dk* zum Selbsttest aufgelistet. Um die Verfahrensweise der Tracker nachstellen und untersuchen zu können, hat die Electronic Frontier Foundation (EFF) einige dieser Attribute in einen Fingerprinting-Algorithmus integriert. Die Testseite *panopticlick.eff.org* nutzt diesen Algorithmus und zeigt, welche Daten abgefragt werden und ob für den Nutzer ein eindeutiger Fingerabdruck berechnet werden kann. [Hei15, LoI]

3.5 Ultraschall-Tracking

Ein Forschungsteam der TU Braunschweig konnte in 234 Android-Apps des Anbieters Silverpush sogenannte *Ultraschall-Beacons* nachweisen. Diese Technologie ist in Apps von Konzernen wie McDonalds oder Krispy Kreme enthalten, die bereits millionenfach heruntergeladen wurden. Dabei wird z. B. in Geschäften, über TV-Werbung oder YouTube-Videos eine vom Menschen nicht hörbare Ultraschallwelle in einem Frequenzbereich zwischen 18 und 20kHz mit einer versteckten Information abgesendet. Von einem Empfangsgerät, wie bspw. einem Smartphone mit einer App des oben genannten Herstellers, die Zugriff auf das Mikrofon hat, wird die versteckte Information aufgezeichnet und daraufhin dekodiert. Dieses Beacon wird anschließend mit Zusatzinformation über den Nutzer vom mobilen Gerät zurück an den Provider gesendet. In Europa konnte das Forschungsteam diese Technologie bereits in 4 von 35 untersuchten Geschäften nachweisen. [AQWR17, Kre17a, Ric17]

Beim Ultraschall-Tracking, bei dem sich Sender und Empfänger am selben Ort befinden müssen, können verschiedene Geräte wie Smartphone, Tablet, PC und Smart-TV einem gemeinsamen Nutzer zugeordnet werden (Cross-Device-Tracking). Dadurch kann einerseits ein umfangreicheres Nutzerprofil erstellt, aber auch Nutzer von Anonymisierungs-Netzwerken wie Tor (siehe *Abschnitt 5.2.1*) deanonymisiert werden. In Geschäften wird die Technologie dazu verwendet, um dem Nutzer, in Abhängigkeit seines Standorts und des aufgesuchten Geschäfts, entsprechende Rabattgutscheine zu übermitteln (Location-Based-Marketing). [AQWR17, Ric17, Wei17]

3.6 Mobile Geräte

Mobile Geräte wie Smartphones oder Tablets sind zu einem permanenten Begleiter ihrer Besitzer im Alltag geworden. Dabei werden sie für unzählige Anwendungen und Funktionen eingesetzt: als Routenplaner, zum Musik hören, zur Organisation von Terminen und Kontaktdaten, zur Kommunikation über E-Mail und Instant-Messenger, zum Telefonieren und für viele weitere Funktionen. Um die vielfältigen Anwendungsfälle unterstützen zu können, verfügen mobile Geräte über eine hohe Anzahl unterschiedlicher Sensoren, Kameras und ein Mikrofon. Demzufolge wird eine große Menge unterschiedlicher Daten auf diesen Geräten verarbeitet, auf welche

wiederum die Anbieter der installierten Apps in unterschiedlichem Maße Zugriff haben.
Für ihre Funktion benötigen Apps **Zugriffsrechte** auf bestimmte Daten- oder Hardwareressourcen, wie Adressbuch, Kalender, Standort, Mikrofon oder Kamera. Allerdings fordern Apps häufig mehr Zugriffsberechtigungen ein, als für ihre eigentliche Funktion erforderlich ist. Über je mehr Berechtigungen eine App verfügt, desto mehr Nutzerdaten kann der App-Anbieter erfassen. [Chr14]
Beispielsweise können Spiele-Apps, welche die Software des Unternehmens Alphonso enthalten (z. B. Pool 3D oder Honey Quest), zu beliebigen Zeitpunkten Audiosignale auswerten, die über das Mikrofon empfangen werden. In diesem Fall sollen dabei Sendungen und Werbespots identifiziert werden, die sich der Nutzer ansieht. Diese Information wird dazu genutzt, um Werbung zu platzieren, die auf den Standort und die Gewohnheiten des Nutzers abgestimmt ist. [Jur17, Mah17]

Häufig werden die erfassten Daten auch an dritte Parteien weitergegeben. So sollen mehr als 75 Prozent aller Android Apps zumindest einen Tracker von **Drittanbietern** enthalten. Betroffen sind unter anderem weit verbreitete Apps wie Tinder, Spotify, Uber oder OKCupid, die alle den Google-Service CrashLytics integrieren. Dieser sammelt primär Absturzberichte, aber auch Erkenntnisse über das Nutzerverhalten. Die weniger weit verbreitete Tracker-Software von FidZup setzt als Tracking-Methode Ultraschall-Signale (siehe *Abschnitt 3.5*) ein und wertet zudem die Verfügbarkeit von WLAN-Netzwerken aus. [Bei17, Her17]

Nicht nur die App-Anbieter und eingebundene Tracker haben Zugriff auf die Nutzerdaten eines Mobilgeräts. In der Regel ist ein mobiles Gerät mit einem **Plattform-Account** verknüpft; so verfügen Android-Geräte meist über einen Google- und iOS-Geräten über einen Apple-Account. Auch an diese Plattform- bzw. App-Store-Betreiber erfolgt eine Datenübertragung. Darüber hinaus haben auch die Mobilfunk-Netzbetreiber Zugriff auf die Daten ihrer Nutzer und speichern diese. [Chr14]

Mobile Geräte verfügen über unterschiedliche **Identifikatoren**, auf welche die installierten Anwendungen Zugriff haben. Dadurch wird das explizite Zuweisen einer eindeutigen Zeichenkette zur Wiedererkennung eines Nutzers überflüssig; Apps können einen bereits bestehenden Identifikator abfragen, an den der Nutzer z. B. über das Gerät (IMEI), die SIM-Karte (IMSI) oder das installierte Betriebssystem gebunden ist. Dies trägt dazu bei, dass mobile Geräte besonders anfällig für das Nutzer-Tracking sind. [SES14]

Mobilgeräte können aber auch deshalb so einfach verfolgt werden, weil sie permanent Signale aussenden, beispielsweise um WLAN oder Bluetooth-Geräte zu finden. Über diese Signale können die Geräte identifiziert und verfolgt werden. Ein mobiles Gerät kann sowohl über Funkzellen, das integrierte GPS-Ortungssystem als auch über die WLAN-Funktion lokalisiert werden. [Ruh17, Sch14a]
Ist ein Smartphone aktiv auf der Suche nach einem **WLAN**, sendet es immer wieder ein *Probe Request* aus, woraufhin die verfügbaren Access Points mit einer *Probe Response* antworten. Diese Antwort beinhaltet den WLAN-Namen (SSID) und weitere Informationen, z. B. zur verwendeten Verschlüsselung. Mit dem *Probe Request* des Smartphones wird unter anderem auch die MAC-Adresse (Seriennummer des WLAN-Chips) übertragen, über die das Gerät eindeutig identifiziert werden kann. Wird der WLAN-Datenverkehr über eine längere Zeit und über mehreren Access Points hinweg überwacht, können die *Probe Requests* ausgewertet und daraus Bewegungsprofile erstellt werden. [Ruh17, WE14]
In der Regel sind auf einem Mobilgerät WLAN-Namen (SSIDs) abgespeichert mit denen automatisch eine Verbindung hergestellt wird, sobald diese in Reichweite sind. Bei den *Probe Requests* werden dann auch diese SSIDs übertragen, aus denen weitere Rückschlüsse gezogen und Informationen gewonnen werden können, z. B. wo sich ein Smartphone-Nutzer häufig aufhält. [WE14]

Ähnlich funktioniert die Lokalisierung über **Bluetooth**, wobei die Bluetooth-Module eines Smartphones eine eindeutige Nummer aussenden, die zur Identifizierung der Nutzer verwendet werden kann. Zugleich können Signale von Bluetooth-Sendern (Beacons) empfangen werden, die Aktionen bei installierten Apps auslösen oder personalisierte Werbung einblenden können. Durch die Auswertung der Signale kann so beispielsweise der Bewegungsablauf eines Smartphone-Nutzers innerhalb von kleineren Arealen, wie einem Zoo oder Flughafen verfolgt werden. [Ruh17, Wol17]
Google kann zudem den Standort über Bluetooth aufzeichnen, selbst wenn der Nutzer die Bluetooth-Funktion deaktiviert hat. Dabei werden Identifikatoren aller Android-Geräte gesammelt, die Bluetooth-Signale (Beacons) aussenden. Die Daten werden dann an Google übertragen. [Fan18]

Insbesondere Behörden nutzen unter anderem **Funkzellenabfragen**, um bei Straftaten Mobilfunkgeräte innerhalb eines bestimmten Funkzellenbereichs oder das Bewegungsprofile eines konkreten Mobilfunk-Nutzers zu ermitteln. Dabei werden Daten vom Mobilfunk-Netzbetreiber angefordert und näherungsweise ausgewertet. [Kre03]
Die Funkzellenabfragen durch das Bundeskriminalamt stiegen vom ersten Halbjahr

2017 mit 149 auf 376 Abfragen im zweiten Halbjahr. [Mon18]
Jedoch können nicht nur Behörden mobile Geräte orten, deren GPS-Funktion deaktiviert ist. Auch Google kann bei Android-Geräten den ungefähren Standort ermitteln. Die Position kann mittels Triangulation zwischen verschiedenen Mobilfunkmasten auf ungefähr 400 Meter genau bestimmt werden. In Städten kann aufgrund der höheren Funkmasten-Dichte die Position entsprechend genauer ermittelt werden. Seit Anfang des Jahres 2017 soll diese Information an Google übermittelt worden sein, um Performance und Geschwindigkeit bei der Nachrichtenübermittlung zu optimieren. Die Daten sollen über den Firebase-Cloud-Messanging-Dienst erhoben werden, daher sind alle Smartphones betroffen, die diesen Hintergrunddienst nutzen. [Gib17, Gie17]

Neben der Funkzellenabfrage kommen besonders bei Behörden auch stille SMS oder IMSI-Catcher zum Einsatz. Bei **stillen SMS** werden vom Computer Kurzmitteilungen an einen bestimmten Empfänger versendet. Diese Nachrichten werden jedoch lediglich gegenüber dem Mobilfunknetz registriert, aber nicht vom Empfangsgerät, d.h. sie bleiben dem Betroffenen verborgen. Allerdings werden dabei Verbindungsdaten erzeugt, die von Behörden wiederum beim Mobilfunkprovider angefordert und ausgewertet werden können. Somit kann eine Person geortet oder – bei wiederholter Anwendung – ein Bewegungsprofil erstellt werden. [Kre03]
Im Jahr 2017 ist die Verwendung der stillen SMS deutlich angestiegen. So wurden im zweiten Halbjahr 2016 noch 143.809 dieser Nachrichten durch den Verfassungsschutz versendet, während ein Jahr später 179.285 stille SMS versendet wurden. Beim Bundeskriminalamt stieg im zweiten Halbjahr 2016 die Anzahl von 16.693 auf 21.932 im Jahr 2017. [Mon18]

Mit **IMSI-Catchern** können sowohl Bewegungsprofile erstellt, als auch Mobilfunktelefonate abgehört oder SMS mitgelesen werden. IMSI steht für *International Mobile Subscriber Identity* und dient der eindeutigen Identifizierung von Netzteilnehmern. Vor der Nutzung einer Mobilfunk-Funktion, wie dem Telefonieren oder Versenden von SMS, muss sich das Mobilgerät an eine Basistation anmelden, wobei die IMSI übermittelt wird.
Ein IMSI-Catcher schaltet sich zwischen Mobiltelefon und Providernetzwerk und simuliert ein Mobilfunknetzwerk. Dadurch werden die Signale der eigentlichen Basisstation überlagert und das Mobilfunknetzwerk des IMSI-Catchers fälschlicherweise für das der Basisstation gehalten. Somit können alle übertragenen Mobilfunkdaten vom IMSI-Catcher abgefangen werden. [Kuk14]

Der Einsatz von IMSI-Catchern stieg bei der Bundespolizei im zweiten Halbjahr von 19 im Jahr 2016 auf 61 im Folgejahr. [Mon18]

Diese Beispiele zeigen, dass bei einem mobilen Gerät weitaus mehr Möglichkeiten und eine größere Datenmenge entstehen, die von unterschiedlichen Interessenten abgefangen werden können.

3.7 Weitere Methoden der Datenerhebung

Abgesehen von den hier aufgeführten Methoden zur Datengewinnung gibt es noch andere Möglichkeiten der Informationsgewinnung.
Beispielsweise besteht die Gefahr, dass bei der Nutzung von Web Real-Time Communication (WebRTC) trotz der Verwendung eines Virtual Private Networks die IP-Adresse des Anwenders mittels JavaScript ausgelesen werden kann. [WS17]
Internet-Provider dagegen haben auch ohne Tracking Zugriff auf die IP-Adresse des Nutzers und können protokollieren zu welcher Zeit, welcher Computer, welche Webseite aufgerufen hat. Ebenso verfügen E-Mail-, VPN- und Proxy-Provider über sensible Daten ihrer Anwender. [Hei15, Los15]
Aufwändiger dagegen sind Verkehrsflussanalysen, bei denen ebenfalls wertvolle Informationen gewonnen werden können. Dabei werden entweder unverschlüsselte Metadaten ausgewertet, wie die Adressen von Absender und Empfänger oder verschlüsselte Daten. Bei letzteren können Anzahl und Größe der übertragenen Pakete analysiert und daraus Rückschlüsse gewonnen werden. [Pet17]

3.8 Zusammenfassung

In diesem Kapitel wurde gezeigt, dass die Erhebung von Nutzerdaten auf Grundlage unterschiedlichster Technologien erfolgt, die auch in Kombination eingesetzt werden. Mit Cookies, eTags und Fingerprintig werden Nutzer identifiziert und deren Aktivität über mehrere Webseitenaufrufe und Browser-Sitzungen hinweg verfolgt. Diese Verfahren ermöglichen eine Wiedererkennung des Nutzers im Internet. Wie in *Abschnitt 3.2* dargestellt wurde, sind insbesondere Evercookies schwer zu kontrollieren, da bei diesen bis zu 13 verschiedene Technologien kombiniert eingesetzt werden, um Cookies redundant auf dem Nutzer-Rechner zu speichern. Zum Löschen müssen

entsprechend alle betroffenen Speicherbereiche gelöscht werden. Wird ein Speicherbereich ausgelassen, kann sich das Evercookie erneut erstellen.
Durch Third-Party Cookies und das Cookie Syncing haben Drittanbieter (wie Werbedienstleister) Zugriff auf die Nutzerdaten bzw. tauschen diese untereinander aus. Die Erfassung und Weitergabe der Daten ist für den Nutzer in aller Regel nicht ersichtlich.
Beim Fingerprinting, das in *Abschnitt 3.4* betrachtet wurde, werden unterschiedliche Merkmale, wie Hard- und Softwareparameter, aber auch Rendering-Merkmale, ausgelesen und zur eindeutigen Identifikation des Nutzers verwendet. Aufgrund der so gewonnenen Informationen kann eine eindeutig identifizierbare Nummernfolge - der Fingerprint - erstellt und zur Identifikation des Nutzers verwendet werden.

Das Verfahren des Ultraschall-Trackings wurde in *Abschnitt 3.5* beschrieben. Es ermöglicht eine Zuordnung unterschiedlicher Geräte zu einem Nutzer (Cross-Device-Tracking), kann aber auch für Location-Based-Marketing genutzt werden. Dabei kann abhängig vom Standort bzw. dem aufgesuchten Geschäft des Nutzers, entsprechende Werbung eingeblendet werden. Bei diesem Verfahren werden Beacons in Geschäften, TV-Werbung oder YouTube-Videos ausgesendet, die von bestimmten Apps auf mobilen Geräten empfangen werden können. Daraufhin können wiederum an den Sender des Beacons, Informationen über den jeweiligen Nutzer übertragen werden.

Staatliche Einrichtungen nutzen die in *Abschnitt 3.1* beschriebenen Hintertüren und Schwachstellen, um die Integrität von IT-Systemen zu kompromittieren oder um Sicherheitsmechanismen zu unterlaufen. In den USA sind Telekommunikationsunternehmen durch CALEA dazu verpflichtet, innerhalb ihrer Systeme Schnittstellen zu integrieren, worüber Behörden Zugriff auf Inhalts- und Metadaten erhalten können. Durch die Zusammenarbeit mit den neun größten Internet- und Kommunikationsunternehmen im Projekt PRISM, hat die NSA die Möglichkeit, digitale Kommunikation von Personen weltweit zu überwachen. Dabei kann sowohl auf gespeicherte Daten, als auch auf Kommunikation in Echtzeit zugegriffen werden.
Im Rahmen von Tempora greift der britische Geheimdienst GCHQ auf 200 Glasfaserkabel zu, die der Datenübertragung zwischen Europa und den USA dienen.
In Deutschland nutzt ZITiS Schwachstellen in Hard- und Software, um Trojaner zu installieren bzw. Mechanismen zur Verschlüsselung zu umgehen. Ziel ist dabei unter anderem, verschlüsselte Kommunikation von Instant-Messengern mitlesen zu können.

Besonders anfällig für das Nutzer-Tracking sind mobile Geräte. In *Abschnitt 3.6* wurden dafür unterschiedliche Gründe dargestellt. Mobile Geräte sind permanente Begleiter der Menschen und auf ihnen wird eine große Menge unterschiedlicher Daten verarbeitet. Auf diese Daten haben die Anbieter der installierten Apps, die Mobilfunk-Netzbetreiber, aber auch Plattform- bzw. App-Store-Betreiber Zugriff. Bei vielen Android Apps werden Daten auch an Dritte übertragen. Zudem fordern einige Apps bereits bei der Installation umfangreichere Berechtigungen, als für die Erfüllung ihrer Funktion erforderlich ist.
Die Ortung und Erstellung eines Bewegungsprofils ist bei einem mobilen Gerät sowohl über die WLAN- bzw. Bluetooth-Funktion möglich, als auch über Funkzellenabfragen oder stille SMS. Beim Einsatz von IMSI-Catcher können zudem Telefonate abgehört und SMS mitgelesen werden.

Häufig haben Verbraucher keine Kenntnis über das Ausmaß des Trackings und die dabei eingesetzten Methoden. Darüber hinaus ist für die Nutzer nicht erkennbar, welche Parteien Zugriff auf ihre Daten erhalten, wohin die Daten fließen und was mit ihnen passiert. Wie die gewonnenen Daten zur Nutzerprofilierung verwendet werden, wird in *Kapitel 4* betrachtet. Mögliche Maßnahmen, mit denen man sich vor diesen Methoden der Datenerhebung schützen kann, sind in *Kapitel 5 Empfehlungen zum digitalen Selbstschutz* beschrieben.

4 Nutzerprofilierung

In diesem Kapitel wird thematisiert, zu welchem Zweck unterschiedliche Einrichtungen Daten sammeln bzw. auswerten. Dazu werden zunächst einführende Beispiele genannt, die verdeutlichen sollen, welche Informationen bereits unterschiedlichen Daten entnommen werden können, dazu gehören auch vorhersagende Prognosen, sogenannte *Predictive Analytics*. Methoden der Privatwirtschaft als auch von staatlichen Einrichtungen werden daraufhin beispielhaft in den jeweiligen Unterkapiteln betrachtet.

Ein Beispiel für *Predictive Analytics* ist die Prognose zu zukünftigen Aufenthaltsorten von Smartphone-Nutzern. Dabei werden Daten von Smartphones ausgewertet, um den Aufenthaltsort des Nutzers für ein Zeitfenster von 24 Stunden vorhersagen zu können. Die Prognosen basieren auf zurückliegenden Informationen wie GPS- und WLAN-Protokollen, Anruf- und SMS-Listen.
Im Rahmen einer britischen Studie konnte der zukünftige Aufenthaltsort umso genauer vorhergesagt werden, je mehr Daten berücksichtigt wurden. Wurden ausschließlich die Daten der einzelnen Teilnehmer ausgewertet, lag der durchschnittliche Fehler bei 1000 Metern. Flossen zudem die Interaktionen zwischen Teilnehmern in die Auswertung mit ein, konnte der durchschnittliche Fehler auf 20 Meter reduziert werden. Bei der Studie wurde darüber hinaus die Erkenntnis gewonnen, dass unter Berücksichtigung sozialer Netzwerke bei der Analyse von Verhaltensmustern die abgeleiteten Prognosen hochgradig zuverlässiger wurden. [Chr14]

Eine belgische Studie befasst sich mit der Analyse von Tastatureingaben. Dabei wurden emotionale Zustände eines Computer-Nutzers aus dem Rhythmus und der Dynamik von Tastatureingaben abgeleitet. Sowohl die Zeitpunkte des Drückens und Loslassens der Tasten, inhaltliche Variablen, wie die Anzahl der gemachten Fehler (Verwendung von Backspace- und Delete-Taste), aber auch der prozentuale Anteil von Sonderzeichen, wie Ziffern, Interpunktion, etc. wurden dabei ausgewertet. Die

Zuverlässigkeit der prognostizierten Gemütszustände anhand der analysierten Tastatureingaben sind in *Tabelle 1* gelistet. [Chr14]

Gemütszustand	**Prognosezuverlässigkeit**
Zuversicht	83%
Unschlüssigkeit	82%
Nervosität	83%
Entspannung	77%
Trauer	88%
Müdigkeit	84%

Tabelle 1: Prognostizierte Gemütszustände durch Analyse von Tastatureingaben

Die Forscher Andrew Reece und Christopher Danforth haben eine Software zur Bildanalyse entwickelt, die mit einer Zuverlässigkeit von bis zu 70% typische Depressionsmerkmale erkennen kann. Dabei wurden über drei Jahre hinweg 43.000 Fotos von 166 Instagram-Nutzern analysiert, wobei die Metadaten und Informationen, die über Gesichtserkennung und Farbanalyse entnommen werden konnten, ausgewertet wurden.
Die Studie zeigt, dass depressive Menschen häufiger dunkle, graue oder Schwarz-Weiß-Aufnahmen veröffentlichen. Zudem bilden ihre Fotos seltener Gesichter ab, bzw. Fotos auf denen nur ein Gesicht abgebildet ist (im Gegensatz zu solchen, die mehrere zeigen). Außerdem würden laut Reece und Danforth Menschen, die unter Depressionen leiden, generell häufiger Bilder posten und am liebsten den Instagram-Filter *Inkwell* verwenden, durch den eine Farbaufnahme in ein Schwarz-Weiß-Bild umwandelt wird. Aufgrund solcher Merkmale sei es möglich, psychisch auffällige Menschen anhand ihrer veröffentlichten Bilder zu erkennen.
Nach Aussage von Danforth könnte die Software dazu eingesetzt werden, Menschen zu helfen, bei denen die Krankheit bislang nicht diagnostiziert worden sei, oder die sich in einem frühen Stadium der Krankheit befänden. [RD17, Spi17a]

4.1 Privatwirtschaft

Internetkonzerne haben bei der Nutzerprofilierung meist das Ziel, personalisierte Werbung anzeigen zu können. Im Online-Handel sind dabei auch Preis- und Suchdiskriminierung gängige Praxis. Bei der Preisdiskriminierung wird verschiedenen potenziellen Käufern das gleiche Produkt zu unterschiedlichen Preisen ange-

boten. Dagegen werden bestimmten Nutzern bei der Suchdiskriminierung in einer Produktkategorie teurere Suchergebnisse angeboten. Beispielsweise hat das Online-Reisebuchungsportal Orbitz bestätigt, dass sie Mac-Nutzern im Rahmen von Experimenten um durchschnittlich 11% teurere Hotels angeboten habe, als Nutzern von anderen Computer-Herstellern. Aber auch Faktoren wie der Standort des Nutzers haben Einfluss auf die Filterung der Suchergebnisse. So gibt es beim US-Bürobedarfshändler Staples eine durchschnittliche Preisdifferenz von 8%, die sich in Abhängigkeit vom Standort des Nutzers ergibt. [Chr14]

Häufig werden Informationen über einen Nutzer, die beim Besuch einer Webseite anfallen, an dritte Parteien weitergegeben. Dies hat bereits eine Untersuchung aus dem Jahr 2014 ergeben. Dabei wurde festgestellt, dass beim Aufruf deutscher Nachrichten-Webseiten die Nutzerdaten an bis zu 59 externe Services übertragen wurden (siehe *Tabelle 2*). Dazu waren bei den Webseiten Code-Fragmente, wie Zählpixel, Web Beacons oder Web Bugs, eingebunden. [Chr14]

Webseite	**Anzahl externer Services**
Die Welt	59
Bild	44
Spiegel	33
Heise Online	19
Süddeutsche	47
Zeit Online	37
FAZ	55
Tagesspiegel	37
Tagesschau	4

Tabelle 2: Weitergabe von Nutzerdaten an externe Services

Solche Drittunternehmen, an welche die Daten der Webseitenbesucher übertragen werden, sind in der Regel Werbenetzwerke oder Analytics-Dienste. Beispielsweise sind Google und zugehörige Services wie *Google Analytics* oder die Werbenetzwerke wie *DoubleClick* und *AdMob* nahezu auf jeder Website eingebunden. Facebook ist überall dort eingebunden, wo ein Facebook-Like-Button integriert ist.
Der Anbieter segment.io wirbt damit, dass durch Einbau des angebotenen Service in Webseiten oder Apps die Daten der Nutzer automatisiert an über 100 andere Dritt-Unternehmen weitergeleitet werden können, ohne dass dies für Nutzer in irgendeiner Weise erkennbar oder nachvollziehbar sei. [Chr14]

Nicht nur zu Werbezwecken besteht Interesse an Nutzerdaten, sondern auch bei der Beurteilung von Angestellten befassen sich Unternehmen mit Analysemöglichkeiten und haben dafür zum Teil spezielle Analytics-Abteilungen. Beispielsweise bewertet das Unternehmen Royal Dutch Shell das Potenzial seiner Bewerber und Angestellten anhand eines Videospiels. Dabei wird jede Spielinteraktion detailliert aufgezeichnet und ausgewertet. Die Rohdaten werden mit anderen Daten abgeglichen und nach Mustern durchsucht. Als Resultat erhält das Unternehmen sowohl Bewertungen über das kreative Potenzial, das Durchhaltevermögen, die Lernkapazität und die soziale Intelligenz des Angestellten bzw. des Bewerbers, als auch über seinen Charakter und seine Fähigkeit aus Fehlern zu lernen. [Chr14]

In den folgenden Unterkapiteln werden beispielhaft Unternehmen genannt, die sich unter anderem auf die Analyse von Daten spezialisiert haben.

