ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/283504593

White Paper Selbstdatenschutz

Book · November 2014

CITATIONS
0

READS
268

8 authors, including:

Murat Karaboga
Fraunhofer Institute for Systems and Innovat…
10 PUBLICATIONS **1** CITATION
SEE PROFILE

Philipp K. Masur
Hohenheim University
15 PUBLICATIONS **69** CITATIONS
SEE PROFILE

Cornelia Mothes
Technische Universität Dresden
20 PUBLICATIONS **42** CITATIONS
SEE PROFILE

Philip Schütz
dm-drogerie markt
11 PUBLICATIONS **18** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt View project

Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt View project

All content following this page was uploaded by Philip Schütz on 05 November 2015.

The user has requested enhancement of the downloaded file.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

SELBSTDATENSCHUTZ

White Paper

SELBSTDATENSCHUTZ

Redaktion:
Philip Schütz[1], Murat Karaboga[1], Michael Friedewald[1], Peter Zoche[1]

Autoren:
Murat Karaboga[1], Philipp Masur[3], Tobias Matzner[2], Cornelia Mothes[3], Maxi Nebel[4], Carsten Ochs[5], Philip Schütz[1], Hervais Simo Fhom[6]

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Tübingen, Internationalen Zentrum für Ethik in den Wissenschaften (IZEW)
(3) Universität Hohenheim, Lehrstuhl für Medienpsychologie, Stuttgart
(4) Universität Kassel, Institut für Wirtschaftsrecht
(5) Universität Kassel, Fachgebiet Soziologische Theorie
(6) Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

Herausgeber:
Peter Zoche, Regina Ammicht-Quinn, Jörn Lamla, Alexander Roßnagel, Sabine Trepte, Michael Waidner

Inhalt

1 Warum Selbstdatenschutz? ... 3
1.1 Gefahren durch Unternehmen – Der gläserne Konsument ... 3
1.2 Gefahren durch Sicherheitsbehörden – Der Bürger unter Verdacht ... 3
1.3 Das weltweite Netz macht es möglich ... 4
1.4 Selbstdatenschutztechniken als Schutzpraktiken ... 4

2 Rechtlicher Rahmen des Selbstdatenschutzes ... 5
2.1 Das Grundrecht auf informationelle Selbstbestimmung ... 5
2.2 Maßnahmen zum Selbstdatenschutz ... 5
2.3 Rechtliche Grenzen des Selbstdatenschutzes ... 6

3 Wer hat ein Interesse an Selbstdatenschutz und warum? ... 8
3.1 Libertäre Technikoptimisten (Cypherpunks) ... 8
3.2 Selbstorganisierte Initiativen & Aktivisten ... 8
3.3 Institutionalisierter Datenschutz ... 9
3.4 Politik: Regierung und parlamentarisch vertretene Parteien ... 10
3.5 Wirtschaftliche Interessenverbände ... 11

4 Was denken und was tun Internetnutzer? ... 13
4.1 Sorgen um Privatheitsverletzungen und Maßnahmen des Selbstdatenschutzes ... 13
4.2 Erklärungen für Einstellungs-Verhaltens-Diskrepanzen ... 14

5 Technische Grundlagen ... 17
5.1 Abstraktes Systemmodell ... 17
5.2 Angriffe auf (mobile) Endgeräte der Nutzer ... 18
5.3 Angriffe auf Kommunikationsnetze ... 18
5.4 Angriffsmöglichkeiten auf Server der Diensteanbieter ... 19

6 Technischer Selbstdatenschutz ... 20
6.1 Sicherheitslösungen für (mobile) Endgeräte der Nutzer ... 20
6.1.1 Maßnahmen zum Schutz sensibler Daten in Smartphone und PC ... 20
6.1.2 Anti-Tracking-Maßnahmen ... 21
6.2 Lösungen für sichere und anonyme Kommunikation ... 21
6.2.1 Beispiel – E-Mail-Verschlüsselung mit OpenPGP und S/MIME ... 21
6.2.2 Beispiel – Sicheres Instant Messaging ... 24
6.3 Anonymisierungstools und –dienste ... 25
6.3.1 Beispiel – Freies Anoymisierungsnetzwerk „Tor" ... 26
6.3.2 Beispiel – Kommerzieller Anonymisierungsdienstleister „JonDonym" ... 27