4.1.1 Flurry

Das Unternehmen Flurry betreibt ein Analyse- und Werbesystem, das umfangreiche Informationen über das Verhalten von Smartphone-Nutzern sammelt. Flurry bietet das System App-Herstellern an, die damit ihre Nutzer analysieren und zielgerichtete Werbung schalten können. Flurry wird laut Eigenangabe in 540.000 Apps auf iOS, Android und anderen Plattformen genutzt und wirbt damit, ein Drittel der globalen App-Aktivität zu vermessen und Zugriff auf durchschnittlich 7 Apps auf über 90% aller Endgeräte weltweit zu besitzen. Dabei werden Nutzer über Apps und Geräte hinweg wiedererkannt. Mit den gesammelten Daten könne ein „*reichhaltiges Bild über die Interessen einer Person*“ gewonnen werden. Flurry, [Chr14, S.66]
Die Plattform bietet zudem diverse Segmentierungsmöglichkeiten, wie das gezielte Ansprechen von Nutzern nach Kriterien wie Interessen, Geschlecht, Alter, Sprache, Gerät, Betriebssystem – und nach sogenannten Personas wie Hardcore-Gamern, Finanz-Geeks, Slots Players oder sexueller Orientierung. [Chr14]

4.1.2 Narus

Ein weiteres Unternehmen, das auf Netzwerk- und Datenanalyse spezialisiert ist, heißt Narus. Deren Produkt nSystem ist ein selbstlernendes System, bei dem Datenmengen automatisiert durchsucht und analysiert werden. Dabei können Daten

einer Tiefenanalyse unterzogen werden und nach Themen, Trends, Communities und Standorten ausgewertet werden. Bei den Analysen sollen alle Internetnutzer sichtbar gemacht werden können und anhand ihres digitalen Fingerabdrucks (siehe *Abschnitt 3.4*) identifiziert werden.
Narus ist ein strategischer Partner der NSA bei Überwachungsaktivitäten und nSystem ist in seinen Funktionen dem NSA Programm *XKeyscore* sehr ähnlich. [Sch14a]

4.1.3 Google

> „*Wer sucht wird zum Zulieferer. Wer kauft, zum Produkt.*“
> Frank Schirrmacher, [Fri15, S.13]

Persönliche Daten sind Rohstoffe mit einer enormen Wirtschaftskraft. Das lässt sich nicht zuletzt daran erkennen, dass Alphabet Inc. (ehemals Google LLC) mit einem Aktienkurs von 902€ (Stand: 27.10.2017) zu den wertvollsten Unternehmen der Welt gehört. Google verfügt über zahlreiche Nutzerdaten und versteht es, finanziellen Profit aus diesen Daten zu erzielen. Dabei wird die riesige Datenmenge des Internets geordnet, systematisiert und durchsucht. Je mehr Wissen über einen Nutzer verfügbar ist, desto zielgerichteter kann Werbung geschaltet werden. [BÖ17, Fri15]

Mehr als 87% (Stand: September 2017) aller Suchmaschinennutzer verwenden ausschließlich Google für Recherchen im Internet. Dabei werden auch intime Informationen gegenüber der Suchmaschine offenbart, da sie auch dann eingesetzt wird, wenn es um Krankheit, Scheidung, sexuelle Orientierung oder finanzielle und berufliche Probleme geht. All diese Suchanfragen werden von Google gespeichert. Darüber hinaus verfügt Google über eine Vielzahl weiterer Informationen von seinen Nutzern, wie deren Wohnort, Interessen oder Produkte für die sie sich interessieren. [Fri15, Sta17]

> „*Aufgrund der Informationen, die Google über dich gesammelt hat, wissen wir grob, wer du bist, wissen ungefähr, was dich interessiert, wissen annäherungsweise, wer deine Freunde sind. Google weiß auch, bis auf wenige Meter genau, wo du gerade bist.*“ Eric Schmidt, [Fri15, S.158]

Allein aus den Suchanfragen können detaillierte persönliche Profile erstellt werden, woraufhin dem Nutzer personalisierte Werbung eingeblendet oder Ergebnisse bei der

Nutzung von Suchmaschinen individuell angepasst werden können. Allerdings werden aufgrund dieser Nutzerprofile auch Prognosen bezüglich der Kreditwürdigkeit oder dem Gesundheitszustand eines Nutzers erstellt. Als Konsequenz könnten diese für Nutzer beispielsweise höhere Zinsen für einen Kredite oder die Ablehnung von einer Krankenkasse bedeuten. [Fri15]

Ferner müssten Google-Nutzer gegebenenfalls höhere Preise für Produkte bezahlen. So sagt Gabriel Weinberg, Gründer der Suchmaschine DuckDuckGo, dass über die Einschätzung der finanziellen Situation von Nutzern festgestellt werden kann, wie wichtig ihnen ein bestimmtes Produkt ist. Der Preis kann anhand von Suchanfragen, Kalenderinhalten und E-Mails angepasst werden. Beispielsweise könnten so überhöhte Preise bei Besserverdienenden durchgesetzt werden. [Fri15]

4.2 Staatliche Einrichtungen

Ebenso wie Internetkonzerne haben auch staatliche Einrichtungen Interesse an der Sammlung und Analyse von Daten. Als Argument dafür wird der Kampf gegen den Terrorismus und die Aufrechterhaltung der Sicherheit genannt. So kommt *Predictive Analytics* beispielsweise im Rahmen von *Predictive Policing* (vorhersagende Polizeiarbeit) zum Einsatz. Dabei wird versucht, umfassende Beobachtungen des alltäglichen Verhaltens dafür zu nutzen, um Straftaten bereits im Vorfeld zu erkennen und zu verhindern. 2010 startete das Los Angeles Police Department dazu einen Modellversuch, wobei in anderen amerikanischen Städten bereits ähnliche Modelle zum Einsatz kommen. Dabei wird eine anlasslose, permanente, in Echtzeit durchgeführte Rasterfahndung eingesetzt, die nicht auf eine Personengruppe beschränkt ist. [Sch14a]
Beispielsweise hat das Los Angeles Police Department (LAPD) zum Zweck von vorhersagenden Prognosen die computergestützte Polizeiarbeit massiv ausgebaut. Ein wesentliches Element dabei sind die sogenannten *Field Interview Cards*. Dabei handelt es sich um Karteikarten, die ein Beamter bei jeder Interaktion mit einem Bürger ausfüllt. Mit diesen Karten werden zum einen allgemeine Angaben zu Name, Geburtstag, Telefonnummer, Adresse, Alter und Kleidung festgehalten, aber auch weitere Informationen, wie Spitznamen, Sozialversicherungsnummer, Bewährungsstatus, Gangmitgliedschaften, Angaben zu Begleitpersonen und Fahrzeug (inklusive Schäden, Aufklebern oder besonderer Ausstattung) gesammelt. Weitere Informationen

werden aus automatischen Nummerschild-Lesern und den Kameras im öffentlichen Raum gewonnen. Smartphones werden über Digital-Receiver-Boxen automatisch registriert und dabei die mobile Kommunikation erfasst. Der Einsatz von Drohnen wird aktuell noch erprobt. Auch am Kauf von Kommunikationsdaten bei Datenhändlern zeigen die Behörden Interesse. Dazu gehören beispielsweise angerufene Telefonnummern, Daten aus sozialen Netzwerken oder von Gesundheitsdiensten.
Aufgrund der gesammelten Daten soll vorhergesagt werden, wo Einbrüche oder Überfälle stattfinden könnten. An diesen Orten werden dann vermehrt Beamte eingesetzt. Darüber hinaus werden aus den Daten auch Listen von verdächtigen Personen erstellt, die zukünftig Straftaten begehen könnten. Um auf eine solche Liste aufgenommen zu werden, muss man jedoch nicht selbst auffällig geworden sein; der Umgang mit den falschen Freunden kann dafür bereits ausreichen. [Kar18]

Neben der vorhersagenden Polizeiarbeit wird in den USA auch die Gefährlichkeit wiederholt straffällig gewordener Personen von einer Software ermittelt. In den Bundesstaaten Arizona, Colorado, Delaware, Kentucky, Oklahoma, Virginia, Washington und Wisconsin wird eine Software Namens COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) eingesetzt. Diese soll das Risikopotential und die kriminelle Energie der befragten Personen vorhersagen. Dabei haben die Betroffenen über 130 Fragen zu beantworten. Diese umfassen z. B. Themen über den familiären Hintergrund, Ausbildung, soziale Stellung, kriminelle Handlungen oder Substanzmissbrauch. Der Software liege die Annahme zugrunde, dass aus sieben Kriterien, die Wahrscheinlichkeit ermittelt werden kann, mit der ein Mensch zukünftig kriminelle Handlungen begehen wird. Kriterien bezüglich der Kriminalität von männlichen Personen sind:

- Probleme in Ausbildung, Arbeit und Finanzen
- Antisoziale Glaubens- und Verhaltensweisen
- Antisoziales und prokriminelles Umfeld sowie Isolation
- Temperament und Selbstkontrollschwäche
- Vernachlässigung familiärer Beziehungen
- Alkohol- und anderer Drogenmissbrauch
- Von der Norm abweichende Sexualität und Erregbarkeit.

Bei jedem männlichen Befragten wird anhand seiner Antworten bezüglich dieser sieben Kriterien ein Wert zwischen 1 und 10 und damit das Maß seiner evtl. Gefährdung kriminell zu werden zugeteilt. Wie die Werte genau berechnet werden, ist nicht bekannt. Die Prognosen fließen unter anderem in Gerichtsentscheidungen ein, die eine etwaige vorzeitige Haftentlassung oder die Festlegung der Höhe von Kautionszahlungen betreffen. [Hil17]

Bei Polizeibehörden in Deutschland liegt der Fokus von *Predictive Policing* aktuell noch auf Wohnungseinbrüchen. So laufen bzw. liefen in Berlin, Baden-Württemberg, Hessen, Niedersachsen und Nordrhein-Westfalen Pilotprojekte; in Brandenburg und Hamburg werden bzw. wurden dazu Studien durchgeführt; in Bayern wird bereits mit *Predictive Policing* gearbeitet und die Einsatzmöglichkeiten sollen ausgeweitet werden. [Hei17]

Wie in *Abschnitt 3.1* beschrieben, sammelt die NSA unter anderem mit PRISM eine große Menge Daten. Für die Auswertung dieser Daten ist ein weiteres Instrument erforderlich: *XKeyscore*. Dieses Programm wurde neben der NSA auch vom Bundesnachrichtendienst und dem Bundesamt für Verfassungsschutz eingesetzt. Beim BfV lief das System allerdings unter dem Namen *Poseidon*.
Mit *XKeyscore* können sowohl Meta- als auch Inhaltsdaten von Chats, E-Mails, (Webcam-) Fotos, Dokumenten, Suchmaschineneingaben und anderen Internetaktivitäten personenspezifisch durchsucht und ausgewertet werden. Dazu werden die gespeicherten Daten zunächst nach hierarchischen Verzeichnisstrukturen mit Schlagworten versehen, z. B. ob es sich um eine E-Mail handelt, von welchem E-Mail-Provider sie stammt oder ob sie mit PGP-verschlüsselt wurde. Daraufhin kann die entsprechende Behörde auf Grundlage unterschiedlichster Suchkriterien die für sie interessanten Daten aus den Datenmassen herausfiltern. Dabei sind Suchanfragen nach einzelnen Begriffen, aber auch komplexe Anfragen möglich, bei denen sowohl die Meta- als auch Inhaltsdaten durchsucht werden können. Beispielsweise können alle Verbindungen angezeigt werden, die zu einer bestimmten IP-Adresse oder Telefonnummer gehören.
Die Auswertung der Daten kann auch in Echtzeit erfolgen, sofern auf den zu überwachenden IT-Systemen Software für diesen Zweck installiert ist. [Bie15, Bis15]

Die Wiedererkennung eines Nutzers ist über Identifikatoren möglich. Dazu kann zum Beispiel die IP-Adresse des Nutzers verwendet oder auf Cookies von kommerziellen Anbietern zugegriffen werden, bei denen dem Nutzer zur Wiedererkennung eine ein-

deutige Zeichenkette zuweisen wird.
Darüber hinaus kann aus charakteristischen Merkmalen in den Daten ein Fingerabdruck des Nutzers erstellt werden, ähnlich wie in *Abschnitt 3.4* beschrieben. Das heißt, dass beispielsweise wiederkehrende Ortsangaben, bestimmte Kommunikationsmerkmale oder die Nutzung spezieller Programme dazu dienen, um ein Verhaltensprofil von einer Person zu entwickeln. Dieses Profil kann das Programm dann in neuen Daten wiederfinden und die Person dadurch identifizieren, selbst wenn kein Name oder ein Identifikator in den Daten enthalten ist. [Bie15, Bis15]
Dieses Verfahren zur Wiedererkennung von Nutzern wird unter anderem dann eingesetzt, wenn die betroffenen Computer über ein VPN (Virtual Private Network) verbunden sind. Aus Schulungsunterlagen zu *XKeyscore* ging hervor, dass die NSA Wert darauf legt, Computer zu identifizieren, die mit einem VPN verbunden sind. *XKeyscore* kann demnach solche Computer lokalisieren und auf der Grundlagen von Fingerprints, also den Eigenschaften der IT-Systeme, die Computer identifizieren, überwachen und infiltrieren. [Sch14a]

4.3 Zusammenfassung

Sowohl staatliche Einrichtungen als auch Unternehmen haben großes Interesse daran, Daten von Bürgern bzw. Verbrauchern zu sammeln und daraus Prognosen zu erstellen. Staatliche Einrichtungen nennen für diese Praktiken als Argument, dass diese der Sicherheit des Staates und deren Bürgern dienen würden und als Schutzmaßnahme gegen den Terrorismus erforderlich seien. Bei Unternehmen aus der Privatwirtschaft hingegen ist das Ziel in der Regel finanzieller Art, z. B. durch das Anzeigen von personalisierter Werbung.

Wie in diesem Kapitel gezeigt wurde, geben die gesammelten Daten Auskunft über Charaktereigenschaften, das soziale Umfeld, die finanzielle Situation, die Gewohnheiten oder die psychische und physische Verfassung von Menschen.
So zeigen Studien, dass der zukünftige Aufenthaltsort von Smartphone-Nutzern mit einer Abweichung von 20 Metern vorhergesagt werden kann. Auch der emotionale Zustand eines Nutzers kann von der Art und Weise seiner Tastatureingaben abgeleitet werden. Ebenso kann anhand veröffentlichter Bilder, eine Depression mit einer Zuverlässigkeit von bis zu 70% erkannt werden.

Nutzerdaten, über die Unternehmen aus der Privatwirtschaft verfügen, werden wie in *Abschnitt 4.1* aufgeführt, unter anderem zur Preis- und Suchdiskriminierung genutzt. Häufig werden Informationen, die ein Nutzer beim Besuch einer Webseite hinterlässt, automatisiert an Dritte weitergegeben. Darüber hinaus werden Analytics-Abteilungen eingesetzt, um Aussagen zum Durchhaltevermögen, der Lernkapazität oder der sozialen Intelligenz von Angestellten oder Bewerbern treffen zu können.
Das Analyse- und Werbesystem von Flurry ist auf Smartphones ausgerichtet; Narus dagegen ist ein Unternehmen, das auf Netzwerk- und Datenanalyse spezialisiert ist. Google hat die Datenmenge des Internets geordnet, systematisiert und durchsuchbar gemacht. Google gehört zur weltweit meist genutzten Suchmaschine, wodurch dem Unternehmen, das jede Suchanfrage speichert, intime Informationen über seine Nutzer offenbart werden.

Neben der bloßen Erstellung von Nutzerprofilen werden vermehrt Prognosen über zukünftige Verhaltensweisen von Personen getroffen. *Predictive Analytics* wird eingesetzt, um das Konsumverhalten, aber auch Straftaten vorhersagen zu können. Wie in *Abschnitt 4.2* aufgeführt, werden im Rahmen von *Predictive Policing* in den USA bereits Daten gesammelt, auf deren Basis dann der Einsatzort von Beamten, aber auch verdächtige Personen ermittelt werden. In Deutschland wird *Predictive Policing* bislang für Vorhersagen von Wohnungseinbrüchen eingesetzt.
Mit *XKeyscore* besteht für die NSA, den BND, das BfV und andere Behörden die Möglichkeit, beliebige Auswertungen über gesammelte Meta- und Inhaltsdaten durchzuführen. Dabei werden auch Computer identifiziert, die VPNs nutzen, indem zur Wiedererkennung das Fingerprinting eingesetzt wird.

Ein Nutzer kann jedoch Maßnahmen ergreifen, mit denen er die Datenerfassung erschwert und damit seine Privatsphäre schützen kann. Solche Maßnahmen werden in *Kapitel 5 Empfehlungen zum digitalen Selbstschutz* beschrieben.

5 Empfehlungen zum digitalen Selbstschutz

Auf die moderne Informationstechnologie kann nicht mehr verzichtet werden. Dabei werden Nutzerdaten auch zukünftig in erheblichem Umfang verarbeitet, gespeichert und ausgewertet. Es gibt verschiedene Ansätze auf rechtlicher, technischer, wirtschaftlicher und politischer Ebene, die dabei helfen können die Privatsphäre in der digitalen Welt besser zu schützen. [Sch14a]

In diesem Kapitel werden daher konkrete Maßnahmen vorgestellt, wie man als Nutzer seine Daten und entsprechend seine Privatsphäre schützen kann. Allerdings ist ein vollständiger, effektiver Schutz gegen Maßnahmen der Privatwirtschaft und staatliche Einrichtungen, die über enorme Ressourcen verfügen, äußerst unrealistisch. Vielmehr soll eine umfassende Überwachung erschwert und die erfasste Datenmenge reduziert werden.

5.1 Grundlegende Aspekte

Es gibt einige grundlegende Aspekte, die ein Anwender berücksichtigen sollte, um seine Privatsphäre im digitalen Bereich zu schützen. In den folgenden Unterkapiteln werden solche Aspekte und Modelle beschrieben.

5.1.1 Datenvermeidung und Produktauswahl

Ein umsichtiger und verantwortungsvoller Umgang mit den eigenen persönlichen Daten ist Grundvoraussetzung für den Schutz eben dieser. Dazu ist es notwendig,

über Anwendungen und Betriebssysteme informiert zu sein, und dass deren Datenschutzeinstellungen, über die der Zugriff auf Nutzerdaten geregelt wird, verstanden und genutzt werden. Dabei gilt es auch zu berücksichtigen, dass es sich niemals nur um die eigenen Daten handelt, die es zu schützen gilt, sondern um die Daten von allen Personen, über die Informationen gespeichert sind, beispielsweise in digitalen Adressverzeichnissen. [Chr14]

Die eingesetzten Anwendungen und Dienste sollten mit Bedacht ausgewählt werden. Es gibt viele Hinweise, dass Produkte aus China oder den USA gezielt Schwachstellen oder Hintertüren enthalten (siehe *Abschnitt 3.1*). Daher sollte man solche Produkte meiden und auf Systeme zurückgreifen, die Vertraulichkeit und Integrität garantieren. Beispielsweise kann Hard- und Software genutzt werden, die in Deutschland oder innerhalb der EU hergestellt bzw. entwickelt wird. Eine weitere Möglichkeit besteht darin, darauf zu achten seine Daten aus unterschiedlichen Anwendungsbereichen über mehrere Anbieter hinweg zu verteilen und nicht ausschließlich einem einzigen Anbieter anzuvertrauen. [Sch14a]

Aber auch der Ort der Datenverarbeitung ist entscheidend und damit die Frage, wo die Daten gespeichert werden und welcher Rechtsordnung sie demnach unterliegen. Dabei ist sowohl der Server- als auch der Unternehmensstandort entscheidend. Wie bereits in *Kapitel 2* aufgeführt, besteht in der EU, der Schweiz, Kanada, Argentinien, Guernsey und auf der Isle of Man ein angemessenes Datenschutzniveau. [Sch14a]

Eine Umleitung von Daten über Server, die sich in den USA oder in Großbritannien befinden, sollte vermieden werden. Allerdings erfolgt die Wegewahl im Internet aktuell nach den Kriterien Preis, Entfernung und Dienstgüte. Da US-Anbieter in der Regel günstiger sind, werden deren Dienste folglich häufiger genutzt. Laut Peter Schaar könnte die NSA und der GCHQ an willkürlichen Datenzugriffen gehindert werden, indem ein *Schengen-Routing* realisiert werden würde und Telekommunikationsverbindungen nur noch über Netze innerhalb der EU erfolgen würden. [Sch14a]

5.1.2 Transparenz und Open Source

Die Eigenschaft Open Source erfüllt eine Software, deren Quelltext für jeden offen gelegt und frei verfügbar ist. Das heißt, jeder kann den Quellcode lesen, mit ihm arbeiten und ihn verändern. Die exakte Definition der Open Source Initiative

ist an zehn Punkte geknüpft, die unter der Webseite *www.opensource.org/docs/osd* eingesehen werden können. [Die07, Ope07]

Die Transparenz, die durch Open Source gegeben ist, ermöglicht eine Überprüfung der vom Hersteller angegebenen Funktionen und damit eine Evaluierung und Zertifizierung des Quellcodes durch unabhängige Fachleute. [Die]
Bei Software, die nicht Open Source ist, besteht die Möglichkeit, dass Hintertüren enthalten sind, die beispielsweise Verschlüsselungsmechanismen unterlaufen oder dass Schnittstellen integriert sind, über die Daten unerlaubt abgerufen werden können (siehe *Abschnitt 3.1*). Nur durch vollständig einsehbaren Quellcode sinkt die Wahrscheinlichkeit, dass solche Hintertüren und Schwachstellen, aber auch Programmierfehler in der Software enthalten sind. [Wei15]

5.1.3 Verschlüsselung

Unverschlüsselte Nachrichten können generell von jedem, der darauf Zugriff hat, gelesen werden, beispielsweise vom Provider oder von dem Dienstleister einer Anwendung. Mit kryptographischen Verfahren können Daten geheim halten werden, indem sie in eine unleserliche Zeichenfolge, den Geheimtext, umgewandelt werden. Nur ein Berechtigter kann dann mit dem entsprechenden Schlüssel den Geheimtext entschlüsseln. Nachrichten und andere Daten können somit vor unautorisiertem Zugriff geschützt werden. [Beu06, Sch14a]

Generell wird bei der Verschlüsselung zwischen symmetrischen und asymmetrischen Verfahren differenziert. Bei einem **symmetrischen** Verschlüsselungsverfahren erfolgt die Ver- und Entschlüsselung entweder mit demselben Schlüssel oder aber die Schlüssel können auseinander berechnet werden. Die Verschlüsselungsfunktion ist hier in jedem Fall umkehrbar. [Beu06]
Dabei besteht jedoch das Problem des Schlüsselaustauschs, der nicht über einen unsicheren Kanal erfolgen sollte. Ein Lösungsansatz stellt hier der Diffie-Hellman-Schlüsseltausch dar. Auch dabei ist zwar vorab eine ungeschützte Interaktion von Sender und Empfänger erforderlich, jedoch wird dabei nicht der Schlüssel selbst übermittelt. Die Teilnehmer einigen sich dabei lediglich auf zwei Ziffern und senden ihrem Gegenüber jeweils das Ergebnis einer Rechenoperation zu, woraus beide Seiten dann den identischen Schlüssel berechnen können. [Beu06]

Bei einem **asymmetrischen** oder Public-Key-Verfahren werden Schlüsselpaare aus öffentlichem und privatem Schlüssel genutzt. Die Nachricht wird dabei mit dem öffentlichen Schlüssel (Public Key) des Empfängers verschlüsselt und mit dem geheimen oder privaten Schlüssel (Secret Key) des Empfängers entschlüsselt. Dabei ist zwar kein Schlüsselaustausch erforderlich, jedoch muss die Identität des Kommunikationspartners überprüft werden. Dabei kommen Zertifikate zum Einsatz, die bestätigen, dass der Inhaber eines öffentlichen Schlüssels tatsächlich derjenige ist, für den er sich ausgibt. [Beu06, Sch14a]

Der Begriff der **Ende-zu-Ende-Verschlüsselung** beinhaltet, dass die übertragenen Daten über alle Stationen hinweg verschlüsselt sind. Das heißt, die Daten werden beim Sender verschlüsselt und erst beim Empfänger entschlüsselt. [Ele17]

Verschlüsselungen werden heute in den verschiedensten Anwendungsbereichen eingesetzt und es wird empfohlen, solche Dienste zu nutzen, bei denen die Daten verschlüsselt übertragen werden. Instant-Messenger, die Verschlüsselung der Nachrichteninhalte anbieten, werden in *Abschnitt 5.10* betrachtet. Für die Verschlüsselung von E-Mails wird das Mailprogramm Thunderbird in Kombination mit dem Plugin Enigmail und dem Kryptographiesystem GnuPG (GNU Privacy Guard) empfohlen. [Dig16]

Auch die Übertragung der Daten im Internet kann durch das *Hypertext Transfer Protocol Secure* verschlüsselt erfolgen und wird in *Abschnitt 5.3* näher betrachtet.

5.1.4 Mix-Modell

Das Mix-Modell bildet die Grundlage für viele Verfahren, die bei der anonymen Internet-Kommunikation eingesetzt werden, so z. B. auch für die in *Abschnitt 5.2.1 Tor Browser* und *Abschnitt 5.2.2 JonDonym* beschriebenen. Mixes haben zum Ziel, die Kommunikationsbeziehung zwischen Absender und Empfänger von E-Mails geheim zu halten. Wobei die Grundidee darin besteht, eingehende E-Mails zu sammeln und zu einem späteren Zeitpunkt stapelweise zu versenden. Zunächst werden die zu versendenden Nachrichten mit dem öffentlichen Schlüssel des Empfängers und daraufhin mit dem öffentlichen Schlüssel des Mix verschlüsselt. In die Verschlüsselungsfunktion fließt eine Zufallszahl ein, wodurch vermieden wird, dass identische Nachrichten einander zugeordnet werden können.
Durch die Sammelfunktion des Mix kommt es zu einer Zeitverzögerung, weshalb

diese für zeitkritische Dienste nicht geeignet ist. Um Rückschlüsse aufgrund der E-Mail-Größe zu verhindern, sollten die Nachrichten auf Einheitsgrößen aufgefüllt werden, was jedoch mit einem großen Overhead verbunden ist.
Um sich nicht ausschließlich auf die Vertrauenswürdigkeit eines einzelnen Mix-Betreibers verlassen zu müssen, sind Mix-Kaskaden entstanden. Dabei werden mehrere Mixes von unterschiedlichen Betreibern hintereinander geschaltet. Ist mindestens ein Mix davon vertrauenswürdig, bleibt die Kommunikation verborgen. [Pet17]

Zu den Nachteilen zählen sowohl die durch die Kaskaden gesteigerte Zeitverzögerung, der erhöhte Rechenaufwand als auch der große Kommunikations-Overhead. Bei längerer Beobachtung des Netzwerkdatenverkehrs können jedoch trotz der Verwendung von Mixes Korrelationen zwischen der Anwesenheit von Absendern und Empfängern hergestellt werden. Das heißt, dass eine Zuordnung der Kommunikationspartner generell möglich ist und Mixes diesbezüglich keine hundertprozentige Sicherheit gewährleisten können. [Pet17]

5.1.5 Verteilte Systeme, dezentrale Netze

Ein weiterer technischer Ansatz, Massenüberwachung zu erschweren, ist der Verzicht auf zentrale Strukturen und Netzwerke. Bei dezentralen Systemen, wie dem Peer-to-Peer-System, gibt es keinen zentralen Server, auf dem alle Daten zusammenlaufen, sondern viele Server, die z. B. auch von Privatpersonen betrieben werden können. Dadurch ist eine Integration einer Schnittstelle oder das Überwachen des Netzwerkverkehrs an einer zentralen Einheit nicht mehr möglich. [Kat16]
Beispielsweise würden bei einem Mobilfunksystem auf Peer-to-Peer-Basis Daten nicht mehr über Funkmasten und Backbone-Netze übertragen, sondern direkt zwischen den Telefonen der Gesprächsteilnehmer. [Kre16b]
Auch bei der Suchmaschine Yacy besteht das Netz aus Servern, die von Nutzern bereitgestellt werden. Dabei wird der Suchindex nicht zentral gespeichert, sondern jede Yancy-Installation trägt einen Teil zum globalen Index bei. Ebenso werden auch Daten über das Nutzerverhalten an keiner zentralen Stelle gespeichert. [Wei16b]
Eine Twitter-Alternative, die auf einem dezentralen Netzwerk basiert, ist Mastodon. Im Gegensatz zu geschlossenen Systemen, werden den Nutzern bei Mastodon überdies viele Freiheiten und Möglichkeiten zur Mitgestaltung gewährt. [Ber17a]

5.2 Anonymisierungsnetzwerke

Anonymisierungsnetzwerke werden eingesetzt, um Zensurmaßnahmen zu umgehen und die eigene Privatsphäre zu wahren. Dabei werden die eigenen Daten Dritten nicht preisgegeben und die Anzeige personalisierter Werbung umgangen.

5.2.1 Tor Browser

Die gemeinnützige Non-Profit-Organisation *Tor Project*, die ihren Sitz in den USA hat, befasst sich mit Forschung und Entwicklung zum Thema Internetanonymität und Datenschutz. Die Organisation entwickelt unterschiedliche Anwendungen, deren Quellcode öffentlich zugänglich ist. In diesem Kapitel wird die Funktionsweise des Tor Browser im Detail betrachtet, der die zentrale Anwendung der Organisation darstellt. [Los15, Tor17]

Der Tor Browser ist ein Open Source-Projekt, das die anonyme Nutzung des Internets ermöglichen soll. Das Tor-Browser-Bundle enthält sowohl die Tor-Netzwerk-Software als auch den Tor-Webbrowser. Dieser basiert auf Mozilla Firefox ESR (Extended Support Release) und ist somit eine modifizierte Version von Firefox. [Los15, Tor17]

Funktionsweise

Der Tor Browser nutzt das *Onion Routing* (Zwiebelschalen-Routing), um eine sichere Netzwerkverbindung zwischen dem Nutzer und der Ziel-Webseite aufzubauen. Dabei wird der Netzwerkdatenverkehr in mehreren Schichten verschlüsselt, die bei der Datenübertragung dann bei jedem *Tor-Relay* entschlüsselt werden.
Tor-Relays, auch Tor-Knoten oder Zwischensysteme genannt, sind Server, auf denen die Tor-Software installiert ist und die den Datenverkehr des Tor-Clients als Eintritts-, Austritts- oder Transit-Konten weiterleiten, um eine direkte Verbindung zwischen dem Tor-Client und der Ziel-Webseite zu vermeiden. Die Betreiber von Tor-Relays können diese so konfigurieren, dass sie nur als Austritts- oder reine Transitknoten verwendet werden. Ebenso ist es möglich, dass ein Relay, das als Austrittsknoten eingerichtet ist, auch als Transitknoten agiert. [Los15]

Um den detaillierten Ablauf darlegen zu können, werden nachstehend zunächst die Bestandteile des Tor-Protokolls genannt und erläutert:

Tor-Client: Sowohl das System, auf dem die Software installiert ist, als auch die Software selbst, wird als Tor-Client bezeichnet. Er nimmt die Verbindung zum Tor-Netzwerk auf.

Tor-Verzeichnisdienst: Verzeichnisdienste entsprechen Servern, die Informationen über aktive Tor-Relays und deren Anforderungen in einer Datenbank pflegen und bereitstellen.

Tor-Eintrittsknoten: Ein Eintrittsknoten nimmt den Netzwerkdatenverkehr von einem Tor-Client entgegen und leitet ihn an einen anderen Tor-Knoten weiter. Dabei handelt es sich um einen beliebigen Typ eines Tor-Relays (Austritts-, Transit- oder Bridge-Knoten).

Tor-Transitknoten: Ein Transitknoten nimmt den Datenverkehr von einem Tor-Knoten entgegen und leitet ihn an einen anderen Tor-Knoten weiter.

Tor-Austrittsknoten: Ein Austrittsknoten nimmt den Netzdatenverkehr von einem Tor-Knoten entgegen und leitet ihn aus dem Tor-Netzwerk an den gewünschten Ziel-Webserver im öffentlichen Datenverkehr. Er stellt also die Verbindung zu dem gewünschten Webserver her und fungiert als dessen Proxy.

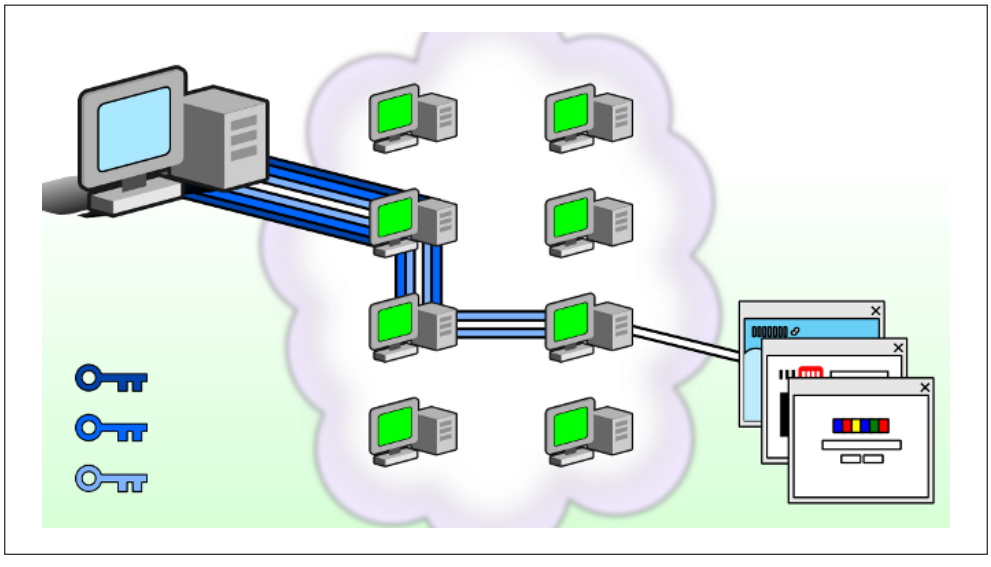

Abbildung 3: Tor Verbindungen [Tor03]

Die Verbindung über das Tor-Netzwerk und die Verschlüsselung der Daten ist in *Abb. 3 Tor Verbindungen* dargestellt.
Bei einem Verbindungsaufbau mit dem Tor-Netzwerk wählt der Tor-Client mit Hilfe des Tor-Verzeichnisservers einen zufälligen Pfad über drei Tor-Relays innerhalb des Tor-Netzwerks, zu denen gestaffelt verschlüsselte Tunnel erstellt werden.
Anschließend werden die Daten dreifach verschlüsselt. Zuerst mit dem Schlüssel des entsprechenden Austrittsknotens, dann mit dem Schlüssel des Transitknotens und zuletzt mit dem Schlüssel des Eintrittsknotens. Nach dieser Dreifachverschlüsselung können die Daten über einen sicheren Tunnel versendet werden.
Der Tor-Client sendet das Datenpaket zum Eintrittsknoten, wo es entschlüsselt und an den Transitknoten weitergeleitet wird. Dort wird das Paket wiederum entschlüsselt und an den Austrittsknoten geleitet, wo das Paket ein letztes Mal entschlüsselt und an das eigentliche Ziel übertragen wird.
Die Verschlüsselungsschichten werden wie Zwiebelschalen abgezogen, daher der Begriff *Onion Routing*. [Los15]

Der Tor-Client hat lediglich ein direkte Verbindung zu dem Tor-Eintrittsknoten (zum Senden und Empfangen der Daten) und dem Tor-Verzeichnisserver (um die Tor-Relays zu ermitteln). Da der Datenverkehr verschlüsselt wird, kennt der Eintrittsknoten nur die IP-Adresse des Clients.
Der zweite Transitknoten kennt weder die Quelle noch das Ziel, sondern nur den Ein- und Austrittsknoten.
Der Austrittsknoten kennt als einziger Knoten das Ziel und hat Zugriff auf die Daten, welche vom oder zum Ziel gesendet werden.
Das Ergebnis ist eine Kommunikationsverbindung, bei der kein Zusammenhang zwischen dem Client und dem angesprochenen Ziel-Server erkennbar ist. [Los15]

Da die aufgerufene Seite nicht in direktem Zusammenhang zu dem Client steht, können Nutzer surfen, ohne persönliche Informationen, insbesondere die IP-Adresse und den Standort, preiszugeben. Beim ausgehenden Datenverkehr sieht es so aus, als würden diese vom Austrittsknoten stammen, beim eingehenden Datenverkehr, scheint es so, als käme er vom Eintrittsknoten. [Los15]

Einschränkungen (der Anonymität)

Der Tor-Browser kann jedoch keine absolute Sicherheit gewährleisten. Wird beispielsweise das Netzwerk der Zielwebseite überwacht, kann der Klartext der Websitzung mitgelesen werden, da die Verbindung vom Austrittsknoten zur Zielwebseite nicht verschlüsselt ist. Die IP-Adresse bleibt dabei zwar verborgen, es wird aber empfohlen zusätzlich HTTPS (siehe *Abschnitt 5.3*) bzw. das Browser Add-on HTTPS Everywhere zu verwenden. [Los15]

Mit Software zur Netzwerküberwachung kann der Tor-Client als Benutzer des Tor-Netzwerks erkannt werden. Wenn man dies umgehen möchte, können zusätzlich Tor-Bridge-Relays verwendet werden, diese sind nicht öffentlich und nur schwer zu entdecken. [Los15]

Tor bietet auch dann keine Sicherheit, wenn ein Computer gehackt wurde und Software oder Hardware installiert wurde, die Tastatureingaben aufzeichnet (Keylogging) und weiterleitet. [Los15]

Um die Anonymität zu wahren, sollten bei bestehender Internetverbindung keine Dokumente geöffnet werden, die mit dem Tor-Browser heruntergeladen wurden. Es kann sein, dass diese Dokumente einen Weblink enthalten, wodurch beim Öffnen des Dokuments der Webinhalt heruntergeladen wird und der Besitzer des Weblinks so die IP-Adresse des Tor-Clients erfährt.
Ebenso sollte der Tor-Browser nicht für solche Dienste verwendet werden, bei denen man sich mit einem Account einloggen muss, der Rückschlüsse auf die eigene Identität zulässt.
Da über einige Browser-Plugins, wie dem Flash-Player, die IP-Adresse des Tor-Clients preisgegeben werden kann und diese Schwachstellen oder Malware enthalten können, wird empfohlen keine Plugins im Tor-Browser zu installieren. [Los15]

5.2.2 JonDonym

Der Anonymisierungsdienst JonDonym basiert auf der AN.ON-Software, die von einem Team der TU-Dresden entwickelt wurde. Sie dient zum Selbstschutz gegen Datensammler und Angreifer, die den gesamten Datenverkehr eines Netzwerkes abhören.
Die Verbindung wird, ähnlich wie beim Tor-Browser, nicht direkt zum Webserver

aufgebaut, sondern über eine sogenannte *Mix-Kaskade*. Wie bereits in *Abschnitt 5.1.4* erwähnt, werden bei Mix-Kaskaden mehrere Mixes von unterschiedlichen Betreibern hintereinander geschaltet. Bei der AN.ON-Software besteht eine Kaskade aus zwei bis drei Mix-Servern, die von zertifizierten Mix-Betreibern bereitgestellt werden.
Das Client-Programm JonDo wird lokal auf dem Rechner des Nutzers installiert und ist über das Internet mit dem Anonymisierungsdienst verbunden. Dieser Dienst besteht aus mehreren hintereinander geschalteten Zwischenstationen, die auch *Mixe* genannt werden. [Jon13, Pro11b]

Zunächst sammelt jeder Mix gleich große Nachrichtenpakete von mehreren Nutzern, die dann entschlüsselt und umsortiert werden. Aufgrund der Entschlüsselung sind ein- und ausgehende Datenpakete nicht identisch, wodurch deren Zuordnung zueinander erschwert wird.
Für jede Zwischenstation müssen die Datenpakete bereits auf dem Client-Rechner verschlüsselt und adressiert werden. Dann werden sie über mindestens zwei Zwischenstationen geleitet, die von unterschiedlichen Mix-Betreibern bereitgestellt werden. Dadurch ist der ersten Station zwar der Absender, aber nicht der Empfänger bekannt, und der zweiten Station ist der Empfänger, jedoch nicht der Absender bekannt. [Jon13, Pro11b]

Eine Zuordnung der Nachricht ist insbesondere deshalb nicht möglich, weil immer mehrere Nachrichten von unterschiedlichen Teilnehmern schubweise bearbeitet und umsortiert werden. Durch die gleiche Länge aller Nachrichten kann ein Beobachter die Route einer Nachricht nicht anhand ihrer Größe ermitteln.
Zudem werden bei den Teilnehmern Leernachrichten (*Dummy-Traffic*) versendet, wenn sie keine Nachrichten zu versenden haben. Durch das Ausbleiben der Nachrichten könnte sonst eine Verbindung zwischen dem Nutzer (der keine Daten mehr versendet) und dem vom letzten Mix adressierten Rechner (der keine Daten mehr erhält) hergestellt werden. [Jon13, Pro11b]

Bei Mixes sind sogenannte *Replay-Attacken* möglich. Dabei zeichnet der Beobachter eine Nachricht auf und spielt diese zu einem späteren Zeitpunkt nochmals ab. Dadurch wird die Nachricht erneut vom Mix entschlüsselt und es entsteht eine zur ursprünglichen Verarbeitung identische Nachricht. Durch einen Vergleich der Mix-Ausgaben kann der Beobachter die wiederholt gesendete Nachricht entdecken und dadurch einen Mix überbrücken.
Um *Replay-Attacken* zu verhindern, besitzt jeder Mix eine Datenbank, in der ein

Fingerabdruck gespeichert wird, der eine Nachricht eindeutig identifiziert. Wird eine Nachricht zur Bearbeitung vorgelegt, wird in der Datenbank abgefragt, ob sie bereits bearbeitet wurde.
Zudem besitzt jede Nachricht einen Zeitstempel und bei der Bearbeitung werden nur diejenigen berücksichtigt, die innerhalb einer bestimmten Zeitschranke liegen. Ältere Nachrichten werden aus der Datenbank wieder gelöscht. [Pro11b]

Das Client-Programm JonDo wird zwar seit Dezember 2016 nicht mehr als eigenständige Software weiterentwickelt, dafür werden die Anonymisierungsfunktionen gebündelt im JonDoBrowser angeboten. [Jon13]

Unter der Adresse *http://ip-check.info* stellt der Hersteller einen Anonymitätstest bereit, mit dem verschiedene Einstellungen in den Ampelfarben rot (schlecht), gelb (mittel) und grün (gut) sichtbar gemacht werden. Dabei werden Eigenschaften zu Cookies, JavaScript, dem User-Agent-String, der Monitorauflösung oder auch zu installierten Schriftarten geprüft, mit dem jeweiligen auslesbaren Wert und der entsprechenden Bewertung angezeigt. [Pro11a]

5.3 Hypertext Transfer Protocol Secure

Das *Hypertext Transfer Protocol Secure* (HTTPS) sorgt dafür, dass bei der Kommunikation zwischen Client und Server die ausgetauschten Informationen verschlüsselt werden und somit nicht im Klartext mitgelesen werden können. Über das Präfix *https://* in der URL wird dem Browser mitgeteilt, dass der Server zusätzlich das SSL- (Secure Sockets Layer) bzw. das TLS-Protokoll (Transport Layer Security) verwenden soll, um Daten zu verschlüsseln, die zum Server gesendet oder vom Server empfangen werden. Durch diese Verschlüsselung kann die Menge der Informationen verringert werden, die man online offenlegt, denn ohne HTTPS kann jeder, der das lokale Netzwerk überwacht, erkennen, welche Webseite besucht wird und welche Informationen gesendet oder empfangen werden. Dazu gehören auch IDs und Passwörter. [Los15]

Die Verwendung von HTTPS dient den Schutzzielen Vertraulichkeit (kein Dritter kann die Daten mitlesen), Integrität (die Daten können während der Übertragung nicht verändert werden) und Authentizität (der Kommunikationspartner ist verifizierbar) beim Datenaustausch zwischen Client und Server.