7 Fazit ... 29

Anhang **... 30**
Informationsquellen ... 30
Anleitungen zur Einrichtung von E-Mail-Verschlüsselung ... 30

1
Warum Selbstdatenschutz?

Die NSA-Affäre macht deutlich, wie leicht personenbezogene Daten in den Zugriffsbereich ausländischer Behörden und Geheimdienste fallen. Da die heutige Datenverarbeitung nicht mehr an einem bestimmten Ort, sondern global erfolgt, verarbeiten und speichern Internetfirmen und Diensteanbieter personenbezogene Daten regelmäßig nicht nur dort, wo die Daten erhoben wurden, sondern weltweit, sei es im Land der Niederlassung des Unternehmens, auf Servern in Drittländern oder fragmentiert in der Cloud. Aufgrund seiner territorialen Begrenzung und eines massiv ausgeprägten rechtspolitischen Vollzugsdefizit findet auf viele Sachverhalte deutsches Datenschutzrecht in der Praxis häufig keine Anwendung. Aus diesem Grund werden - jenseits der Verantwortlichkeit von Politik und Wirtschaft, den Bürger[1] vor unrechtmäßiger Überwachung zu schützen - immer mehr Stimmen nach einem effektiven Selbstdatenschutz laut, der das Individuum über Landesgrenzen hinweg in die Lage versetzen soll, sich selbst zu schützen.

1.1
Gefahren durch Unternehmen – Der gläserne Konsument

Daten stellen schon heute zentralen „Rohstoff" und wichtigste Geschäftsgrundlage vieler IKT (Informations- und Kommunikationstechnologie) Anwendungen dar. Obwohl sich Unternehmen, bedingt durch ihre Geschäftsmodelle, im Grad der Abhängigkeit von personenbezogenen Daten unterscheiden, eint sie doch alle das Interesse, entweder ihre Produkte und Services mit Hilfe von Werbung und maßgeschneiderten Angeboten erfolgreich zu verkaufen oder einen noch größeren Profit durch den Weiterverkauf von Daten bzw. Analysen zu generieren. Insbesondere durch das Internet ist hier ein hinter den digitalen Kulissen agierender Wirtschaftssektor entstanden, der sich aus personenbezogenen Daten speist und den zu bewerbenden Kunden bzw. dessen Daten zum gehandelten Produkt hat werden lassen. Oftmals durch Werbung oder den Datenhandel finanziert, können solche Unternehmen ihre digitalen Angebote für jeden nutzbar, kostenlos und obendrein noch stark auf den Kunden zugeschnitten auf den Markt bringen. Dieses Geschäftsmodell hat zu einem Paradigmenwechsel im IKT-Sektor hin zu einer *data-driven economy* geführt, so dass heute auch traditionelle Unternehmen, die für ihre Services und Produkte vom Kunden bezahlt werden, verstärkt auf das Sammeln personenbezogener Daten setzen. Dies bedeutet auch im Hinblick auf eine zunehmende Verschmelzung von virtuellem und physischem Raum, dass Überwachung nicht auf das Internet – obwohl hier besonders stark ausgeprägt – beschränkt ist. Insbesondere das Internet der Dinge, also die Internetanbindung von häufig mit Sensoren ausgestatteten Alltagsgegenständen wie dem Telefon, TV-Gerät oder Auto, schafft hier neue Möglichkeiten der Überwachung.