Heutzutage sollte das TLS-Protokoll (Transport Layer Security) verwendet werden, eine Weiterentwicklung des weiterhin verfügbaren SSL-Protokolls (Secure Sockets Layer). Teilweise wird noch immer von SSL gesprochen, obwohl die technische Implementierung von TLS gemeint ist, daher sind die Grenzen zwischen beiden Protokollen nicht immer klar zu trennen.
Im OSI-Schichtenmodell ist SSL/TLS auf Schicht 5, der Sitzungsschicht angeordnet. Nicht nur HTTP, sondern alle Anwendungsprotokolle, die SSL bzw. TSL beherrschen, können mittels SSL/TLS verschlüsselt werden und damit den *secure*-Zusatz erhalten, wie SMTPS, POPS oder IMAPS. [Sch14b, SEL17]

Bestandteil von SSL/TLS ist die Zertifizierung des öffentlichen Schlüssels, die Authentifizierung des Servers, die Validierung des übermittelten Zertifikats und schließlich die verschlüsselte Übertragung von Daten zwischen Sender und Empfänger. Um den öffentlichen Schlüssel des Ansprechpartners und dessen Server zu authentifizieren werden Zertifikate verwendet. Beim Verbindungsaufbau, auch Handshake genannt, erhält der Client das Zertifikat vom Server und kann überprüfen, ob der dort genannte Name dem Server entspricht, mit dem er sich verbinden möchte. Darüber hinaus einigen sich Client und Server beim Handshake auf die Verschlüsselungsmethode und tauschen die symmetrischen Schlüssel aus, mit denen die Daten vor der Übertragung verschlüsselt werden.
In einem Zertifikat sind unter anderem der Domainname, der öffentliche Schlüssel, ein Gültigkeitsdatum und eine Instanz angegeben, welche die Vertrauenswürdigkeit des Inhabers bestätigt hat. Durch das Zertifikat authentisiert sich der Server gegenüber dem Client, der das Zertifikat überprüft (Validierung) und somit die Vertrauenswürdigkeit des Servers feststellt (Authentizität). [Sch14b, SEL17]

5.4 Anonyme Suchmaschinen

Die weltweit meist genutzte Suchmaschine Google speichert verfügbare Informationen seiner Nutzer und erstellt daraus detaillierte persönliche Profile (siehe *Abschnitt 4.1.3*). Dabei gibt es inzwischen viele Suchmaschinen, welche die Privatsphäre des Nutzers respektieren und dabei nicht zwangsläufig schlechtere Suchergebnisse liefern. Drei dieser Anbieter werden in den folgenden Unterkapiteln vorgestellt: StartPage, DuckDuckgo und MetaGer. Dabei wird insbesondere untersucht, ob der Quellcode der Anbieter Open Source verfügbar ist, ob HTTPS bzw. *Perfect Forward*

Secrecy unterstützt wird und ob ein Proxy-Server für den Zugriff auf die Suchergebnisse angeboten wird. Darüber hinaus wird sowohl der Unternehmens- und Server-Standort betrachtet, als auch die Einbindung von Werbung.
Die Eigenschaft des *Perfect Forward Secrecy* (PFS) ist dann erfüllt, wenn beim Verschlüsselungsprotokoll die Sitzungsschlüssel nachträglich nicht aus den Langzeitschlüsseln rekonstruiert werden können. Dadurch wird verhindert, dass aufgezeichnete verschlüsselte Kommunikation nachträglich bei Kenntnis des Langzeitschlüssels entschlüsselt werden kann.

5.4.1 StartPage

Die Suchmaschinen StartPage und Ixquick stammen von dem niederländischen Unternehmen Surfboard Holding B.V. Im März 2016 wurden die beiden zu der Suchmaschine StartPage zusammengeführt, jedoch sind weiterhin beide Domains *StartPage.com* und *Ixquick.com* erreichbar.
Bei diesen Seiten werden Ergebnisse von Google angezeigt, indem die Suchanfrage anonymisiert an Google weitergeleitet und die Ergebnisse zurück gesendet werden. Für diese Kooperation erhält Google pro angezeigtem Eintrag einen Beitrag.
Das Unternehmen versichert, dass bei der Nutzung der Suchmaschine innerhalb Europas, die Suchanfragen ausschließlich auf Server weitergeleitet werden, die sich ebenfalls in Europa befinden. Die Server in den USA werden ausschließlich für die dort gestellten Anfragen verwendet.
In den Einstellungen kann die Region der Server selbst gewählt werden. So kann anstelle des Standardwertes *den nächsten/schnellsten* die Option *EU-Server* oder *US-Server* angegeben werden. Die Suchmaschine finanziert sich über nicht personalisierte Werbung (Google Ads), die bei den Ergebnissen angezeigt wird.
Bei der Nutzung von StartPage werden, abgesehen von der Gesamtsumme der Suchanfragen auf die Webseite pro Tag, keine Nutzerdaten gespeichert und keine Daten an Dritte weitergegeben, abgesehen von der Suchanfrage selbst. Zusätzlich unterstützt die Seite eine verschlüsselte Verbindung über HTTPS (siehe *Abschnitt 5.3*).
Suchergebnisse können darüber hinaus über den *StartPage Proxy* geöffnet werden. Dabei wird die gewünschte Webseite von StartPage aufgerufen und angezeigt. Der Webserver hat dadurch lediglich Zugang zu der IP-Adresse von StartPage und nicht zu der des Nutzers.
Der Ladevorgang dauert bei einem Seitenaufruf über den Proxy entsprechend länger

und er kann nicht verwendet werden, um Formulare auszufüllen. Zudem deaktiviert der Proxy JavaScript und lädt keine Frames von externen Webseiten (also von Seiten die nicht der aufgerufenen entsprechen). [Str16, Sur17a, Sur17b]

StartPage setzt das *Perfect Forward Secrecy*-Verfahren in Kombination mit der SSL-Verschlüsselung ein. Dabei wird ein sicherer Tunnel erstellt, durch den die Suchanfragen und -ergebnisse der Nutzer nicht von anderen Webseiten abgehört werden können. Das PFS-Verfahren ist ein zusätzlicher Schutzmechanismus für den Fall, dass der private SSL-Schlüssel nicht mehr geheim ist (durch Gerichtsbeschluss, Online-Attacken oder Kryptoanalyse). Dabei kommt zusätzlich ein Session-Schlüssel zum Einsatz, ohne den die Daten nicht entschlüsselt werden können. [Sur13]

Darüber hinaus übermittelt StartPage die Suchanfragen standardmäßig per POST-Methode, wodurch (im Gegensatz zur GET-Methode, die von anderen Suchmaschinen benutzt wird) die Suchanfragen nicht von den Log-Dateien der aufgerufene Webseiten erfasst werden können.
Nutzerspezifische Einstellungen werden bei StartPage in der Regel in einem Cookie gespeichert. Alternativ dazu kann man vorgenommene Einstellungen auch in einer URL speichern, die mit Hilfe des URL-Generators als Volltext oder codiert erstellt werden kann. [Sur17b, Sur17c]

Vor der Zusammenführung mit StartPage war Ixquick eine Metasuchmaschine, die zwar noch auf der Seite *Ixquick.eu* erreichbar ist, aber nur noch sporadisch Updates erhält. Auf dieser Seite werden Suchanfragen anonym an verschiedenen Suchmaschinen weitergeleitet und deren Ergebnisse angezeigt. [Str16]

5.4.2 DuckDuckGo

DuckDuckGo wurde 2008 von Gabriel Weinberg gegründet. Das Unternehmen Duck Duck Go Inc. hat seinen Standort in den Vereinigten Staaten und ist eine Kombination aus Metasuchmaschine und Webcrawler. Die Suchergebnisse basieren auf über 400 Quellen, darunter andere Suchmaschinen wie Wikipedia, Bing und Yahoo, aber auch selbst indizierten Seiten. [Ducc]

DuckDuckGo nutzt sowohl eigene Server, aber auch die des Anbieters *Amazon Web Services* und finanziert sich sowohl über Werbung (Bing Ads), die auf Schlüsselworte des Suchterms abgestimmt ist, als auch über eine Partnerschaft mit Amazon und

eBay. Dabei erhält das Unternehmen eine Provision, wenn die genannten Seiten über DuckDuckGo aufgerufen werden. [Duca, Duc13]

Das Unternehmen gibt an, keine Nutzerdaten zu speichern. Es werden zwar Suchdaten gespeichert, um beispielsweise die Rechtschreibkorrektur verbessern zu können, allerdings würden dazu aggregierte Daten verwendet, die keine IP-Adresse oder sonstige eindeutige Nutzer-Identifikatoren enthalten. [Duc12]

Neben der verschlüsselten Datenübertragung via SSL kommt auch hier das *Perfect Forward Secrecy*-Verfahren zum Einsatz. [Duc12]
In den Einstellungen kann der Standardwert für die zu verwendende HTTP-Anfragemethode von *GET* zu *POST* geändert werden. Dadurch wird der Suchterm nicht an andere Webseiten übermittelt. Allerdings wird durch diese Methode gewöhnlich der zurück-Button außer Funktion gesetzt und die Such-URL kann nicht aus der Adress-Zeile kopiert werden. [Ducb]

Cookies werden lediglich bei Anpassungen in den Einstellungen gespeichert, jedoch nur auf dem Nutzerrechner und nicht auf den DuckDuckGo-Servern. Der Inhalt des Cookies ist nicht verschlüsselt und kann so vom Nutzer jederzeit eingesehen werden. Alternativ zum Cookie können Einstellungen auch über Adressparameter in der Suchanfrage angegeben werden. Die Parameter sind auf der Webseite *duckduckgo.com/params* aufgeführt. Nach vorgenommenen Anpassungen in den Einstellungen, kann die URL dort direkt angezeigt werden.
Sollen die gleichen Einstellungen auf mehreren Geräten genutzt werden, können diese anonym in einer Cloud gespeichert werden. Dazu muss man lediglich eine einzigartige Passphrase angeben, über die man seine Einstellungen speichern und erneut laden kann. [Duc12, Ducb]

Eine Besonderheit der Suchmaschine, die zum Teil Open Source zur Verfügung steht, sind die *!bang*-Funktionen, bei denen über Kürzel auf interne Suchfunktionen von Webseiten oder anderen Suchmaschinen zugegriffen werden kann. So erhält man bei der Eingabe eines Kürzels mit Suchbegriff, beispielsweise *!w Enigma* in die DuckDuckGo-Suchleiste, alle Wikipedia Einträge zum Thema *Enigma*.

5.4.3 MetaGer

MetaGer ist eine Suchmaschine, die 1996 von einem Forscherteam der Universität Hannover entwickelt wurde. Inzwischen wird MetaGer von SUMA-EV (Verein für freien Wissenszugang e.V.) in Kooperation mit der Leibniz Universität Hannover betrieben und weiterentwickelt. Der gemeinnützige Verein arbeitet zwar nicht gewinnorientiert, muss aber dennoch Werbung von Yahoo bei den Suchergebnissen einblenden. Ähnlich wie DuckDuckGo, handelt es sich bei MetaGer um eine Metasuchmaschine, die eine ganze Reihe von Web-Suchmaschinen durchsucht und diese mit selbst indizierten Quellen kombiniert. Die Ergebnisse werden dann zusammengefasst und Doubletten, soweit möglich, entfernt.
In der Ergebnisliste ist erkennbar, aus welcher Quelle das jeweilige Suchergebnis stammt. Der Nutzer kann aber auch schon vor einer Suche festlegen, welche Quellen für seine Suche genutzt werden sollen. [SUMa, SUM14, SUM17b]

Die Server von MetaGer befinden sich ausschließlich in Deutschland, wodurch MetaGer dem deutschen Datenschutzrecht unterliegt. Zudem versichern die Betreiber, dass keine Nutzerdaten gespeichert und die Suchanfragen ausschließlich anonymisiert an die Suchdienste weitergegeben werden. [SUMa, SUM14]

Ebenso wie bei StartPage können auch bei MetaGer die Suchergebnisse über einen Proxy-Server geöffnet werden. Diese Funktion wird über den Link *Anonym öffnen* bei den einzelnen Ergebnissen bereitgestellt.
Darüber hinaus erfolgt die Verbindung zu MetaGer verschlüsselt über das HTTPS-Protokoll. Dadurch wird die Suchabfrage vom Nutzerrechner zum MetaGer-Server sicher übertragen. Der Quellcode von MetaGer steht zudem seit August 2016 Open Source zu Verfügung. [SUMa, SUMb, SUM14]

Neben der Suchmaschine bietet MetaGer mit dem Kartendienst *Maps.MetaGer.de* eine interessante Alternative zu Google Maps. Der Routenplaner und Kartendienst basiert auf Karten von OpenStreetMap. Aktuell ist die Karte zwar noch auf Deutschland begrenzt, eine Erweiterung auf europäisches und schließlich weltweites Kartenmaterial ist jedoch in Planung. Seit März 2017 kann auf diese Dienstleistung auch über eine Android-App zugegriffen werden. [SUM17a]

5.4.4 Zusammenfassung

Beim Vergleich der Suchmaschinen lässt sich festhalten, dass lediglich MetaGer seinen Quellcode Open Source bereitstellt. Eine verschlüsselte Verbindung über HTTPS bieten alle drei Anbieter an, *Perfect Forward Secrecy* dagegen erfüllen nur StartPage und DuckDuckGo. Einen Proxy-Server mit dem auch Suchergebnisse anonym geöffnet werden können, wird sowohl bei StartPage als auch MetaGer angeboten. Diese Ergebnisse sind in *Tabelle 3 Merkmale der Suchmaschinen* zusammengefasst.

Merkmal	**StartPage**	**DuckDuckGo**	**MetaGer**
Open Source	nein	nein	ja
HTTPS	ja	ja	ja
Perfect Forward Secrecy	ja	ja	nein
Proxy-Server	ja	nein	ja

Tabelle 3: Merkmale der Suchmaschinen

Neben den drei untersuchten Suchmaschinen, gibt es weitere, welche auf die Privatsphäre des Nutzers Wert legen. Dazu gehören beispielsweise Cliqz, Qwant, yacy, Disconnect, hulbee, deusu, Wegtam und unbubble, welche in dieser Arbeit nicht näher betrachtet werden können.

5.5 Maßnahmen gegen Cookies

Die in *Abschnitt 3.2* beschriebenen Cookie-Arten erfordern zum Teil unterschiedliche Schutzmaßnahmen. Am einfachsten kann man sich gegen **Third-Party Cookies** schützen, da alle modernen Browser die Möglichkeit bieten, diese über die Einstellungen zu blockieren. Dem Nutzer entstehen dadurch in der Regel keine Nachteile, da Third-Party Cookies meist ausschließlich für das Nutzer-Tracking eingesetzt werden. [Mau15]
Allerdings werden durch das Setzten des Konfigurationsparameters Funktion *Cookies von Drittanbietern akzeptieren: nie* in Firefox nur wenige externe Dienste blockiert. Dies hat zumindest der Selbstversuch mit dem Firefox-Add-on Lightbeam gezeigt, mit dem Verflechtungen von Third-Party-Trackern visualisiert werden können. So ergab das Setzten dieser Funktion lediglich einen Unterschied von 147 zu 136 Verbindungen zu externen Diensten (also eine Reduzierung um rund 7,5%). Der

Versuch hat gezeigt, dass besonders Ad-Blocker beim Blockieren von Third-Party Cookies und anderen Third-Party Trackern hilfreich sind. *Abb. 4* zeigt die Third-Party-Tracker beim Aufruf der drei Nachrichtenseiten *www.spiegel.de*, *www.welt.de* und *www.zeit.de* ohne Add-Blocker (jedoch mit der Blockierung von Third-Party Cookies über die Firefox-Funktion). Dabei sind beim Aufruf dieser drei Seiten 136 externe Dienste involviert. Einige der Dienste werden dabei von mehreren oder allen aufgerufenen Webseiten eingebunden.

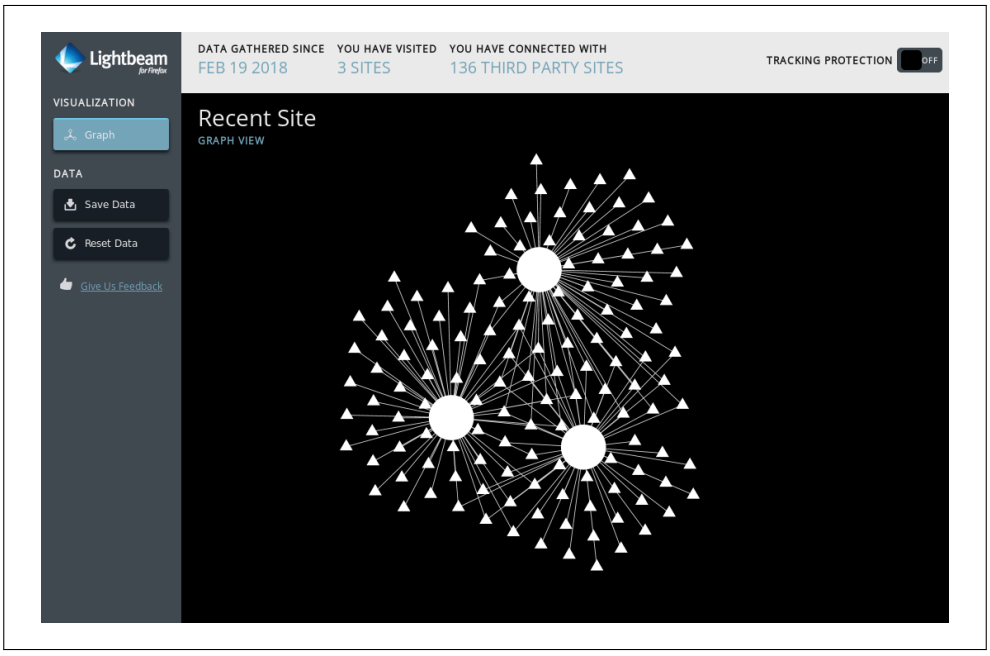

Abbildung 4: Externe Dienste ohne Add-ons

Häufig empfohlene Add-ons zum Blockieren von Third-Party Cookies und anderen Trackern sind *uBlock Origin* und *Privacy Badger*. Sind diese beiden Add-ons aktiviert, werden beim Aufruf der drei genannten Nachrichtenseiten lediglich 22 externe Dienste eingebunden. Dieses Resultat ist in *Abb. 5* dargestellt. Wird ausschließlich das Add-on *uBlock Origin* eingesetzt, wird eine Verbindung zu 32 externen Diensten aufgebaut. Der Einsatz von Ad- und Tracking-Blockern, wie *uBlock Origin* und *Privacy Badger* ist daher zu empfehlen.

Ebenso wie Third-Party Cookies können auch **First-Party Cookies** für das Nutzer-Tracking verwendet werden, allerdings sind an diese auch viele Funktionalitäten gekoppelt. Deshalb können Webseiten und deren Funktionen nicht mehr genutzt werden, wenn Cookies generell blockiert werden. Als Kompromiss könnte man Positivlisten, sogenannte Whitelists nutzen, auf denen Webseiten angegeben werden,

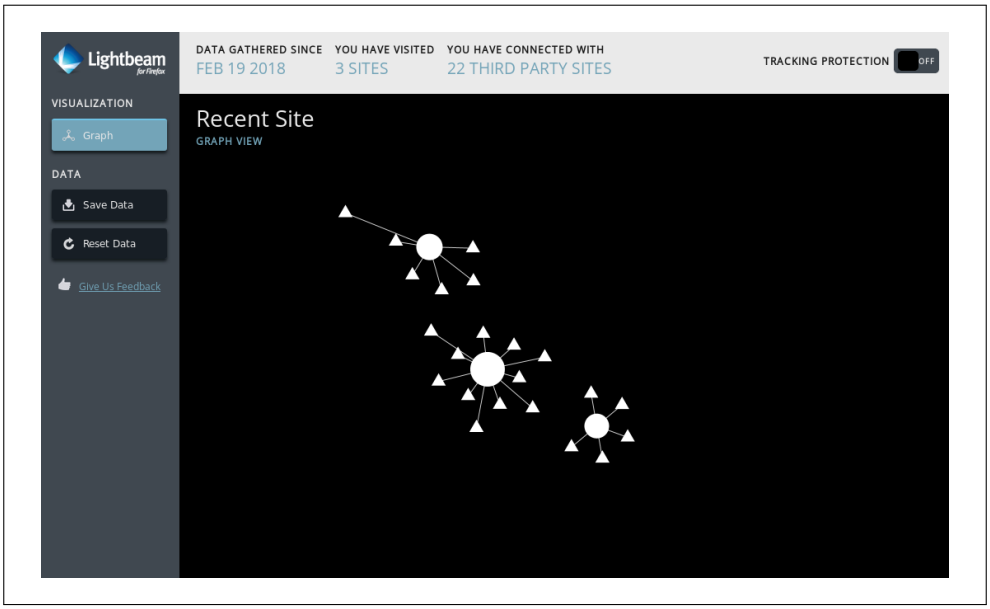

Abbildung 5: Externe Dienste mit uBlock Origin und Privacy Badger

die vertrauenswürdig sind und bei deren Besuch das Setzen von Cookies erlaubt wird. Alle Webseiten, die nicht auf der Liste angegeben sind, dürfen keine Cookies setzen. Für den Nutzer entsteht dadurch jedoch ein hoher Verwaltungsaufwand und darüber hinaus können diese individuellen Listen für die Methode des Fingerprintings genutzt werden, wodurch der Nutzer eindeutig identifizierbar wird und seine Daten wiederum erfasst und gesammelt werden können. [Mau15]
Alternativ dazu ist es möglich das Speichern von Cookies nur temporär zu gestatten. In den Einstellungen von Firefox kann man beispielsweise festlegen, dass Cookies mit dem Beenden des Browsers wieder entfernt werden sollen. Um weitere Speicherbereiche, auf die ein Browser Zugriff hat, vor der Speicherung von Cookies zu schützen, kann man den *Private-Mode* (*Inkognito-Modus*) nutzen, den die meisten modernen Browser anbieten. Dabei werden sowohl Cookies, Formulareinträge, Chronik, Downloadlisten und temporäre Dateien nicht dauerhaft, sondern lediglich temporär bis zum Sitzungsende gespeichert. [Mau15, Moz17]

Evercookies sind für den Nutzer intransparenter und schwieriger zu löschen als andere Cookies. Bei diesen werden Daten redundant mit unterschiedlichen Verfahren gespeichert, deshalb müssen hier alle Speicherbereiche bereinigt werden, sowohl die vom Browser zugänglichen Bereiche als auch jene, die darüber hinaus für die Speicherung von Evercookies infrage kommen. Wird dabei ein Speicherort ausgelassen, kann sich ein Cookie selbst rekonstruieren. [AEE+14, Sch16]

Betroffen sind auch die Speicherbereiche, auf die der Browser Zugriff hat, wie der Cache (siehe *Abschnitt 3.3*) oder die Suchhistorie. Verwendet ein Nutzer mehrere Browser, müssen diese Daten in allen Browsern gleichzeitig entfernt werden. Darüber hinaus müssen die Daten der HTML5-Speicherbereiche und die Flash-Cookies entfernt werden. Bei der Verwendung des Private-Mode eines Browsers werden Cookies, z. B. auch im HTML5-Storage, nur temporär gespeichert und mit dem Beenden des privaten Modus wieder gelöscht. [AEE+14, Sch16]
Da viele Cookies mittels JavaScript gesetzt werden, wäre es von Vorteil dieses vollständig zu blockieren, was für die reibungslose Internetnutzung jedoch nicht praktikabel ist. [Ele15]
Der von Evercookies genutzte Speicherbereich IndexedDB kann deaktiviert werden, indem im Konfigurationseditor für Firefox, der mit *about:config* aufgerufen werden kann, die Einstellung *dom.indexedDB.enabled* auf den Wert *false* gesetzt wird. Ebenso kann auch der LocalStorage (*dom.storage.enabled*) deaktiviert werden, wodurch **Flash-Cookies** keinen lokalen Speicherplatz mehr nutzen können. Durch die Deaktivierung von LocalStorage und IndexedDB kann es allerdings auch zu Einschränkungen bei den Funktionalitäten von Webseiten kommen. [Mau15, Sch16]
Der beste Schutz gegen Flash-Cookies ist der Verzicht auf den Flash-Player, indem man ihn deinstalliert. Sofern man auf den Player nicht verzichten kann, sollte zumindest die standardmäßige Annahme von Flash-Cookies deaktiviert werden. Der Nutzer wird dann vor der Verwendung des Flash-Plugins gefragt, ob Adobe Flash aktiviert werden soll. Des weiteren sollten über den *Adobe Einstellungs-Manager* die Flash-Cookies regelmäßig gelöscht werden. [AEE+14, Sch16]

5.6 Maßnahmen gegen eTags

Das Speichern von Informationen im Browser-Cache (siehe *Abschnitt 3.3*) kann verhindert werden, indem der Cache entweder regelmäßig geleert oder komplett deaktiviert wird. [Sch13]
Beim Browser Firefox kann in den Einstellungen unter *Zwischengespeicherte Webinhalte* das automatische Cache-Management deaktiviert und die Speicherplatzgröße für den Cache auf Null limitiert werden. Diese Deaktivierung hat jedoch auch höhere Ladezeiten und Bandbreitenbelastung zur Folge. [San16, Sch13]

Bei der Verwendung des Private-Mode werden keine temporären Dateien oder Daten, die für die Offline-Verwendung vorgesehen sind gespeichert, weshalb diese Maßnahme sowohl gegen Cookies als auch eTags hilfreich sein kann. [Moz17]

5.7 Maßnahmen gegen Fingerprinting

Gegen die Methode des Fingerprintings, die in *Abschnitt 3.4* beschrieben ist, kann man sich schützen, wenn man einen Anonymisierungsdienst, wie den Tor-Browser verwendet oder indem JavaScript und Flash vollständig blockiert werden. Dadurch können vom Browser keine Merkmale mehr aktiv abgefragt werden, wodurch sich die Menge der Daten, aus denen ein Fingerprint berechnet werden kann, deutlich reduziert. Darunter fallen Informationen über die installierten Plugins oder welche Schriftarten installiert sind. Allerdings ist diese Option äußerst unpraktikabel, da ohne JavaScript kaum eine Webseite uneingeschränkt funktioniert. [Bis14, Ele15, Mau15]
Die Option Whitelists zu erstellen, die alle Webseiten enthalten, bei deren Besuch JavaScript aktiviert werden darf, verschiebt das Problem nur. Einerseits wird JavaScript dabei generell blockiert und die definierten Ausnahmen können in vollem Funktionsumfang genutzt werden. Andererseits können die dabei entstehenden individuellen Listen ebenfalls als Merkmal für das Fingerprinting genutzt werden, wodurch ein Nutzer wiederum eindeutig identifiziert werden kann. [Mau15, MBYS11]

Neben Whitelists können auch Browser Add-ons, die eigentlich dem Schutz der Privatsphäre dienen, dazu verwendet werden, um einen individuellen Fingerprint zu erstellen. Solange eine Erweiterung nicht auch von einer Vielzahl anderer Nutzer eingesetzt wird, können sie, ebenso wie individuelle Einstellungen oder wenig verbreitete Browser, erheblich zu der Erzeugung eines Fingerprints beitragen, weil sie selbst ein charakteristisches Fingerprinting-Merkmal darstellen. [Eck10, ubu17]
Beispielsweise konnten Nutzer von Privoxy, einem sogenannten Content-Filtering-Proxy, bereits im Jahr 2010 eindeutig identifiziert werden. Privoxy hat zur Aufgabe die Privatsphäre zu schützen, indem z. B. Werbebanner automatisch aus dem Seiteninhalt entfernt und das Setzen von Tracking-Cookies verhindert werden sollte. Allerdings enthielt der *User-Agent-String* – eine Zeichenkette, die unter anderem Versionsnummer, Browser-Name und Betriebssystem beinhaltet und der beim Abruf von Webseiten an den Server übertragen wird – den Wert *Privoxy*. Da der Dienst

nur von wenigen Nutzern verwendet wurde, stellte der Wert des *User-Agent-Strings* ein sehr markantes Merkmal dar, das in Kombination mit weiteren Merkmalen die Nutzer eindeutig identifizierbar machte. [Eck10, ubu17]

Dennoch sollten nur solche Skripte ausgeführt werden, die auch erforderlich sind. Die Electronic Frontier Foundation empfiehlt dazu die Installation einer Erweiterung wie Privacy Badger oder Disconnect. Diese blockieren Domains, die einen Fingerabdruck erstellen möchten. Zudem wird das Add-on NoScript für die Verwaltung von JavaScript und ein Werbeblocker, wie uBlock Origin empfohlen. [Ele15]

Eine andere Strategie sich zu schützen, besteht darin, die Informationen, die beim Fingerprinting abgefragt werden zu verfälschen. Dabei können entweder zufällig generierte Daten zu denen des Nutzers hinzugefügt oder aber auf jedem System identische Fingerprinting-Merkmale erzeugt werden, wodurch die Ergebnisse unbrauchbar werden. [Mau15]
Das Abändern der Daten ist technisch generell möglich, so kann beispielsweise der User-Agent-String mit Hilfe von Add-ons wie dem *User Agent Overrider* oder *User Agent Switcher* verändert werden. Dabei kann auf einem Linux-System bei dem Firefox als Browser verwendet wird, der User-Agent-String zu einem Windows-System mit dem Internet Explorer als Browser geändert werden. [Mau15]
Ebenso können installierte Schriftarten mit der Anwendung Fluxfonts manipuliert werden. Dabei werden Schriftarten regelmäßig zufällig neu erzeugt und gelöscht, um zu verhindern, dass ein identischer Fingerprint erneut erzeugt werden kann. [Ale17]
Auch andere Informationen könnten verändert werden, wobei es dabei zu beachten gilt, dass durch Manipulationen beispielsweise eine Webseite nicht mehr optimal dargestellt wird. Darüber hinaus kann die Manipulation der Daten für die Tracker auch nachvollziehbar sein, wenn ihnen widersprüchliche Informationen vorliegen. [Mau15]

Auch die Browser-Hersteller ergreifen Maßnahmen, die gegen Fingerprinting schützen sollen. So soll der User-Agent-String bei Safari in Zukunft nicht mehr verändert werden, wodurch die Variation aufgrund der unterschiedlichen Versionsnummern deutlich verringert wird. Der konstante User-Agent-String soll mit *Safari Technology Preview 46* verfügbar sein. Zudem wurde bereits in Safari 11 eine Funktion integriert, mit der Tracking-Anbieter automatisch identifiziert und die Nutzerverfolgung über mehrere Webseiten hinweg unterbunden werden soll. [Bec17a, Bec17b]

Dieser Abschnitt zeigt, wie ambivalent die Schutzmaßnahmen gegen nur eine Methode der Datenerhebung sein können. Häufig sind diese Schutzmaßnahmen auch mit Funktionseinbußen verbunden. Einen einheitlichen und effektiven Schutz gegen das Fingerprinting gibt es bislang nicht. Je nachdem, welche Maßnahmen der Nutzer zu ergreifen bereit ist, müssen die verschiedenen Aspekte dabei gegeneinander abgewogen und die individuellen Merkmale überprüft werden. Dazu kann man unter der Seite *panopticlick.eff.org* oder *amiunique.org* auch testen, wie viele Informationen durch Fingerprinting abgerufen werden können.

5.8 Maßnahmen gegen Ultraschall-Tracking

Ebenso wie beim Fingerprinting gibt es bislang auch gegen das Cross-Device-Tracking mit Ultraschall (*Abschnitt 3.5*) noch keine einheitliche Schutzmaßnahme.
Ultraschall-Signale sollen besonders häufig in der Werbung abgespielt werden. Daher kann das Aussenden von Ultraschall-Wellen verhindert werden, indem der Ton beim Abspielen von Werbung deaktiviert wird.
Ein andere mögliche Maßnahme besteht darin, die Berechtigungen von installierten Apps zu prüfen und lediglich solchen Apps das Zugriffsrecht auf das Mikrofon zu erteilen, die dieses tatsächlich benötigen. Dadurch wird die Wahrscheinlichkeit minimiert, dass Ultraschall-Signale von Apps, die Zugriff auf das Mikrofon haben, empfangen werden können. [Fri16]

Ein Forscherteam des University College London und der University of California, Santa Barbara stellt auf der Webseite *ubeacsec.org* für Chrome die Browsererweiterung SilverDog bereit, die Ultraschallwellen herausfiltert. Dabei werden alle Audiosignale von aufgerufenen Webseiten gescannt und nicht hörbare Frequenzen blockiert. Folglich können von Webseiten keine Ultraschallwellen mehr abgespielt werden, allerdings nur für Nutzer des Chrome Browsers.
Eine zweite Software für Android-Geräte erweitert das Berechtigungssystem. Dabei wird eine neue Berechtigungsstufe für unterschiedliche Frequenzbereiche eingeführt, durch welche Frequenzen im hörbaren Bereich von denen im hochfrequenten abgegrenzt werden. Der Nutzer kann also hörbare Frequenzen zulassen und nicht hörbare, wie Ultraschallwellen, blockieren. [Kre16a, MHF+16]

5.9 Schutzmaßnahmen bei mobilen Geräte

In diesem Kapitel werden Maßnahmen genannt, mit denen die Datenerhebung auf mobilen Geräten (*Abschnitt 3.6*) eingeschränkt werden kann.
Wie bereits als grundlegender Aspekt in *Abschnitt 5.1.1 Datenvermeidung und Produktauswahl* aufgeführt, sollten auch Apps auf mobilen Geräten mit Bedacht ausgewählt werden. Dabei sollte ein Nutzer stets abwägen, ob eine App tatsächlich benötigt wird und der Anbieter vertrauenswürdig ist oder ob stattdessen auf den Dienst verzichtet werden kann. Häufig kann die Funktion einer App durch den Aufruf einer Webseite im Browser ersetzt werden. Es wird also empfohlen, möglichst wenige Apps zu installieren und auch die damit verknüpften Accounts, soweit möglich, zu reduzieren. Zudem sollten solche Apps genutzt werden, die den Datenschutz und die Privatsphäre des Nutzers respektieren. [Gro16]

Durch das Deaktivieren von Funktionen mobiler Geräte, können die installierten Apps diese in der Regel nicht mehr nutzen, wodurch weniger Daten erfasst werden. Daher sollten Funktionen, wie GPS, WLAN und Bluetooth, die anfällig für Missbrauch sind, nur bei Bedarf aktiviert werden. Sowohl die Identifikation oder Ortung eines mobilen Geräts, als auch die Erstellung eines Bewegungsprofils kann dadurch verhindert werden. Demzufolge sollte auch der Offline-Modus immer dann verwendet werden, wenn dies möglich ist. Daten, die der Nutzer unterwegs benötigt, wie z. B. Straßenkarten, können bereits vorab geladen werden.
Eine weitere Funktion, die generell deaktiviert werden sollte, ist die automatische Synchronisation. Bei dieser Funktion werden Personendetails, Kalender, Kontakte, Musik, App-Daten und weitere Informationen mit dem Plattform-Konto synchronisiert. Durch die Deaktivierung wird die Datenmenge, die an Google oder Apple übertragen wird, erheblich reduziert. [Gro16, Sch14a]

In Abhängigkeit ihrer Zugriffsrechte können Apps mehr oder weniger Nutzerdaten abrufen, speichern und auswerten. Daher besteht eine wichtige Maßnahme darin, die Berechtigungen installierter Apps zu überprüfen und diese soweit wie möglich einzuschränken. Für Geräte mit dem Betriebssystem Android können seit Version 6.0 Berechtigungen App-spezifisch verwaltet werden. Unter diesen *App-Berechtigungen* können die verschiedenen Zugriffs-Bereiche, wie Kalender, Mikrofon, Kamera, Standort, etc. aufgerufen und bearbeitet werden. Nach der Auswahl eines Bereichs werden alle Apps angezeigt, denen der entsprechende Zugriff gewährt bzw. entzogen werden

kann. Allerdings erscheint z. B. beim Versuch, dem Google Play-Dienst die Berechtigung für Kontakte zu entziehen die Meldung: *Wenn Sie diese Berechtigung deaktivieren, funktionieren grundlegende Funktionen Ihres Geräts möglicherweise nicht mehr ordnungsgemäß.*
Der Anwender kann durch das bewusste Zuweisen der Berechtigungen also Zugriffsrechte und damit die Optionen für die Datenerfassung deutlich einschränken. Es gibt aber auch einige Apps, insbesondere vorinstallierte Anwendungen der Hardware-Hersteller (sogenannte Bloatware), bei denen mit Funktionseinbußen zu rechnen ist, wenn Rechte entzogen werden. Bloatware-Funktionen (insbesondere die Google Play Services, die auf handelsüblichen Android-Smartphones bereits vorinstalliert sind) werden auch von anderen Apps genutzt, welche dann ebenfalls nicht mehr funktionieren. [Gro16, Spi17b]

Ein Nutzer, der Bloatware entfernen möchte, kann - neben möglichen Funktionseinbußen - zudem auf das Problem stoßen, dass er selbst nicht über die dafür erforderliche Berechtigung verfügt. Da ein Hersteller die Funktionsfähigkeit seiner Geräte garantieren muss, werden dem Anwender standardmäßig lediglich eingeschränkte Berechtigungen eingeräumt. Dadurch soll vermieden werden, dass ein Anwender das System so modifiziert, dass es nicht mehr fehlerfrei funktioniert. Allerdings kann diese beschränkte Berechtigung aufgehoben werden, indem sich ein Anwender nachträglich selbst die höchste Berechtigungsstufe zuteilt. Bei Android-Geräten wird dabei von Root-Rechten gesprochen, bei Apple-Geräten vom sogenannten Jailbreak. [dig17, Sch18]

Dabei sollten jedoch sowohl die Lizenzbestimmungen, als auch die Hersteller-Garantie berücksichtigt werden. Android-Betriebssysteme werden unter Open Source-Lizenzen entwickelt, deren Merkmale unter anderem die freie Möglichkeit der Bearbeitung und Vervielfältigung der Software beinhaltet. Die mobilen Betriebssysteme von Apple (iOS) und Microsoft (Windows Phone bzw. Windows 10 Mobile) dagegen unterstehen streng proprietären Lizenzbestimmungen, weshalb es aus urheberrechtlicher Sicht nicht gestattet ist, solche Software zu modifizieren. Auch wenn in der Praxis kaum gegen Modifikationen proprietärer Software vorgegangen wird, sollte bedacht werden, dass über die Lizenzbestimmungen lediglich Modifikationen der meisten Android-Systeme erlaubt sind. Aus diesem Grund werden im Weiteren primär Android-Geräte betrachtet. [Gä12]
Darüber hinaus erlischt durch das Rooten in den meisten Fällen (eine Ausnahme hiervon ist z. B. das Fairphone) die Hersteller-Garantie. Dafür können dann tief-

greifende Modifikationen der Oberfläche oder der Systemeinstellungen vorgenommen und unter anderem Bloatware entfernt oder deaktiviert werden. Zudem können mit Root-Rechten Apps installiert werden, die sonst nicht oder nur eingeschränkt funktionieren würden, wie z. B. systemweite Werbeblocker. Ebenso kann mit Root-Rechten ein alternatives Betriebssystem installiert werden. [dig17, Sch18]

Bei den Betriebssystemen, die standardmäßig auf Smartphones oder Tablets installiert sind, ist es sehr schwer auf einen Account von Google oder Apple zu verzichten. Abhilfe kann bei Android-Geräten die Installation eines alternativen Betriebssystems, sogenannter Custom-ROMs schaffen. Zu ihnen gehören Betriebssysteme wie *LineageOS* (Nachfolger des 2016 eingestellten *CyanogenMod*), *Dirty Unicorns*, *Paranoid Android*, *Resurrection Remix* oder *SlimRoms*. Diese Systeme werden ohne proprietäre Google-Apps ausgeliefert, womit auch die Abhängigkeit von einem Google-Account hinfällig wird. Ein weiterer Vorteil von Custom-ROMs ist, dass bei ihnen oft über viele Jahre hinweg Sicherheits- und System-Updates bereitgestellt werden – auch für ältere Geräte. Die Hersteller dagegen stellen oft nach nur zwei bis drei Jahren die Updates für ein Betriebssystem ein. Wodurch entweder ein großes Sicherheitsrisiko entsteht oder der Anwender zum Kauf eines neues Geräts gedrängt wird. Darüber hinaus haben Custom-ROMs, aufgrund der geringen Anzahl vorinstallierter Apps, meist eine sehr gute Performance. [FH18]
Häufig enthalten Custom-ROMs auch bessere Datenschutzoptionen. So stellte CyanogenMod lange vor Android 6.0 den *Privacy Guard* zur Verfügung, mit dem Beschränkungen von Zugriffsrechten für einzelne Apps vorgenommen werden konnten. Ebenso ist mit dem *Privacy Guard* von LineageOS eine feingranularere Verwaltung von Zugriffsrechten möglich, als mit dem Berechtigungsmanager, der seit Android 6.0 integriert ist. [FH18, Kuk17a]

Anstelle des Goolge Play Store kann bei Android-Geräten der alternative App-Store *F-Droid* verwendet werden. Über ihn werden ausschließlich freie und quelloffene Apps, sogenannte FOSS-Apps (Free and Open Source Software) bereitgestellt. Betrieben wird F-Droid von der gemeinnützigen Organisation F-Droid Limited. [F-D17] Zwar ist die Auswahl in F-Droid deutlich geringer als im Goolge Play Store, allerdings gibt es inzwischen zu einigen proprietären Apps quelloffene Alternativen, die einen vergleichbaren Funktionsumfang aufweisen. [Kuk17b]

Nicht nur hinsichtlich der installierten Software, sondern auch bei der Auswahl eines neuen Geräts gibt es datenschutzfreundliche Alternativen.

Das Berliner Unternehmens GSMK bietet unter anderem mit dem *CryptoPhone 500* ein abhörsicheres Mobiltelefon an. Telefonate und die Übertragung von Textnachrichten erfolgen Ende-zu-Ende-verschlüsselt, aber auch die Hardware ist speziell gesichert. Bei verdächtigen Verbindungen zur Basisstation, die auf den Einsatz eines IMSI-Catcher hinweisen, wird der Nutzer eines solchen Geräts gewarnt. Ermöglicht wird diese Funktion durch die Integration einer Baseband-Firewall. [GSM17, Tho14]

Auch bei dem Smartphone *Librem 5* von Purism, das ab Januar 2019 ausgeliefert werden soll, ist eine Ende-zu-Ende-verschlüsselte Kommunikation standardmäßig geplant. Darüber hinaus soll das Gerät über Schalter verfügen, über die das Mikrofon, WLAN, die Kamera, Bluetooth oder auch der Mobilfunk deaktiviert werden können. Das *Librem 5* ist ein Open-Source-Smartphone aus San Francisco, auf dem ausschließlich quelloffene Software zum Einsatz kommen soll. [Ber17b]

Ein weiteres Gerät mit Fokus auf Datensicherheit ist das Blackphone. Es wurde von SGP Technologies entwickelt, einem Gemeinschaftsprojekt von GeekPhones und Silent Circles. Durch das Security Center, welches im Modell *Blackphone 2* integriert ist, werden Nutzer über sicherheitsrelevante Verbesserungsmaßnahmen informiert. Zudem verfügt das Blackphone 2 über ein detailliertes Berechtigungssystem, bei dem beispielsweise Lese- und Schreibrechte unabhängig voneinander verwaltet werden können. Darüber hinaus kann ein Nutzer auf diesem Gerät verschiedene Profile, sogenannte *Spaces* anlegen. Dem Nutzer werden viele Möglichkeiten bereitgestellt, diese Spaces zu konfigurieren. So können diese strikt voneinander getrennt und ihnen unterschiedliche Funktionen und Berechtigungen zugewiesen werden. Zum Beispiel kann festgelegt werden, welcher Space auf das Internet oder auf das Adressbuch zugreifen darf.
Auch bei diesem Gerät werden Daten verschlüsselt, sowohl beim Ablegen auf dem Dateisystem als auch beim Telefonieren oder Versenden von Nachrichten. [Eng17]

Der Datenerhebung auf mobilen Geräten kann ein Anwender also mit unterschiedlichen Maßnahmen entgegentreten. Am einfachsten zu realisieren sind dabei Einstellungen, die dem Schutz der eigenen Daten dienen, das Deaktivieren von Funktionen und das Einschränken der Berechtigungen für Apps. Aber auch die Auswahl der installierten Anwendungen ist entscheidend. Aufwendiger dagegen ist das Erlangen von Root-Rechten, mit deren Hilfe ein Anwender auf Google-Dienste und proprietäre Anwendungen verzichten kann. Dazu sind beim Nutzer fortgeschrittene technische Kenntnisse notwendig. Am effektivsten ist die Installation eines Custom-ROMs, bei

dem kein Google- oder Apple-Account erforderlich ist. Dabei muss ein Anwender allerdings – ebenso wie bei der Nutzung des alternativen App-Store F-Droid – auf gewohnte Anwendungen und Bequemlichkeit verzichten.

Kriterien, die beispielsweise bei der Auswahl eines Instant-Messenger entscheidend sein können, werden im folgenden *Abschnitt 5.10* erläutert.

5.10 Instant-Messenger

Mit einem Instant-Messenger können Kommunikationsteilnehmer Textnachrichten und Dateien in Echtzeit austauschen. Wie bereits erwähnt, sollten Anwendungen und Dienste mit Bedacht ausgewählt werden. Welche Kriterien bezüglich der Sicherheit persönlicher Daten bei Instant-Messengern relevant sein können, wird in den folgenden Abschnitten beispielhaft an Threema, Telegram und Signal untersucht.

Bei den genannten Messengern wird geprüft, ob diese eine anonyme Kennung verwenden, eine Ende-zu-Ende Verschlüsselung bieten, ob sie Zugriff auf das Telefonbuch erfordern, ob deren Quellcode Open Source zu Verfügung steht und ob die Eigenschaft des *Perfect Forward Secrecy* erfüllt wird.
Weitere Merkmale, die man nicht außer Acht lassen sollte, sind sowohl das Geschäftsmodell des Unternehmens und damit die Frage, worüber sich dieses finanziert, als auch der Unternehmens- und der Server-Standort.

5.10.1 Threema

Threema wird von einem Schweizer Unternehmen entwickelt, dessen Server ebenfalls in der Schweiz stehen. Der Name Threema ist vom Akronym EEEMA abgeleitet, was für *End-to-End Encrypted Messaging Application* steht. Im März 2017 hatte der Dienst über 4,5 Millionen Nutzer. Der Messenger arbeitet mit einer asymmetrischen Ende-zu-Ende-Verschlüsselung, jedoch ist der Quellcode nicht vollständig öffentlich, weshalb eine vollständige Analyse der Datenübertragung nicht möglich ist.
Der kostenpflichtige Messenger steht für das Betriebssystem Android, iOS und Windows Phone für 2,99 EUR zur Verfügung. Mit Einschränkungen kann Threema auch auf BlackBerry OS und Amazon Fire OS verwendet werden. Die Anwendung kann auch außerhalb des Google Play Store direkt bei Threema gekauft werden. [Thr17]

Threema ermöglicht das verschlüsselte Versenden von Text- und Sprachnachrichten, Bildern, Videos, Audiodateien und Dokumenten. Die Anwendung kann auch anonym verwendet werden, da die Identität nicht an die Rufnummer gebunden ist, sondern an die *Threema-ID*, eine achtstellige eindeutige Adresse, die aus Buchstaben und Zahlen besteht. [Hei15, Hes17, Thr17]

Der Nutzer kann selbst entscheiden, ob die Anwendung sein Adressbuch auslesen und die Daten pseudonymisiert speichern darf. Von dieser Zustimmung sind jedoch keine Funktionen des Messengers abhängig, weshalb die Option jederzeit in den Einstellungen angepasst werden kann. [Sti14, Thr17]

Die asymmetrische Kryptografie der Anwendung ist über zwei Verschlüsselungsschichten umgesetzt: Eine Ende-zu-Ende-Verschlüsselung zwischen dem Sender und Empfänger der Nachricht, sowie einer weiteren für die Realisierung von *Perfect Forward Secrecy* bei der Netzwerkübertragung. Bei der zuletzt genannten Schicht kommen zufällige temporäre Schlüssel zwischen Client und Server zum Einsatz, die bei jedem Neustart der Anwendung neu generiert werden. Durch *Perfect Forward Secrecy* kann aufgezeichneter Netzwerkverkehr, selbst mit vorhandenem Schlüssel, im Nachhinein nicht entschlüsselt werden. Threema verfügt zwar über *Perfect Forward Secrecy* auf Netzwerk-Ebene, jedoch nicht auf Nachrichtenebene. [Thr17]

Für jede Nachricht wird (mittels *Curve25519*, einer Hashfunktion und einer *Nonce*) ein 256 Bit langer symmetrischer Schlüssel erstellt. Für die Verschlüsselung der Nachricht wird die Stromchiffre *XSalsa20* verwendet. Zudem wird ein 128 Bit langer *Message Authentication Code* (MAC) zur Entdeckung von Manipulationen hinzugefügt. [Thr17]

Bei erstmaliger Einrichtung der *Threema-ID* wird ein Schlüsselpaar für die Verschlüsselung der Nachrichten auf Basis von *Elliptic Curve Cryptography* (ECC) generiert. Die für die Generierung des Schlüsselpaares nötigen Zufallsdaten werden vom Zufallszahlengenerator des Smartphones bezogen und mit weiteren Zufallsdaten vermischt, die durch Wischen auf dem Bildschirm vom Nutzer selbst erzeugt werden. [Thr17]

5.10.2 Telegram

Telegram ist neben WhatsApp ein relativ weit verbreiteter Messenger mit mehr als 100 Millionen Nutzern (Stand Februar 2016), der von den aus Russland stammenden Brüdern Pavel und Nikolai Durov entwickelt wurde. Finanziert wird die Entwicklung der Anwendung aus dem Vermögen von Pavel Durov.