1.2
Gefahren durch Sicherheitsbehörden – Der Bürger unter Verdacht

Daten bedeuten Informationen, Wissen, Kontrolle und Macht. Aus diesem Grund sind nicht nur Unternehmen, sondern auch staatliche Institutionen – hier insbesondere Sicherheitsbehörden und Geheimdienste – an personenbezogenen Daten interessiert. Dies bedarf rechtlicher Grundlagen, obwohl die NSA-Spähaffäre gezeigt hat, dass ein rechtliches Vakuum bzgl. des Agierens ausländischer Geheimdienste auf deutschem Territorium bzw. im Internet besteht. Zum einen verabschiedet die Politik selbst Gesetze

zur Überwachung der Bürger wie dies bei der vor Kurzem durch den EuGH als rechtswidrig eingestuften Vorratsdatenspeicherung der Fall war, zum anderen greifen Sicherheitsbehörden regelmäßig gemäß Strafprozessordnung, der Telekommunikationsüberwachungsverordnung (TKÜV) oder dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G-10-Gesetz) auf die massenhaft gesammelten und verarbeiteten Daten privatwirtschaftlicher Akteure zurück.

1.3 Das weltweite Netz macht es möglich

In seiner technischen Ausgestaltung hat das Internet bedingt durch entwicklungsgeschichtlich verankerte Strukturen, Standards und Regeln bis heute stark auf das Paradigma der Offenheit gesetzt. Im Web 2.0 kam dann vor allem das Ziel der einfachen Bedienbarkeit von Anwendungen hinzu. Datensicherheit und Datenschutz für die Nutzer hingegen wurden bis heute strukturell vernachlässigt. Diese Entwicklung setzt sich nun auch massiv im Mobile Computing und im Internet der Dinge fort, wodurch technische Möglichkeiten des Ausspähens von Personen allgegenwärtig sind. Obwohl heutzutage die uns am einflussreichsten erscheinende digitale Welt das Internet ist, gibt es unzählige andere Netze und mittlerweile auf digitaler Verarbeitung basierende, vernetzte Technologien, die Überwachung ermöglichen – sei es die Kredit- oder Bonuskarte beim Einkaufen oder eine Überwachungskamera am Bahnhof. Allerdings haben sich Selbstdatenschutzpraktiken vor allem im Hinblick auf die Nutzung des Internets herausgebildet.

1.4 Selbstdatenschutztechniken als Schutzpraktiken

Selbstdatenschutztechniken lassen sich als technische Schutzpraktiken begreifen. *Praktiken* stellen in diesem Zusammenhang verfestigte Routinen dar, die sowohl von menschlichen (Nutzer) als auch technischen Komponenten (Softwaretools) kollektiv gebildet werden und eng mit soziokulturellen Verhaltensregeln, Wahrnehmungsweisen, Kompetenzen usw. verwoben sind.[2] *Selbstdatenschutz* lässt sich indes als die Gesamtheit der „durch den Einzelnen zum Schutz seiner Datenschutzgrundrechte ergriffenen technischen, organisatorischen und rechtlichen Maßnahmen" definieren.[3] Des Weiteren sind *passive* und *aktive* Maßnahmen zu unterscheiden: Bei passiven Maßnahmen handelt es sich vor allem um die Vermeidung der Herausgabe zutreffender personenbezogener Daten (Datensparsamkeit). Aktive Maßnahmen betreffen die Angabe von Pseudonymen, die Nutzung von datenschutzfreundlicher Technik - sogenannter *Privacy Enhancing Technologies* (Verschlüsselung, Anonymisierung, Pseudonymisierung) - sowie organisatorische und rechtlich geregelte Maßnahmen. Letztere werden jedoch häufig erst *ex post* – also im Schadensfall ergriffen. Aktiver Selbstdatenschutz hat aktuell – insbesondere vor dem Hintergrund der NSA-Affäre – wieder einige Aufmerksamkeit erfahren[4] und gilt als eine spezifische Option zum Schutz informationeller Privatheit.[5] Wir werden diese Option im Folgenden interdisziplinär aus soziologischer, medienpsychologischer, rechtlicher und informatischer Perspektive beleuchten. Unser übergeordnetes Ziel besteht schließlich darin, Möglichkeiten und Probleme zu benennen, die sich mit der Option des Selbstdatenschutzes verbinden.