Der Firmensitz des Unternehmens wird verschleiert, um nach Aussage von Pavel Durov den möglichen Druck von Geheimdiensten auf Mitarbeiter zu verhindern. Zudem soll dadurch auch vermieden werden, dass Nutzerdaten für Dritte (wie für staatliche Stellen) zugänglich gemacht werden müssten. Dazu sei „*eine unkonventionelle rechtliche und organisatorische Struktur unseres Projekts*“ erforderlich. „*Teil dieser Struktur ist, dass wir niemals die exakten Positionen unserer Büros*“ [...] „*öffentlich machen*“. Mit der Veröffentlichung dieser Informationen würde sich das Unternehmen „*zu einem einfacheren Ziel für Datenanfragen machen*“. Das Kernteam der Entwickler würde lediglich zwei bis drei Monate an einem Ort arbeiten und dann zum nächsten Ort weiterziehen. Dadurch ist jedoch auch gänzlich unklar, welchen Datenschutzregeln sich Telegram gegenüber verpflichtet fühlt.
Die Server von Telegram sind auf viele Länder verteilt, weshalb für eine Weitergabe von Nutzerdaten richterliche Beschlüsse mehrerer Länder vorliegen müssten. [Hes17, Ver16]

Die kostenlose Open Source-Anwendung steht für die Betriebssysteme Android, iOS und Windows zur Verfügung und kann über den alternativen App-Store F-Droid bezogen werden.
Nachrichten werden bei Telegram nicht standardmäßig Ende-zu-Ende-verschlüsselt übertragen, dazu muss erst ein geheimer Chat gestartet werden, in dem dann auch Fotos, Videos und sonstige Dokumente verschlüsselt versendet werden können.
Gruppen-Chats sind nur unverschlüsselt möglich. [Tel17]

Die Registrierung und Identität ist bei Telegram an die Rufnummer gebunden, weshalb die Anwendung nicht anonym verwendet werden kann.
Zudem muss der Nutzer dem Zugriff und der Speicherung seiner Adressbucheinträge zustimmen. Diese Zustimmung ist nicht optional und kann nachträglich nicht geändert werden. Die Kontaktdaten werden auf Telegrams Servern dauerhaft gespeichert. [Hes17, Tel17]

Bei dem Quelltext der Client-Anwendung handelt es sich um quelloffene freie Software (Open Source), nicht jedoch bei dem Quellcode der Serverseite. [Tel17]

Telegram basiert auf dem selbst entwickelten *MTProto-Protokoll*. [Tel17]
Die Ende-zu-Ende-Verschlüsselung von Telegram kritisiert der Verschlüsselungsexperte Rüdiger Weis: „*Telegram benutze ausgerechnet die von der NSA entwickelte und inzwischen als gebrochen angesehene Hashfunktion SHA-1*“. Bei den kryptographischen Verfahren würde zudem kein sicheres Standardverfahren eingesetzt. Die kryptographischen Schlüssel werden nicht gänzlich zufällig generiert, sondern basieren teilweise auf dem Inhalt der Nachricht. [DN16]

Die Eigenschaft *Perfect Forward Secrecy* erfüllt Telegram nur in abgeschwächter Form: Der Schlüssel für die Verschlüsselung wird erst dann getauscht, wenn er mehr als 100 Mal oder länger als eine Woche verwendet wurde. [Tel17]

5.10.3 Signal

Der kostenlose Instant-Messenger Signal wurde von der Organisation Open Whisper Systems, die sich aus Spenden und Förderungen finanziert, zunächst unter dem Namen TextSecure veröffentlicht. Die Anwendung, mit der neben Textnachrichten auch Bilder, Videos, Audiodateien und Kontaktdaten verschlüsselt versendet werden können, ist für Android und iOS verfügbar. Zudem sind verschlüsselte Gruppenchats und Video-Anrufe möglich. [Hes17, Ope16]

Der komplette Quellcode von Signal für die Client- und die Server-Anwendung ist auf GitHub frei verfügbar und wurde 2016 von einem unabhängigen akademischen Team analysiert, wobei sie als sicher eingestuft wurde und Anforderungen wie *Perfect Forward Secrecy* erfüllt. [CGCD+16]
Die Nachrichten werden über die Server von Open Whisper Systems geleitet, die sich in den USA befinden. Allerdings setzt Signal auf Datensparsamkeit und konnte so auf eine Anordnung eines US-Bundesbezirksgerichts, die den Anbieter zur Herausgabe von Nutzerdaten verpflichtet hatte, lediglich die Zeitpunkte, wann der Signal-Account erstellt wurde und wann sich der Nutzer zuletzt mit den Signal-Servern verbunden hatte, zur Verfügung stellen. [Hes17, Mü17b]

Seit Februar 2017 kann Signal auch ohne Google-Play-Dienste installiert werden. Allerdings ist ein Signal-Account stets an eine Handynummer gebunden, mit der sich der Nutzer beim ersten Start der Anwendung anmelden muss. [Hes17, Mü17b]

Bei der Installation wird der Zugriff auf das Adressbuch angefordert. Verweigert man den Zugriff, muss man die Telefonnummern der Empfänger per Hand eintippen und kann sie nicht in der Kontaktliste speichern. Nach Angaben von Signal werden Kontaktdaten anonymisiert auf deren Servern abgeglichen und anschließend wieder gelöscht. Der regelmäßige Abgleich der Kontaktdaten mit dem Signal-Server kann unter Android in den Konteneinstellungen deaktiviert werden. [Hes17]

Bei der asynchronen Ende-zu-Ende-Verschlüsselung von Nachrichten kommt das Signal-Protokoll (ehemals Axolot-Protokoll), welches auf *Curve25519*, *AES-256* und *HMAC-SHA256* basiert, zum Einsatz. [Bö14, Ope16]
Das Verschlüsselungsprotokoll von Signal gilt als „*Goldstandard*“ in der Kryptoszene und wurde auch von WhatsApp und dem Facebook-Messenger übernommen. Open Whisper Systems gibt keine Auskunft über seine Nutzerzahlen. [Hes17]

5.10.4 Zusammenfassung

Das Resultat der untersuchten Merkmale bei den drei Instant-Messengern ist in der folgenden *Tabelle 4 Merkmale der Instant-Messenger* nochmals zusammengefasst: Threema ist nicht vollständig Open Source und erfüllt *Perfect Forward Secrecy* nur auf Netzwerk-Ebene, jedoch nicht auf Nachrichtenebene.
Telegram erfüllt keines der Merkmale vollständig, da nur die Client-Anwendung Open Source ist, aber nicht die Server-Anwendung und *Perfect Forward Secrecy* nur in abgeschwächter Form zum Einsatz kommt. Da ein Signal-Account stets an eine Handynummer gebunden ist, erfüllt dieser Messenger alle Merkmale mit Ausnahme der anonymen Kennung. Wird jedoch der Zugriff auf das Telefonbuch verweigert, kann der Messenger nur mit hohem Komfortverlust verwendet werden.

Neben den drei genannten Instant-Messengern, gibt es noch weitere Messenger, wie myEnigma, Hoccer, Kontalk, SIMSme oder Wickr, die ebenfalls Kriterien zum Schutz der persönlichen Daten erfüllen.

Merkmal	Threema	Telegram	Signal
anonyme Kennung	ja	nein	nein
immer Ende-zu-Ende verschlüsselt	ja	nein	ja
kein Telefonbuch-Zugriff	ja	nein	ja
Open Source	teils	teils	ja
Perfect Forward Secrecy	teils	teils	ja

Tabelle 4: Merkmale der Instant-Messenger

5.11 Zusammenfassung

Die Maßnahmen, mit denen ein Nutzer seine Daten und Privatsphäre schützen kann, sind, wie die Betrachtungen in diesem Kapitel gezeigt haben, sehr unterschiedlich und dementsprechend mit mehr oder weniger Aufwand und Komforteinbußen verbunden.

Wie in *Abschnitt 5.1* aufgeführt, ist ein umsichtiger und verantwortungsvoller Umgang mit den eigenen Daten Grundvoraussetzung für den Schutz eben dieser. Ein Anwender sollte bereits bei der Auswahl von Hard- und Software darauf achten, ob Eigenschaften wie Open Source oder Verschlüsselungsmechanismen gegeben sind. Es sollten solche Produkte verwendet werden, bei denen die Privatsphäre der Nutzer geachtet wird und z. B. keine Nutzerdaten gespeichert werden. Darüber hinaus sind auch die Interessen der Hersteller entscheidend, wie sie sich finanzieren und welche Gesetzeslage mit dem Unternehmens- und Serverstandort verbunden ist. Kriterien, die bei der Auswahl einer Suchmaschine bzw. bei einem Instant-Messenger relevant sein können, wurden in *Abschnitt 5.4* bzw. *Abschnitt 5.10* dargelegt.

Soweit möglich, sollten Einstellungen vorgenommen werden, durch die weniger Daten erfasst oder an Dritte weitergegeben werden können. Aber auch Daten, die für das Nutzer-Tracking verwendet werden können, sollten regelmäßig gelöscht werden. Die verschiedenen Tracking-Methoden, mittels Cookies, Fingerprinting oder Ultraschall erfordern unterschiedliche Schutzmaßnahmen, die sich auch gegenseitig behindern können. So können die individuellen Listen bei Whitelists, welche unter anderem gegen Cookies eingesetzt werden können, für die Erstellung eines eindeutigen Fingerprints genutzt werden.
Dennoch ist es wichtig, Maßnahmen zu ergreifen, die dem Datenschutz dienen. Je mehr Menschen ebenfalls solche Maßnahmen einsetzen, desto weniger können diese als identifizierende Merkmale für das Fingerprinting verwendet werden. So tritt

nicht nur eine Verbesserung für den eigenen Datenschutz, sondern auch gegenüber der Allgemeinheit ein.

Durch die Verwendung des Private-Mode werden Daten im Browser nur temporär bis zum Sitzungsende gespeichert und dann wieder gelöscht. Dadurch werden sowohl eTags als auch Cookies (zumindest diejenigen, auf die der Browser Zugriff hat) mit dem Beenden des Browsers gelöscht. Third-Party Cookies sollten generell blockiert werden, da sie ausschließlich für das Nutzer-Tracking im Einsatz sind. Neben der Browser-Funktion sollten zusätzlich Add- und Tracking-Blocker, wie *uBlock Origin* und *Privacy Badger* verwendet werden, um externe Dienste zu blockieren. Zudem sollten JavaScript und Flash entweder generell blockiert oder nur dann zulassen werden, wenn die entsprechenden Skripte tatsächlich erforderlich sind. Zudem sollten Flash-Cookies über den Adobe Einstellungs-Manager regelmäßig gelöscht werden.

Bei privaten Recherchen im Internet sollte stets ein Anonymisierungsdienst, wie der Tor-Browser oder der JonDoBrowser, verwendet werden. Wie in *Abschnitt 5.2.1* und *Abschnitt 5.2.2* beschrieben, kann ein Nutzer durch das dabei eingesetzte Onion Routing bzw. die Mix-Kaskaden im Internet surfen, ohne dabei Informationen wie die IP-Adresse preiszugeben. Zudem kann man sich dadurch auch gegen die Wiedererkennung durch das Fingerprinting schützen.

Wie in *Abschnitt 5.9* beschrieben, sollten bei mobilen Geräten die Berechtigungen der installierten Apps soweit wie möglich eingeschränkt werden. Auch die Menge der genutzten Accounts und Apps sollte möglichst gering gehalten werden. Die automatische Synchronisation mit dem Plattform-Account sollte, ebenso wie nicht benötigte Funktionen (GPS, WLAN und Bluetooth) deaktiviert werden. Android-Nutzer, die über technisches Fachwissen verfügen oder sich dieses aneignen möchten, sollten ihr Gerät rooten. Dadurch kann beispielsweise Bloatware deinstalliert werden. Die meisten Kontrollmöglichkeiten erhält ein Anwender von Android-Geräten durch die Installation eines Custom-ROMs, wodurch mobile Geräte ohne Plattform-Account und proprietäre Apps genutzt werden können.

Neben den in diesem Kapitel genannten Schutzmaßnahmen gibt es noch viele andere Möglichkeiten seine digitalen Daten zu schützen. Dazu gehören insbesondere die Verwendung eines Proxys oder eines Virtual Private Networks (VPN), aber z. B. auch die Entfernung der Metadaten bei Anwendungsdateien.

Zwar ist ein vollkommener und effektiver Schutz gegen die Überwachung von staatlichen Einrichtungen oder Internetkonzernen, die über enorme Ressourcen verfügen, äußerst unwahrscheinlich. Dennoch sollte jeder Nutzer Verantwortung übernehmen und entsprechende Maßnahmen zum Schutz der Daten und der Privatsphäre ergreifen. Verantwortung hat man dabei nicht nur gegenüber den eigenen Daten, sondern auch gegenüber den Daten, die man von anderen Personen gespeichert hat.

6 Fazit

Das Aufhalten der Digitalisierung ist, ebenso wie ein Verzicht auf informationsverarbeitende Systeme, weder zielführend noch möglich. Jedoch ist die Frage des Mitwirkens bezüglich der Entwicklung und des Umgangs mit diesen Systemen entscheidend. Ein wesentlicher Aspekt dabei ist, dass Anwender ein tieferes Bewusstsein und Verständnis sowohl gegenüber ihren Freiheitsrechten, den Methoden der Datenerhebung, als auch über die Erstellung von Nutzerprofilen, der Berechnung von Scoring-Werten oder von *Predictive Analytics* entwickeln müssen. Insbesondere die daraus erwachsenden Gefahren müssen stärker ins öffentliche Blickfeld rücken.

Wie in *Kapitel 2* gezeigt wurde, sind die Rechtslage und damit auch die Grundlagen zum Datenschutz in jedem Staat unterschiedlich geregelt. Dabei gilt das Datenschutzniveau innerhalb der Europäischen Union als angemessen, ebenso wie das in der Schweiz, Kanada, Argentinien, Guernsey und auf der Isle of Man. Während das Datenschutzniveau innerhalb der EU in jüngster Zeit angehoben wurde, sank hingegen das deutsche, unter anderem wegen Einführung von ZITiS, der Quellen-TKÜ oder der Online-Durchsuchung stark ab. In den Vereinigten Staaten wird das Datenschutzniveau als niedrig eingestuft; vergleichbare Regelungen auf Bundesebene, wie sie z. B. innerhalb Deutschlands bestehen, gibt es in den USA nicht.

Verschiedene Methoden der Datenerfassung wurden in *Kapitel 3* beschrieben. Über die darin beschriebenen Technologien, wie Cookies, eTags oder Fingerprinting können Nutzer im Internet wiedererkannt werden, wodurch ihre Gewohnheiten und ihr Verhalten verfolgt werden können. Darüber hinaus können einem Nutzer durch das Ultraschall-Tracking verschiedene Geräte zugeordnet werden. Auch werden Informationen, die bei der Nutzung des Internets entstehen, verstärkt mit Informationen der Offline-Welt kombiniert.
Besonders staatliche Einrichtungen nutzen in Software enthaltene bzw. integrierte Hintertüren und Schwachstellen (*Abschnitt 3.1*), um weltweit Informationen über Bürger zu sammeln. Durch die Enthüllungen um den ehemaligen NSA-Mitarbeiter

Edward Snowden wurden insbesondere konkrete Methoden dieser Institution öffentlich. So werden auch in Deutschland Schwachstellen genutzt, um verschlüsselte Nachrichten mitlesen zu können.
Wie in *Abschnitt 3.6* dargelegt, sind insbesondere mobile Geräte, wie Smartphones und Tablets, für das Sammeln personenbezogener Daten und die Verfolgung ihrer Nutzer anfällig. Dies liegt an der Fülle von Daten, die auf diesen Geräten verarbeitet werden und auf welche die installierten Apps zugreifen können. Ferner senden mobile Geräte in der Regel permanent Signale aus, die ebenfalls zum Nutzer-Tracking verwendet werden können.

Die so gesammelten Daten können für die Nutzerprofilierung verwendet werden, wie in *Kapitel 4* beispielhaft gezeigt wurde. Als Begründung für das Sammeln und Auswerten von Nutzerdaten wird einerseits die Aufrechterhaltung der Sicherheit und Schutz vor Terrorismus genannt. Zum Anderen dienen diese Methoden dem finanziellen Profit, indem personalisiert Werbung angezeigt oder Informationen weiterverkauft werden.
Die so errechneten Nutzerprofile geben Auskunft über Charaktereigenschaften, Aufenthaltsorte, Gewohnheiten, das soziale Umfeld, die finanzielle Situation oder die psychische und physische Verfassung von Menschen. Auch können mittels *Predictive Analytics* auch immer mehr Prognosen über zukünftige Verhaltensweisen von Personen getroffen werden.
Die Verwendungsmöglichkeiten dieser Informationen sind nahezu grenzenlos und werden schon heute vermehrt zur Beurteilung von Menschen eingesetzt. Häufig ist dabei nicht transparent, welche Daten genau über einen Nutzer erfasst werden, wohin diese Daten fließen und wie die Algorithmen zur Datenauswertung arbeiten.

Ein vollkommener Schutz gegen die weitreichende technologische Übermacht von Internetkonzernen und staatlichen Einrichtungen ist äußerst unrealistisch. Dennoch kann die erfasste Datenmenge reduziert werden, wenn Empfehlungen zum digitalen Selbstschutz, wie in *Kapitel 5* beschrieben wurden, angewendet werden. Dabei müssen jedoch bisherige Gewohnheiten zuweilen abgelegt oder verändert und Einbußen beim Komfort in Kauf genommen werden. Der Schutz der Privatsphäre in der digitalen Welt ist mit erheblichem Mehraufwand verbunden, der besonders Menschen, die wenig Erfahrung im Umgang mit der Informationstechnologie haben, von entsprechenden Maßnahmen abschreckt. Bereits bei der Auswahl von Hard- und Software sollte auf solche Merkmale geachtet werden, die sowohl Transparenz als auch Datenschutz gewährleisten. Aber auch das regelmäßige Löschen von Daten,

die für das Nutzer-Tracking verwendet werden können und das Vornehmen datenschutzfreundlicher Einstellungen ist ebenso relevant wie die Berücksichtigung der Datenvermeidung oder -verschlüsselung.
Kriterien, die bei der Auswahl einer Suchmaschine von Relevanz sind, wurden in *Abschnitt 5.4* dargelegt, was hingegen bei der Wahl eines Instant-Messengers beachtet werden sollte, wurde in *Abschnitt 5.10* ausgeführt. Auch etwaige Maßnahmen zur Vermeidung von Ultraschall-Tracking, Cookies, eTags und Fingerprinting können zum Schutz der Privatsphäre beitragen, wenngleich sich diese Maßnahmen unter Umständen gegenseitig behindern können.

7 Ausblick

Der Ausbau der Informationsinfrastruktur und damit einhergehend die Möglichkeiten zur Überwachung werden auch in Zukunft durch staatliche Einrichtungen und Internetkonzerne vorangetrieben werden. Dabei bergen insbesondere die Erfassung der Daten über immer mehr Lebensbereiche des Menschen hinweg und die wachsende Vernetzung dieser Daten Gefahren. Häufig ist dabei intransparent, wer über welche Daten verfügt, welche Prognosen oder Scorings aus den Daten berechnet werden und welche Auswirkungen dies auf den einzelnen Menschen hat oder zukünftig haben wird. So wies die Juristin und Schriftstellerin Juli Zeh als Reaktion auf die NSA-Affäre bereits 2013 in einem offenen Brief an die Bundeskanzlerin Angela Merkel auf die Tragweite dieser Entwicklungen hin:
„*Wir können uns nicht wehren. Es gibt keine Klagemöglichkeit, keine Akteneinsicht. Während unsere Privatleben transparent gemacht wird, behaupten die Geheimdienste ein Recht auf maximale Intransparenz ihrer Methoden. Mit anderen Worten: Wir erleben einen historischen Angriff auf unseren demokratischen Rechtsstaat, nämlich die Umkehrung des Prinzips der Unschuldsvermutung hin zu einem millionenfachen Generalverdacht.*“ Juli Zeh, [Zeh13]

Auf die Frage, ob Konsequenzen auf die Handlungen des BND, die gegen geltendes Gesetz verstoßen haben, folgen würden, sagte der Geheimdienstkoordinator des Bundeskanzleramts, Klaus-Dieter Fritsche: „*Es gab keinen Grund für disziplinarrechtliche Maßnahmen*“. [Bie17]
Vier Jahre nach der NSA-Affäre kam der Generalbundesanwalt zu dem Ergebnis, dass es keinen Anfangsverdacht für die Massenüberwachen durch Geheimdienste gibt. Man habe keine Anhaltspunkte finden können, dass „*Nachrichtendienste eigenmächtig den deutschen Telekommunikations- und Internetverkehr rechtswidrigerweise systematisch und massenhaft überwachen*“ würden. [Bis17]

Diese Entscheidungen lassen keine Bestrebungen für eine Richtungsänderung im Umgang mit personenbezogenen Daten durch staatliche Institutionen erkennen.

Statt der Einführung von Gesetzen und Kontrollinstanzen, um die Überwachungsmethoden einzugrenzen oder gar ganz zu unterbinden, nutzen deutsche Staatsorgane selbst solche Methoden und schaffen entsprechende Gesetze, um diese zu legitimieren.

Auch Überlegungen führender Politiker der amtierenden Bundesregierung sehen nicht vor, Maßnahmen zur Überwachung bzw. deren Legitimierung einzugrenzen. So äußerte Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz, die Empfehlung, die **Vorratsdatenspeicherung** zukünftig auszuweiten, wie das nachstehende Zitat erkennen lässt: „*Mich würde interessieren: Wer schaut sich gerade auf seinem Computer Enthauptungsvideos an, die auf einem Server in Malaysia liegen. Ich würde gern die IP-Adressen bekommen und mit unserer Gefährderdatenbank abgleichen.*“ [Kre17b]
Darüber hinaus befürwortet Maaßen einen einfacheren Zugriff auf Nutzerdaten von Messengerdiensten wie WhatsApp oder Telegram. Derzeit ist auf Basis des G10-Gesetzes lediglich eine Überwachung in Einzelfällen möglich. Maaßen plädiert hingegen für eine Überwachung der gesamten Kommunikation zwischen Gebieten, die vom sogenannten Islamischen Staat besetzt sind und Deutschland. [Kre17b]

Im Rahmen eines Pilotprojekts am Bahnhof Berlin Südkreuz werden Fahrgäste und Passanten per Video erfasst und auf Basis einer Bilddatenbank nach Möglichkeit identifiziert. Bei einem Erfolg des Projekt soll dieses Modell der **intelligenten Videoüberwachung** laut Bundesinnenminister Thomas de Maizière flächendeckend eingeführt werden. Aktuell wird eine Erkennungsrate von 70% und eine Fehlerquote unter einem Prozent erzielt, was nach Aussagen de Maizières als erfolgreich zu werten ist. Diesbezüglich sagte der damalige Präsident des Bundeskriminalamts Jörg Zierke im Rahmen einer Testphase zur Videoüberwachung am Mainzer Hauptbahnhof 2007: „*Der Einsatz dieser Systeme ist nur sinnvoll, wenn die Trefferquote bei nahezu 100 Prozent liegt.*“ [Kur17b, Sch17a]
Neben der Gesichtserkennung könne laut de Maizière aber auch der Einsatz von **DNA-Analysen** zur Verbesserung der Sicherheitslage führen. In dem Interview *Leitlinien für einen starken Staat in schwierigen Zeiten* wird de Maizières Interesse am Einsatz von DNA-Analysen deutlich: „*Der starke Staat muss mit den technischen Entwicklungen und Nutzungen Privater Schritt halten, sie aber auch für seine Arbeit nutzen können. Dies gilt auch für den bislang rechtlich stark limitierten Einsatz der DNA-Analyse. Die biometrische Auswertung etwa durch Gesichtserkennung*

muss entschieden vorangebracht werden. Eine Fahndung mit Gesichtserkennung, etwa nach einem flüchtigen Terroristen, ist ein wichtiges Instrument.“ [Fra17]

Auch Unternehmen arbeiten verstärkt mit biometrischen Daten. Beispielsweise hat die israelische Firma Faception Interesse daran, Terroristen automatisiert am Gesicht zu erkennen. Diese Firma entwickelt eine Software, mit deren Hilfe es möglich ist, eine Persönlichkeitsprofilierung in Echtzeit aufgrund der Erkennung und Auswertung von Gesichtern zu erstellen. Dabei werden auf Grundlage von Fotos, die z. B. Terroristen abbilden, andere Personen ermittelt, die ähnlich aussehen. Durch die Software sei es mit hoher Genauigkeit möglich, Charakterzüge aus Gesichtern herauszulesen. Das heißt, es wird dabei von einem Zusammenhang zwischen optischen Merkmalen und dem Charakter eines Menschen ausgegangen. [Rö16]

Neben staatlichen Einrichtungen und Unternehmen möchten auch die Verbraucher selbst moderne Technologien einsetzen, um den Komfort zu erhöhen oder Sicherheitsaspekte zu verbessern. Häufig werden jedoch beim Einsatz dieser Technologien Bedenken bezüglich des Datenschutzes außer Acht gelassen. Beispielsweise wird nach Angaben der *Verbraucherzentrale Bundesverband* der Absatz von Smart-Home-Geräten deutlich ansteigen. Bis 2020 soll die Zahl der deutschen Haushalte mit zentraler Steuerung auf 2,4 Millionen ansteigen. Werden dabei funkfähige Geräte jedweder Art berücksichtigt, nutzt im Jahr 2020 eine jede Person durchschnittlich zehn dieser Geräte. Für 2020 werden mehr als 800 Millionen vernetzte Geräte in Deutschland prognostiziert. [Ver17]
Viele Verbraucher wollen die Vorteile der modernen Technologie für ihre Bedürfnisse nutzen, z. B. auch, um die Sicherheit ihrer Kindern auf dem Schulweg zu erhöhen. In Wolfsburg und Ludwigsburg sind Pilotprojekte, unter anderem in Kooperation mit Volkswagen und dem Schulranzen-Hersteller Scout, geplant, bei dem der Schulweg von Kindern überwacht werden soll. Dabei sollen Schulkinder stets einen Tracker, in Form eines Smartphones oder GPS-Senders bei sich tragen, über welchen die Kinder permanent von ihren Eltern geortet werden können. Die wesentliche Funktion soll jedoch darin bestehen, dass Autofahrer anhand der Standortdaten gewarnt werden, wenn sich Kinder in der Nähe befinden. Aktuell müssen Autofahrer dazu noch eine App installieren, zukünftig soll eine Warnung jedoch über das Boardsystem des Autos erfolgen. [GH17]

Ein Szenario mit viel größerer Tragweite wird gerade in China und Shanghai erprobt, bei dem umfassende Instrumente zur Überwachung der Bevölkerung eingesetzt wer-

den. In Shanghai wurde diesbezüglich im November 2016 die App *Ehrliches Shanghai* veröffentlicht. Diese App hat Zugriff auf bis zu 3000 Datensätze, die aus ca. 100 unterschiedlichen, staatlichen Datenbeständen stammen, wobei diese zukünftig um kommerziell gesammelte Daten erweitert werden sollen. Zur Registrierung gibt ein neuer Nutzer seine nationale Identifikationsnummer ein, woraufhin dessen Gesicht gescannt wird und alle verfügbaren Daten über ihn ausgewertet werden. Auf Basis seiner Kreditwürdigkeit und Rechtstreue erhält der Nutzer einen ermittelten Wert, den Sozialkredit; je höher dieser ist, desto mehr Annehmlichkeiten für den Nutzer, wie beispielsweise günstigere Preise beim Kauf eines Flugtickets. Mit einem schlechten Score hingegen können diverse Mali verbunden sein, z. B. dass ein Nutzer keinen Büchereiausweis mehr erhält. Die Teilnahme an dem Sozialkreditsystems ist bislang freiwillig; allerdings ist bereits eine landesweite Ausweitung geplant, wozu bis 2020 alle Datenbanken des Landes vereint werden sollen. [Deu17, Lob17]

Die Vermarktung persönlicher Daten wird stetig vorangetrieben, wodurch immer mehr Beurteilungen von Menschen bereits heute häufig auf Algorithmen und Wahrscheinlichkeiten beruhen. Entscheidungen, die Auswirkungen auf das Leben der Menschen haben, hängen immer häufiger von berechneten Scoring-Werten ab. So werden über US-Bürger bereits bis zu 8000 verschiedene Scoring-Werte erhoben, bei EU-Bürgern sind es etwa 600 Werte. Beispielsweise gibt es bei Versicherungen Rabatte, wenn Krankenversicherte ihre Vitalwerte oder Kfz-Versicherte ihr Fahrverhalten überwachen lassen. [Kle17]
Eine mögliche Gefahr besteht hierbei darin, dass dieser Zugriff und die Auswertung der Nutzerdaten in Zukunft nicht mehr auf freiwilliger Basis geschieht, sondern Voraussetzung dafür wird, dass eine Person überhaupt versichert wird. Darüber hinaus können sowohl Daten, als auch Prognosen, die auf Wahrscheinlichkeiten beruhen, fehlerhaft sein. In der Regel sind sowohl die Parteien, die Zugriff auf Nutzerdaten erhalten, als auch die Berechnungsgrundlagen der Scoring-Werte vollkommen intransparent. Zu den Folgen der flächendeckenden Überwachung und den Scoring-Systemen sei auch eine *soziale Abkühlung* (*Social Cooling*) genannt. Diese führt aus Angst vor negativen Auswirkungen dazu, dass Menschen ihre Meinung nicht mehr frei im Internet äußern, also zu einer individuellen Selbstzensur und risikovermeidendem Verhalten. Zudem vermeiden es Menschen, Artikel mit bestimmten Inhalten aufzurufen. So sanken z. B. nach den Snowden-Enthüllungen die Abrufzahlen für Artikel, die Inhalte zu Terror-Organisationen enthielten, rapide. [Kle17]

„*Ein Mensch, der observiert wird, ist kein freier Mensch mehr.*“ Juli Zeh, [Don13]

Literaturverzeichnis

[AEE+14] Acar, Gunes ; Eubank, Christian ; Englehardt, Steven ; Juarez, Marc ; Narayanan, Arvind ; Diaz, Claudia: *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*. https://dl.acm.org/citation.cfm?id=2660347. Version: 2014

[Ale17] Aleksandersen, Daniel: *Fluxfonts – font fingerprint cloaking*. https://www.ctrl.blog/entry/fluxfonts. Version: 2017. – abgerufen am 27.12.2017

[AQWR17] Arp, Daniel ; Quiring, Erwin ; Wressnegger, Christian ; Rieck, Konrad: *Privacy Threats through Ultrasonic Side Channels on Mobile Devices*. http://christian.wressnegger.info/content/projects/sidechannels/2017-eurosp.pdf. Version: 2017

[BB16] Breithut, Jörg ; Böhm, Markus: *Schleichend zum Überwachungsstaat*. http://www.spiegel.de/netzwelt/netzpolitik/deutschland-schleichend-zum-ueberwachungsstaat-a-1121162.html. Version: 2016. – abgerufen am 29.11.2016

[BB17] Beuth, Patrick ; Biermann, Kai: *Dein trojanischer Freund und Helfer*. http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss. Version: 2017. – abgerufen am 17.07.2017

[Bec17a] Becker, Leo: *Gegen Fingerprinting: Apple friert Safaris User Agent ein*. https://www.heise.de/mac-and-i/meldung/Gegen-Fingerprinting-Apple-friert-Safaris-User-Agent-ein-3925679.html. Version: 2017. – abgerufen am 27.12.2017

[Bec17b] Becker, Leo: *Safari 11: Apples Browser will Werbe-Tracking unterbinden.* https://www.heise.de/mac-and-i/meldung/Safari-11-Apples-Browser-will-Werbe-Tracking-unterbinden-3736398.html. Version: 2017. – abgerufen am 27.12.2017

[Bei17] Beiersmann, Stefan: *Android: Mehr als 75 Prozent aller Android-Apps spionieren Nutzer aus.* http://www.zdnet.de/88319773/android-mehr-als-75-prozent-aller-android-apps-spionieren-nutzer-aus/?inf_by=5a52504c681db8c5468b4889. Version: 2017. – abgerufen am 07.01.2018

[Ber17a] Berger, Daniel: *Dezentral und Open Source: Ist Mastodon das bessere Twitter?* https://www.heise.de/newsticker/meldung/Dezentral-und-Open-Source-Ist-Mastodon-das-bessere-Twitter-3675432.html. Version: 2017. – abgerufen am 29.11.2017

[Ber17b] Bergert, Denise: *Librem 5: 2,1 Millionen US-Dollar für freies Smartphone.* https://www.heise.de/newsticker/meldung/Librem-5-2-1-Millionen-US-Dollar-fuer-freies-Smartphone-3870473.html. Version: 2017. – abgerufen am 20.01.2018

[Beu06] Beutelspacher, Albrecht: *Moderne Verfahren der Kryptographie : von RSA zu Zero-knowledge.* 6., verb. Aufl. Wiesbaden : Vieweg, 2006 (Studium). http://www.gbv.de/dms/ilmenau/toc/506614468beute.PDF. – Literaturverz.

[Beu17] Beuth, Patrick: *Der Spion, der aus der Küche kam.* http://www.zeit.de/digital/datenschutz/2017-07/roomba-staubsauger-roboter-daten-wohnung-verkaufen. Version: 2017. – abgerufen am 18.10.2017

[Bie15] Biermann, Kai: *Diese Spähsoftware findet jedes Passwort.* http://www.zeit.de/digital/datenschutz/2015-08/bfv-verfassungsschutz-was-kann-xkeyscore. Version: 2015. – abgerufen am 13.02.2018

[Bie17] Biermann, Kai: *Kanzleramt erklärt NSA-Affäre endgültig für beendet.* http://www.zeit.de/politik/deutschland/2017-02/ns

a-skandal-angela-merkel-kanzleramt-bnd-geheimdienste/komplettansicht. Version: 2017. – abgerufen am 24.02.2018

[Bis14] Biselli, Anna: *How-To Analyze Everyone – Teil VIII: Browser-Fingerprints und Informationskrümel ohne Cookies.* https://netzpolitik.org/2014/how-to-analyze-browser-fingerprinting-bhaviour-tracking/. Version: 2014. – abgerufen am 26.12.2017

[Bis15] Biselli, Anna: *Mehr Details über den Aufbau und die Funktionen der Überwachungssuchmaschine XKeyscore veröffentlicht.* https://netzpolitik.org/2015/mehr-details-ueber-den-aufbau-und-die-funktionen-der-ueberwachungssuchmaschine-xkeyscore-veroeffentlicht/. Version: 2015. – abgerufen am 13.02.2018

[Bis17] Biselli, Anna: *Nichts gefunden: Auch der Generalbundesanwalt hat NSA-Affäre beendet.* https://netzpolitik.org/2017/nichts-gefunden-auch-der-generalbundesanwalt-hat-nsa-affaere-beendet/. Version: 2017. – abgerufen am 25.01.2018

[Ble16] Bleich, Holger: *EU-Datenschutzverordnung gilt ab Mai 2018.* https://www.heise.de/newsticker/meldung/EU-Datenschutzverordnung-gilt-ab-Mai-2018-3197099.html. Version: Mai 2016. – abgerufen am 16.12.2016

[Bri17] Briegleb, Volker: *WannaCry: Was wir bisher über die Ransomware-Attacke wissen.* https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html. Version: Mai 2017. – abgerufen am 13.07.2017

[Bun] Bundesrepublik Deutschland: *Gesetze im Internet.* https://www.gesetze-im-internet.de/. – abgerufen am 10.07.2017

[Bun13] Bundesamt für Sicherheit in der Informationstechnik: *Glossar und Begriffsdefinitionen.* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt

/Glossar/glossar_node.html. Version: 2013. – abgerufen am 09.07.2017

[Bun16] Bundeszentrale für politische Bildung : *Vor 35 Jahren: Datenschutzkonvention des Europarates*. http://www.bpb.de/politik/hintergrund-aktuell/219563/datenschutzkonvention. Version: 2016. – abgerufen am 29.01.2018

[BÖ17] BÖRSENMEDIEN AG: *Alphabet AKTIE*. http://www.deraktionaer.de/aktien/US02079K3059.htm. Version: 2017. – abgerufen am 29.10.2017

[Bö14] Böck, Hanno: *Snowden empfiehlt Textsecure und Redphone*. https://www.golem.de/news/verschluesselung-snowden-empfiehlt-textsecure-und-redphone-1403-105052.html. Version: 2014. – abgerufen am 17.03.2017

[CGCD+16] Cohn-Gordon, Katriel ; Cremers, Cas ; Dowling, Benjamin ; Garratt, Luke ; Stebila, Douglas: *A Formal Security Analysis of the Signal Messaging Protocol*. https://eprint.iacr.org/2016/1013.pdf. Version: 2016

[Chr14] Christl, Wolfie: *Kommerzielle digitale Überwachung im Alltag*. http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Version: 2014

[Deu17] Deuber, Lea: ÜBERWACHUNG Orwell auf Chinesisch. In: *Wirtschafts-Woche* (2017), Nr. 017. https://www.wiso-net.de/document/WW__43773038-9429-4BB8-BAE1-41F83287FE31. – abgerufen am 05.12.2017

[Die] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: *Transparente Software - eine Voraussetzung für datenschutzfreundliche Technologien*. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/TransparenteSoftware.html. – abgerufen am 26.11.2017

[Die07] Diedrich, Oliver: *Die Woche: Was ist Open Source?* https://www.heise.de/ct/artikel/Die-Woche-Was-ist-Open-Source-222121.html. Version: 2007. – abgerufen am 26.11.2017

[Dig16] Digitalcourage e.V.: *E-Mails verschlüsseln wird immer einfacher.* https://digitalcourage.de/digitale-selbstverteidigung/e-mails-verschluesseln-wird-immer-einfacher. Version: 2016. – abgerufen am 11.12.2017

[dig17] digitalcourage e.V.: *Befreien Sie Ihr Smartphone!* https://digitalcourage.de/digitale-selbstverteidigung/befreien-sie-ihr-smartphone. Version: 2017. – abgerufen am 10.01.2018

[DN16] Dörner, Stephan ; Nagel, Lars-Marten: *Sicherheitslecks beim Messenger-Dienst Telegram?* https://www.welt.de/wirtschaft/webwelt/article152206932/Sicherheitslecks-beim-Messenger-Dienst-Telegram.html. Version: 2016. – abgerufen am 24.03.2017

[Don13] Donaukurier: *Ein observierter Mensch ist nicht frei.* http://www.donaukurier.de/nachrichten/digital/datenschutz/Frau-wochennl302013-Juli-Zeh-im-Interview-Ein-observierter-Mensch-ist-nicht-frei;art251975,2793492. Version: 2013. – abgerufen am 24.01.2018

[Duca] DuckDuckGo: *Advertising and Affiliates.* https://duck.co/help/company/advertising-and-affiliates. – abgerufen am 05.10.2017

[Ducb] DuckDuckGo: *Einstellungen.* https://duckduckgo.com/settings. – abgerufen am 05.10.2017

[Ducc] DuckDuckGo: *Welcome to the DuckDuckGo Help library!* https://duck.co/help. – abgerufen am 04.10.2017

[Duc12] DuckDuckGo: *We don't collect or share personal information.* https://duckduckgo.com/privacy. Version: 2012. – abgerufen am 04.10.2017

[Duc13] DuckDuckGo: *Architecture*. https://duck.co/help/company/architecture. Version: 2013. – abgerufen am 05.10.2017

[Eck10] Eckersley, Peter: *How Unique Is Your Web Browser?* https://panopticlick.eff.org/static/browser-uniqueness.pdf. Version: 2010

[Ele15] Electronic Frontier Foundation: *About Panopticlick*. https://panopticlick.eff.org/about. Version: 2015. – abgerufen am 18.12.2017

[Ele17] Electronic Frontier Foundation: *End-to-end encryption*. https://ssd.eff.org/en/glossary/end-end-encryption. Version: 2017. – abgerufen am 11.12.2017

[Eng17] Enge, Stefanie: *Blackphone 2 im Test: das Fort Knox der Smartphones*. https://curved.de/reviews/blackphone-2-im-test-das-fort-knox-der-smartphones-452317. Version: 2017. – abgerufen am 21.01.2018

[Eur00] Europäische Union: *CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION*. http://www.europarl.europa.eu/charter/pdf/text_de.pdf. Version: 2000. – abgerufen am 09.07.2017

[Eur17] European Commission: *Proposal for a Regulation on Privacy and Electronic Communications*. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications. Version: 2017. – abgerufen am 10.10.2017

[F-D17] F-Droid Limited: *Was ist F-Droid?* https://f-droid.org/de/. Version: 2010-2017. – abgerufen am 10.01.2018

[Fan18] Fanta, Alexander: *Android sammelt Daten über Bluetooth, auch wenn Bluetooth ausgeschaltet ist*. https://netzpolitik.org/2018/android-sammelt-daten-ueber-bluetooth-auch-wenn-bluetooth-ausgeschalten-ist/. Version: 2018. – abgerufen am 27.01.2018

[FH18] Ferrari-Herrmann, Eric: *Custom-ROMs für Android im Überblick.* https://www.androidpit.de/die-besten-custom-roms-android-varianten-im-ueberblick. Version: 2018. – abgerufen am 20.01.2018

[For16] Forschungsstelle Recht im DFN: *Speicherrechte nach dem Telemediengesetz und dem Telekommunikationsgesetz.* https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Speicherrechte_nach_dem_TMG_und_TKG.pdf. Version: 2016. – abgerufen am 08.10.2017

[Fra17] Frankfuter Allgemeine Zeitung: *Leitlinien für einen starken Staat in schwierigen Zeiten.* https://www.bmi.bund.de/SharedDocs/interviews/DE/2017/01/namensartikel-faz.html. Version: 2017. – abgerufen am 27.01.2017

[Fri15] Fricke, Torsten ; Epstein, Robert (Hrsg.): *Die Akte Google : wie der US-Konzern Daten missbraucht, die Welt manipuliert und Jobs vernichtet.* München : Herbig, 2015 http://d-nb.info/1062992040/04

[Fri16] Frickel, Claudia: *Cross-Device-Tracking: So schützen Sie sich.* http://www.pc-magazin.de/ratgeber/cross-device-tracking-daten-schutz-tipps-3195539.html. Version: 2016

[GH17] Greiner, Lena ; Horchert, Judith: *Der Spion im Ranzen.* http://www.spiegel.de/netzwelt/netzpolitik/schutzranzen-wolfsburg-stoppt-projekt-mit-peilsendern-an-schultaschen-a-1189624.html. Version: 2017. – abgerufen am 26.01.2018

[Gib16] Gibson Research Corporation: *Web Browser Cookies Operation.* https://www.grc.com/cookies/operation.htm. Version: 2016. – abgerufen am 19.02.2018

[Gib17] Gibbs, Samuel: *Google has been tracking Android users even with location services turned off.* https://www.theguardian.com/technology/2017/nov/22/google-track-android-users-location-services-turned-off-sim. Version: 2017. – abgerufen am 07.01.2018

[Gie17] Gierow, Hauke: *Google bekommt Standortdaten auch ohne GPS-Aktivierung*. https://www.golem.de/news/android-google-bekommt-standortdaten-auch-ohne-gps-aktivierung-1711-131269.html. Version: 2017. – abgerufen am 07.01.2018

[Gre17a] Greis, Friedhelm: *Bundesnetzagentur setzt Vorratsdatenspeicherung aus*. http://www.zeit.de/digital/datenschutz/2017-06/gerichtsurteil-vorratsdatenspeicherung-bundesnetzagentur. Version: 2017. – abgerufen am 10.07.2017

[Gre17b] Greis, Friedhelm: *Bundesnetzagentur setzt Vorratsdatenspeicherung aus*. https://www.golem.de/news/nach-gerichturteil-bundesnetzagentur-setzt-vorratsdatenspeicherung-aus-1706-128628.html. Version: 2017. – abgerufen am 10.07.2017

[Gro16] Grote, Matthias: *Android am Spionieren hindern*. https://www.heise.de/download/blog/Android-am-Spionieren-hindern-3349754. Version: 2016. – abgerufen am 14.01.2018

[GSM17] GSMK Gesellschaft für sichere Mobile Kommunikation mbH: *GSMK Cryptophone 500*. http://www.cryptophone.de/en/products/mobile/cp500/. Version: 2017. – abgerufen am 20.01.2018

[Gä12] Gäfgen, Clemens: *Jailbreak, Root und Custom-Rom legal? Google Android, Apple iOS, Windows Phone 7*. http://www.pcgameshardware.de/Panorama-Thema-233992/Specials/Jailbreak-iphone-4s-ipad-3-Root-Custom-rom-873885/3/. Version: 2012. – abgerufen am 20.01.2018

[Hei15] Hein, Andreas: *Schnelleinstieg Sicher Surfen im Web : zeigen Sie potenziellen Betrügern, wer auf Ihrem Rechner das Sagen hat ; Abzocke im Internet? Nicht mit mir!* Franzis Verlag, 2015. – ISBN 978–3–645–60397–3

[Hei17] Heitmüller, Ulrike: *Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report*. https://www.heise.de/newsticker/meldung/Predictive-Policing-Die-deutsche-Polize

i-zwischen-Cyber-CSI-und-Minority-Report-3685873.html. Version: 2017. – abgerufen am 09.02.2018

[Her17] Hern, Alex: *Three quarters of Android apps track users with third party tools – study.* https://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university. Version: 2017. – abgerufen am 07.01.2018

[Hes17] Hesseling, Claus: *Verschlüsselte Messenger: Threema, Signal, Telegram, WhatsApp.* https://mobilsicher.de/ratgeber/verschluesselt-kommunizieren-per-app. Version: 2017. – abgerufen am 07.04.2017

[Hil17] Hiller, Alexandra: *Radiofeature: Algorithmen als Schicksalsmaschinen.* https://netzpolitik.org/2017/radiofeature-algorithmen-als-schicksalsmaschinen/. Version: 2017. – abgerufen am 10.02.2018

[HM17] Heidrich, Joerg ; Maekeler, Nicolas: Alexa, darfst du das? In: *c't* (2017), Nr. 22. https://www.wiso-net.de/document/CT__1509066717928698

[Jon13] JonDos GmbH: *JonDonym.* https://www.anonym-surfen.de/. Version: 2013. – abgerufen am 16.07.2017

[Jur17] Jurran, Nico: *Smartphone-Spiele belauschen Nutzer.* https://www.heise.de/newsticker/meldung/Smartphone-Spiele-belauschen-Nutzer-3928850.html. Version: 2017. – abgerufen am 16.01.2018

[Kam10] Kamkar, Samy: *evercookie.* https://samy.pl/evercookie/. Version: 2010. – abgerufen am 22.11.2017