2
Rechtlicher Rahmen des Selbstdatenschutzes

Im ersten Schritt wird zunächst der rechtliche Rahmen informationeller Selbstbestimmung skizziert und anschließend werden Maßnahmen und Grenzen des Selbstdatenschutzes diskutiert.

2.1
Das Grundrecht auf informationelle Selbstbestimmung

In Deutschland gilt für jedermann das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht bereits 1983 im Volkszählungsurteil als Grundrecht formuliert hat.[6] Das Recht auf informationelle Selbstbestimmung gewährleistet jedem Einzelnen die Befugnis, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[7] Dies schützt einerseits die individuellen Entfaltungsmöglichkeiten des Einzelnen, der je nach Kontext und Situation entscheiden und kontrollieren können muss, welche Daten über ihn jeweils preisgegeben werden, da er sonst „in seiner Entscheidung wesentlich gehemmt werden kann, aus eigener Selbstbestimmung zu planen und zu entscheiden."[8] Andererseits betrifft die informationelle Selbstbestimmung auch das Gemeinwohl, „weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[9]
Das Recht auf informationelle Selbstbestimmung verleiht dem Einzelnen nicht nur ein Abwehrrecht gegen staatliche Eingriffe; vielmehr obliegt dem Staat die Pflicht, sich schützend und fördernd vor die Grundrechte jedes Einzelnen zu stellen und vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren.[10] Möglichkeiten zur Schutzpflichterfüllung umfassen eine Evaluierung und Bereitstellung der notwendigen Infrastruktur von Selbstdatenschutztechniken, ggf. durch regulatorische Maßnahmen, aber auch Informationskampagnen mit dem Ziel Bürger in Fragen des Datenschutzes zu sensibilisieren bzw. das Wissen um Selbstdatenschutztechniken zu verbessern. Sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof haben anlässlich der Richtlinie zur Vorratsdatenspeicherung Grundsätze zu Grenzen der anlasslosen Überwachung formuliert.[11] Daher obliegt den staatlichen Organen die Pflicht, innerhalb dieser Grenzen die informationelle Selbstbestimmung der Bürger sicherzustellen. Wo die Ressourcen des Staates nicht ausreichen, die informationelle Selbstbestimmung zu gewährleisten, besteht ein rechtmäßiges Interesse des Bürgers, seine Privatheit durch den Einsatz geeigneter technischer Werkzeuge selbst zu schützen.[12]

2.2
Maßnahmen zum Selbstdatenschutz

Selbstdatenschutztechniken wirken grenzübergreifend und unabhängig von anwendbarem Datenschutzrecht. Selbstdatenschutz wird insbesondere dort wichtig, wo zu befürchten steht, dass Datenschutzrecht gebrochen oder ausländischen Gesetzen unterworfen wird. Um Selbstdatenschutz zu fördern und die informationelle Selbstbestimmung zu gewährleisten, müssten datenverarbeitende Technologien eigentlich generell grundlegende Prinzipien wie das der Erforderlichkeit, Transparenz, Zweckbindung und Anonymisierung erfüllen.[13]
Das Prinzip der Erforderlichkeit bestimmt, dass personenbezogene Daten nur verwendet werden dürfen, wenn diese zur Erreichung des zulässigen Zwecks unverzichtbar sind.[14] Um die Erforderlichkeit personenbezogener Daten für eine konkrete Datenverarbeitung zu beurteilen, muss der Betroffene in der Lage sein, die Datenerhebung zu erkennen und zu beeinflussen.[15] Wichtige Grundlage ist deshalb eine transparente