[Kar18] Kartheuser, Boris: *Kontrolle ist gut, Überwachung ist besser.* http://www.spiegel.de/panorama/justiz/predictive-policing-in-los-angeles-kontrolle-ist-gut-ueberwachung-ist-besser-a-1188578.html. Version: 2018. – abgerufen am 10.02.2018

[Kat16] Katzenbeisser, Stefan: Technischer Schutz vor geheimdienstlicher Überwachung. In: *Datenschutz und Datensicherheit - DuD* 40 (2016), Feb, Nr. 2, 98–100. http://dx.doi.org/10.1007/s11623-016-0554-5. – DOI 10.1007/s11623–016–0554–5. – ISSN 1862–2607

[Kau15] Kaufmann, Annelie: *Den Geheimdienstkontrolleuren reicht's.* http://www.zeit.de/politik/deutschland/2015-06/geheimdienst-kontrolle-g-10-kommission. Version: 2015. – abgerufen am 08.10.2017

[Kle17] Kleinz, Torsten: *34C3: Daten kontra Freiheit.* https://www.heise.de/newsticker/meldung/34C3-Daten-kontra-Freiheit-3928458.html. Version: 2017. – abgerufen am 27.01.2017

[Kre03] Krempl, Stefan: *Stille SMS - Überwachung per Mobilfunk.* https://www.heise.de/ct/artikel/Stille-SMS-1899173.html. Version: Mai 2003. – abgerufen am 15.01.2018

[Kre16a] Krempl, Stefan: *33C3: Tor-Angriff mit Ultraschall-Spyware und verräterische Selfies.* https://www.heise.de/newsticker/meldung/33C3-Tor-Angriff-mit-Ultraschall-Spyware-und-verraeterische-Selfies-3583185.html?hg=1&hgi=1&hgf=false. Version: 2016. – abgerufen am 11.01.2018

[Kre16b] Krempl, Stefan: *Mit verteilten Systemen gegen den digitalen Überwachungskolonialismus.* https://www.heise.de/newsticker/meldung/Mit-verteilten-Systemen-gegen-den-digitalen-Ueberwachungskolonialismus-3131896.html. Version: 2016. – abgerufen am 29.11.2017

[Kre17a] Krempl, Stefan: *Tracking: Forscher finden Ultraschall-Spyware in 234 Android-Apps.* https://www.heise.de/newsticker/meldung/Tracking-Forscher-finden-Ultraschall-Spyware-in-234-Android-Apps-3704642.html. Version: Mai 2017. – abgerufen am 13.07.2017

[Kre17b] Krempl, Stefan: *Verfassungsschutzchef will IP-Adressen von Abrufern von Enthauptungsvideos.* https://www.heise.de/newsticker/meldung/Verfassungsschutzchef-will-IP-Adressen-von-Abrufern-von-Enthauptungsvideos-3850821.html. Version: 2017. – abgerufen am 26.01.2018

[Kre17c] Krempl, Stefan: *Überwachung: Koalition macht Staatstrojaner zum polizeilichen Alltagswerkzeug.* https://www.heise.de/newsticker/meldung/Ueberwachung-Koalition-macht-Staatstrojaner-zum-polizeilichen-Alltagswerkzeug-3748014.html. Version: 2017. – abgerufen am 09.10.2017

[Kuk14] Kuketz, Mike: *IMSI-Catcher Erkennung für Android – AIMSICD.* https://www.kuketz-blog.de/imsi-catcher-erkennung-fuer-android-aimsicd/. Version: 2014. – abgerufen am 15.01.2018

[Kuk17a] Kuketz, Mike: *Android: XPrivacy ist bis maximal Android 6 nutzbar.* https://www.kuketz-blog.de/android-xprivacy-ist-bis-maximal-android-6-nutzbar/. Version: 2017. – abgerufen am 20.01.2018

[Kuk17b] Kuketz, Mike: *F-Droid und App-Alternativen – Android unter Kontrolle Teil3.* https://www.kuketz-blog.de/f-droid-und-app-alternativen-android-unter-kontrolle-teil3/. Version: 2017. – abgerufen am 10.01.2018

[Kur17a] Kurz, Constanze: *Bundesdatenschutzbeauftragte rügt Vorhaben, den Staatstrojaner-Einsatz drastisch zu erweitern.* https://netzpolitik.org/2017/bundesdatenschutzbeauftragte-ruegt-vorhaben-den-staatstrojaner-einsatz-drastisch-zu-erweitern/. Version: Mai 2017. – abgerufen am 10.07.2017

[Kur17b] Kurz, Constanze: *De Maizière plant flächendeckende Gesichtserkennung trotz hoher Fehlerquoten am Südkreuz.* https://netzpolitik.org/2017/de-maiziere-plant-flaechendeckende-gesichtserkennung-trotz-hoher-fehlerquoten-am-suedkreuz/. Version: 2017. – abgerufen am 27.01.2017

[Lob17] Lobe, Adrian: *"Honesty ShanghaiÄpp bewertet, ob ein Bürger vertrauenswürdig ist.* https://www.berliner-zeitung.de/digital/-honesty-shanghai--app-bewertet--ob-ein-buerger-vertrauenswuerdig-ist-27765300. Version: 2017. – abgerufen am 05.12.2017

[LoI] LoIacono, Luigi: Krümelspuren im Web. In: *FKT : offizielles Organ der Fernseh- und Kinotechnischen Gesellschaft ; die Fachzeitschrift für Fernsehen, Film und elektronische Medien*

[Los15] Loshin, Peter: *Anonym im Internet mit Tor und Tails : nutze die Methoden von Snowden und hinterlasse keine Spuren im Internet.* Haar bei München : Franzis, 2015 (Hacking mit Franzis). http://deposit.d-nb.de/cgi-bin/dokserv?id=5284709&prov=M&dok%5Fvar=1&dok%5Fext=htm

[Mah17] Maheshwari, Sapna: *That Game on Your Phone May Be Tracking What You're Watching on TV.* https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html. Version: 2017. – abgerufen am 16.01.2018

[Mau15] Mauerer, Thomas: *Web Privacy.* https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-09-1/NET-2015-09-1_04.pdf. Version: 2015

[MBYS11] Mowery, Keaton ; Bogenreif, Dillon ; Yilek, Scott ; Shacham, Hovav: *Fingerprinting Information in JavaScript Implementations.* http://cseweb.ucsd.edu/~hovav/dist/jspriv.pdf. Version: 2011

[Mei16] Meier, Stefan: *Datenschutz-Grundverordnung (DSGVO).* https://dsgvo-gesetz.de. Version: 2016. – abgerufen am 10.10.2017

[Mes14] Messmann, Waltraud: *Experte: Notrufsystem eCall ein trojanisches Pferd.* https://www.noz.de/deutschland-welt/gut-zu-wissen/artikel/496105/experte-notrufsystem-ecall-ein-trojanisches-pferd#gallery&0&0&496105. Version: 2014. – abgerufen am 17.10.2017

[Mez17] Mezger, Lukas: *Entwurf der EU-ePrivacy-Verordnung: (Katastrophale) Konsequenzen für die Onlinewerbung?* http://www.onlinemarketingrecht.de/2017/01/entwurf-der-eu-eprivacy-verordnung-geleakt-konsequenzen-fuer-die-onlinewerbung/. Version: 2017. – abgerufen am 10.10.2017

[MHF+16] Mavroudis, V. ; Hao, S. ; Fratantonio, Y. ; Maggi, F. ; Kruegel, C. ; Vigna, G.: *The Ultrasound Tracking Ecosystem.* http://ubeacsec.org/downloads/report.pdf. Version: 2016

[Mon18] Monroy, Matthias: *Bundesbehörden spähen immer öfter Mobiltelefone aus.* https://netzpolitik.org/2018/bundesbehoerden-spaehen-immer-oefter-mobiltelefone-aus/. Version: 2018. – abgerufen am 25.01.2018

[Moz17] Mozilla Corporation: *Privater Modus – Kontrolle über die von Firefox gespeicherten Daten behalten.* https://support.mozilla.org/de/kb/privater-modus. Version: 2017. – abgerufen am 25.12.2017

[MV16] Ministerium für Ländlichen Raum ; Verbraucherschutz Baden-Württemberg: *Smart Home – Vorteile und Risiken.* https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Smart+Home+_+Vorteile+und+Risiken. Version: 2016. – abgerufen am 18.10.2017

[Mü17a] Mühlenmeier, Lennart: *Chronik des Überwachungsstaates.* https://netzpolitik.org/2017/chronik-des-ueberwachungsstaates/. Version: 2017. – abgerufen am 31.01.2018

[Mü17b] Mühlenmeier, Lennart: *Signal für Android jetzt ohne Google Play Store.* https://netzpolitik.org//2017/signal-fuer-android-jetzt-ohne-google-play-store/. Version: 2017. – abgerufen am 17.03.2017

[NKJ+13] Nikiforakis, Nick ; Kapravelos, Alexandros ; Joosen, Wouter ; Kruegel, Christopher ; Piessens, Frank ; Vigna, Giovanni: *Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprin-*

ting. https://lirias.kuleuven.be/bitstream/123456789/393661/1/cookieless_sp2013.pdf. Version: 2013

[Ope07] Open Source Initiative: *The Open Source Definition*. https://opensource.org/docs/osd. Version: 2007. – abgerufen am 26.11.2017

[Ope16] Open Whisper Systems: *Home*. https://whispersystems.org/. Version: 2016. – abgerufen am 17.03.2017

[Pet17] Petrlic, Ronald ; Sorge, Christoph (Hrsg.): *Datenschutz Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*. Wiesbaden : Springer Vieweg, 2017 (SpringerLink : Bücher). http://dx.doi.org/10.1007/978-3-658-16839-1

[Praa] Praetor Intermedia UG: *Freiheitssphäre und Privatsphäre*. https://www.menschenrechtserklaerung.de/freiheitssphaere-und-privatsphaere-3614/. – abgerufen am 07.10.2017

[Prab] Praetor Intermedia UG: *Grundrechteschutz - Ihre Grundrechte in Deutschland und Europa*. https://www.grundrechteschutz.de. – abgerufen am 09.07.2017

[Prac] Praetor Intermedia UG: *Die Menschenrechtsabkommen der Vereinten Nationen — UN-Menschenrechtsabkommen*. https://www.menschenrechtsabkommen.de/. – abgerufen am 07.07.2017

[Pro11a] Projekt Anonymität im Internet: *JAP Anonymity & Privacy*. https://anon.inf.tu-dresden.de/. Version: 2011. – abgerufen am 16.07.2017

[Pro11b] Projekt Anonymität im Internet: *Technischer Hintergrund von JAP*. https://anon.inf.tu-dresden.de/JAPTechBgPaper.pdf. Version: 2011

[PT18] Pinkert, Reiko ; Tanriverdi, Hakan: *Polizei spioniert Handynutzer mit Trojaner aus*. http://www.sueddeutsche.de/digital/ueberwachung-polizei-spioniert-handynutzer-mit-trojaner-aus-1.3842439. Version: 2018. – abgerufen am 27.01.2018

[RD17] Reece, Andrew G. ; Danforth, Christopher M.: *Instagram photos reveal predictive markers of depression.* https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-017-0110-z. Version: 2017

[Reu16] Reuter, Markus: *Mehr Geld für Überwachung: Deutlich höhere Budgets für BND und Verfassungsschutz geplant.* https://netzpolitik.org/2016/mehr-geld-fuer-ueberwachung-deutlich-hoehere-budgets-fuer-bnd-und-verfassungsschutz-geplant/. Version: 2016. – abgerufen am 10.03.2017

[Ric17] Richter, David: *Unbemerkt: Ultraschall-Apps verfolgen Android-Nutzer geräteübergreifend.* https://netzpolitik.org/2017/unbemerkt-ultraschall-apps-verfolgen-android-nutzer-geraeteuebergreifend/. Version: 2017. – abgerufen am 17.06.2017

[Ruh17] Ruhenstroth, Miriam: *Was ist eigentlich Offline-Tracking?* https://mobilsicher.de/hintergrund/was-ist-eigentlich-offline-tracking. Version: 2017. – abgerufen am 07.01.2018

[Rö16] Rötzer, Florian: *Israelisches Unternehmen will Terroristen an Gesichtern erkennen.* https://www.heise.de/tp/features/Israelisches-Unternehmen-will-Terroristen-an-Gesichtern-erkennen-3380248.html. Version: 2016. – abgerufen am 27.01.2017

[San16] Sander, Sebastian: *Firefox: Cache Dateien deaktivieren.* http://praxistipps.chip.de/firefox-cache-dateien-deaktivieren_12332. Version: 2016. – abgerufen am 06.01.2018

[Sch13] Schmidt, Jürgen: *User-Tracking im Web: Forscher warnt vor heimtückischer Tracking-Technik.* https://www.heise.de/security/meldung/User-Tracking-im-Web-Forscher-warnt-vor-heimtueckischer-Tracking-Technik-2048507.html. Version: 2013. – abgerufen am 03.01.2018

[Sch14a] Schaar, Peter: *Überwachung total : wie wir in Zukunft unsere Daten schützen.* 1. Aufl. Berlin : Aufbau-Verl., 2014

http://deposit.d-nb.de/cgi-bin/dokserv?id=4564514&prov=M&dok%5Fvar=1&dok%5Fext=htm

[Sch14b] Schnabel, Patrick: *SSL - Secure Socket Layer*. http://www.elektronik-kompendium.de/sites/net/0902281.htm. Version: 2014. – abgerufen am 05.09.2017

[Sch16] Schonschek, Oliver: *Verlassen Sie sich nicht auf den Cookie-Manager!* https://www.datenschutz-praxis.de/fachartikel/verlassen-sie-sich-nicht-auf-den-cookie-manager/. Version: 2016. – abgerufen am 17.12.2017

[Sch17a] Schaar, Peter: *Trügerische Sicherheit*. https://media.ccc.de/v/34c3-9287-trugerische_sicherheit. Version: 2017. – abgerufen am 25.01.2018

[Sch17b] Schlosser, Jochen: *Cookie Matching*. http://www.digitalwiki.de/cookie-matching/. Version: 2017. – abgerufen am 01.02.2018

[Sch17c] Schreiber, Manuel: *Heizkörperthermostat per Handy und Sprache steuern: Diese Regler sind Smartphone-ready*. http://www.chip.de/artikel/Heizkoerperthermostat-per-Handy-und-Sprache-steuern-Diese-Regler-sind-Smartphone-ready_124599005.html. Version: 2017. – abgerufen am 18.10.2017

[Sch18] Schreiber, Manuel: *Android rooten: Vorteile und Nachteile*. http://www.chip.de/artikel/Android-rooten-Vorteile-und-Nachteile_131608081.html. Version: 2018. – abgerufen am 20.01.2018

[SEL17] SELFHTML e.V.: *Grundlagen/HTTPS und TLS*. https://wiki.selfhtml.org/wiki/Grundlagen/HTTPS_und_TLS. Version: 2017. – abgerufen am 05.09.2017

[SES14] Schneider, Markus ; Enzmann, Matthias ; Stopczynski, Martin: *Web-Tracking-Report 2014*. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf. Version: 2014

[Sis17] Sistig, Martin: *Der gläserne Fahrer*. http://www.zeit.de/wirtschaft/2017-09/datenschutz-autohersteller-apps-datenverschluesselung-stiftung-warentest. Version: 2017. – abgerufen am 17.10.2017

[Spi14] Spiegel Online: *Neue Methode zum Online-Tracking macht Verstecken fast unmöglich*. http://www.spiegel.de/netzwelt/web/canvas-fingerprinting-macht-internetnutzung-nachverfolgbar-a-982280.html. Version: 2014. – abgerufen am 11.11.2016

[Spi17a] Spiegel Online: *Foto-Software erkennt Depressive auf Instagram*. http://www.spiegel.de/gesundheit/psychologie/depressionen-software-scannt-instagram-fotos-a-1161845.html. Version: 2017. – abgerufen am 06.09.2017

[Spi17b] Spier, Alexander: *So bekommen Sie mehr Privatsphäre bei Android*. http://www.spiegel.de/netzwelt/web/android-und-die-sicherheit-tipps-zu-datenschutz-einstellungen-a-1138251.html. Version: 2017. – abgerufen am 14.01.2018

[Spr] Springer Gabler — Springer Fachmedien Wiesbaden GmbH: *Definition Backdoor*. http://wirtschaftslexikon.gabler.de/Definition/backdoor.html. – abgerufen am 09.07.2017

[Sta17] Statista GmbH: *Marktanteile der meistgenutzten Suchmaschinen weltweit bis September 2017*. https://de.statista.com/statistik/daten/studie/225953/umfrage/die-weltweit-meistgenutzten-suchmaschinen/. Version: 2017. – abgerufen am 29.10.2017

[Ste17] Stern, Jenny: *WannaCry - Angriffstool aus dem Waffenschrank der NSA*. http://faktenfinder.tagesschau.de/wanna-cry-cyberangriff-101.html. Version: Mai 2017. – abgerufen am 13.07.2017

[Sti14] Stiftung Warentest: *WhatsApp und Alternativen: Datenschutz im Test*. https://www.test.de/WhatsApp-und-Alternativen-Datenschutz-im-Test-4675013-0/?mc=kurzurl.messenger. Version: 2014. – abgerufen am 18.03.2017

[Str11] Streib, Simon: *Big Brotherhood is watching you : unseren Daten auf der Spur*. Berlin : BibSpider, 2011 (Excellence in teaching and learning). http://d-nb.info/1009947710/04

[Str16] Strathmann, Marvin: *Zwei diskrete Suchmaschinen wachsen zusammen*. http://www.zeit.de/digital/internet/2016-03/startpage-ixquick-google-datenschutz. Version: 2016. – abgerufen am 28.09.2017

[SUMa] SUMA-EV - Verein für freien Wissenszugang (e.V.): *MetaGer - FAQ*. https://metager.de/faq. – abgerufen am 24.11.2017

[SUMb] SUMA-EV - Verein für freien Wissenszugang (e.V.): *MetaGer - Über Uns*. https://metager.de/about. – abgerufen am 24.11.2017

[SUM14] SUMA-EV - Verein für freien Wissenszugang (e.V.): *MetaGer - Datenschutz und Privatsphäre*. https://metager.de/datenschutz. Version: 2014. – abgerufen am 24.11.2017

[SUM17a] SUMA-EV - Verein für freien Wissenszugang (e.V.): *Newsletter 13.03.2017: Die aktuellen Entwicklungen in und um MetaGer*. https://blog.suma-ev.de/node/223. Version: 2017. – abgerufen am 26.11.2017

[SUM17b] SUMA-EV - Verein für freien Wissenszugang (e.V.): *"Wieso du nur mit Google suchst Interview von www.krautreporter.de*. https://blog.suma-ev.de/node/229. Version: 2017. – abgerufen am 24.11.2017

[Sur13] Surfboard Holding B.V.: *StartPage und Ixquick: Neueste Verschlüsselungsstandards gegen Massenüberwachung Erstmals Kombination von TLS 1.1/1.2 und "Perfect Forward Secrecy" im Einsatz*. https://classic.startpage.com/deu/press/pr-pfs.html#hmb. Version: 2013. – abgerufen am 05.10.2017

[Sur17a] Surfboard Holding B.V.: *Erklärung für StartPage Proxy*. https://www.startpage.com/proxy/deu/help.html#hmb. Version: 2017. – abgerufen am 28.09.2017

[Sur17b] Surfboard Holding B.V.: *StartPage schützt Ihre Privatsphäre!* https://classic.startpage.com/deu/protect-privacy.html#hmb. Version: 2017. – abgerufen am 28.09.2017

[Sur17c] Surfboard Holding B.V.: *Der URL-generator*. https://classic.startpage.com/deu/urlgenerator-details.html#hmb. Version: 2017. – abgerufen am 05.10.2017

[Tan17] Tanriverdi, Hakan: *Das plant Deutschlands oberster Codeknacker*. http://www.sueddeutsche.de/digital/zitis-das-plant-deutschlands-oberster-codeknacker-1.3663540. Version: 2017. – abgerufen am 28.01.2017

[Tel17] Telegram Messenger LLP: *Home*. https://telegram.org/. Version: 2017. – abgerufen am 18.03.2017

[Tho14] Thoma, Jörg: *Verschlüsselung nicht für jedermann*. https://www.golem.de/news/cryptophone-verschluesselung-nicht-fuer-jedermann-1409-109371.html. Version: 2014. – abgerufen am 20.01.2018

[Thr17] Threema GmbH: *Threema Home*. https://threema.ch/de. Version: 2017. – abgerufen am 24.03.2017

[Tor03] Tor Project: *Tor Benutzer-Anleitung*. https://archive.torproject.org/tor-package-archive/manual/short-user-manual_de.xhtml. Version: 2003. – abgerufen am 21.10.2016

[Tor17] Tor Project: *Tor Home*. https://www.torproject.org. Version: 2017. – abgerufen am 21.10.2016

[ubu17] ubuntu Deutschland e. V.: *Privoxy*. https://wiki.ubuntuusers.de/Privoxy/. Version: 2017. – abgerufen am 18.12.2017

[Ver16] Vertical Media GmbH: *Ist Telegram wirklich ein Berliner Start-up?* http://www.gruenderszene.de/allgemein/telegram-berlin-oder-nicht. Version: 2016. – abgerufen am 24.03.2017

[Ver17] Verbraucherzentrale Bundesverband e.V.: *Hintergrundpapier des VZBV zum Thema Smart Home*. https://www.vzbv.de/sites/default/files/downloads/2017/

09/05/170905_hintergrundpapier_smart_home.pdf. Version: 2017. – abgerufen am 26.01.2018

[W3S17] W3Schools: *HTML5 Web Storage*. https://www.w3schools.com/html/html5_webstorage.asp. Version: 2017. – abgerufen am 20.11.2017

[WE14] Wischnjak, David ; Eikenberg, Ronald: Auf Schritt und Tritt. In: *c't* (2014), Nr. 21. https://www.wiso-net.de/document/CT__1411932798574172

[Wei15] Weis, Rüdiger: *Kryptographie, Open Source und Gesellschaft*. https://netzpolitik.org/2015/kryptographie-open-source-und-gesellschaft/. Version: 2015. – abgerufen am 26.11.2017

[Wei16a] Weisensee, Jan: *Amnesty klagt gegen G10-Gesetz*. https://www.golem.de/news/bundesverfassungsgericht-amnesty-klagt-gegen-g10-gesetz-1611-124478.html. Version: 2016. – abgerufen am 10.07.2017

[Wei16b] Weisensee, Jan: *Goodbye Google? Suchmaschinen selber hosten*. https://www.golem.de/news/howto-goodbye-google-suchmaschinen-selber-hosten-1610-123482-6.html. Version: 2016. – abgerufen am 29.11.2017

[Wei17] Weisensee, Jan: *Ultraschall-Tracking kann Tor-Nutzer deanonymisieren*. https://www.golem.de/news/anonymitaet-ultraschall-tracking-kann-tor-nutzer-deanonymisieren-1701-125434.html. Version: 2017. – abgerufen am 17.06.2017

[Wol17] Wolfangel, Eva: *Ein Königreich für deine Konsumwünsche*. http://www.zeit.de/digital/datenschutz/2017-04/konsum-zukunft-tracking-google-beacons-einzelhandel/seite-2. Version: Mai 2017. – abgerufen am 08.01.2018

[WS17] Winter-Shangama, Kristin: Web Real-Time Communication: Chancen, Risiken und Schutzbedarf. In: *Datenschutz-Berater* (2017), Nr. 01. https://www.wiso-net.de/document/DSB__DSBDSB1226400

[Zeh13] Zeh, Juli: *Deutschland ist ein Überwachungsstaat.* http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/offener-brief-an-angela-merkel-deutschland-ist-ein-ueberwachungsstaat-12304732.html. Version: 2013. – abgerufen am 24.01.2018

[ZEI15] ZEIT ONLINE: *Senat beschließt Reform der NSA-Spähgesetze.* http://www.zeit.de/politik/ausland/2015-06/nsa-patriot-act-reform-senat. Version: 2015. – abgerufen am 10.10.2017

Abbildungsverzeichnis

Tabellenverzeichnis