Datenverarbeitung. Hierfür sind Anwendungen in Web-Browsern denkbar, die die Präferenzen des Nutzers berücksichtigen, über Datensammlung informieren und ungewollte Datenübermittlung verhindern.[16] Zur Unterstützung der Zweckbindung - also der Begrenzung der Datenerhebung und –verwendung auf einen bestimmten Zweck - sollte jeder Einzelne für jeden Zweck ein anderes Pseudonym verwenden, um eine Zweckentfremdung der preisgegebenen Daten zu erschweren.[17]
Die effektivste Möglichkeit zum Schutz der informationellen Selbstbestimmung ist, durch Anonymisierung erst gar keine personenbezogenen Daten entstehen zu lassen oder nachträglich zu entfernen. Anonymisierte Daten sind so verändert, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßigem Aufwand[18] an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Anwendungsfelder für Anonymisierung ergeben sich dort, wo es auf die Identität des Einzelnen nicht ankommt, z.B. bei der Suche nach und dem Austausch von Informationen.[19] Auch bei vertraulicher Kommunikation kann Anonymität entscheidend sein, nicht zwischen Gesprächspartnern, aber gegenüber Dritten wie bspw. Anbietern. Anonymisierungstechnologien wie etwa Tor oder JonDonym (siehe Fallbeispiel Anonymisierungsdienste) verschleiern die Identität des Nutzers durch Verwendung fremder IP-Adressen und den verschlüsselten Verbindungsaufbau der Kommunikation über mehrere Zwischenstationen.[20] Zwar verpflichten gesetzliche Vorschriften zur Anonymisierung von personenbezogenen Daten,[21] diese Pflicht steht aber unter dem Vorbehalt der tatsächlichen und rechtlichen Möglichkeiten und Zumutbarkeit für die verantwortliche Stelle. Da bei einem Verstoß keine negativen Konsequenzen drohen, ist es besonders wichtig, mit eigens eingesetzten Techniken Daten zu anonymisieren.

2.3 Rechtliche Grenzen des Selbstdatenschutzes

Die informationelle Selbstbestimmung sowie das Fernmeldegeheimnis ermöglichen dem Einzelnen, seine Kommunikation durch Maßnahmen des Selbstdatenschutzes zu schützen. Beide haben dort ihre Grenzen, wo ein überwiegendes Allgemeininteresse an der Aufdeckung der wahren Identität des Einzelnen die informationelle Selbstbestimmung oder das Fernmeldegeheimnis überwiegt. Daher ist Selbstdatenschutz einschränkbar durch Gesetz, wenn es im überwiegenden Allgemeininteresse liegt und der Eingriff im Hinblick auf das Regelungsziel geeignet, erforderlich und angemessen ist.[22] Rückwirkende Aufdeckung der Identität eines Nutzers kann z.B. notwendig sein, um Straftaten zu verfolgen und aufzuklären. Sowohl im nationalen Recht als auch im Recht anderer Staaten bestehen Gesetze, die Anbieter verpflichten, Angaben zur Identität sowie zu den Kommunikationsvorgängen zu erheben und zu speichern, um diese im Einzelfall Behörden zugänglich zu machen. Sowohl in Deutschland als auch in den USA, wo die meisten der Diensteanbieter ihren Sitz haben, existieren Regelungen, die Behörden und Geheimdiensten unter bestimmten Voraussetzungen den Zugriff auf personenbezogene Daten ermöglichen. Die Enthüllungen Edward Snowdens im Rahmen der NSA-Spähaffäre haben jedoch gezeigt, dass die rechtlichen Anforderungen sowie deren praktische Umsetzung zum Sammeln und Auswerten von Daten weit über das hinausgehen, was nach deutschem und europäischem Recht als zulässig erachtet wird.
In Deutschland bestehen für Anbieter von Telekommunikationsdiensten[23] Auskunftspflichten gegenüber Sicherheitsbehörden;[24] hierfür zu erhebende Daten sind u.a. die Anschlusskennung, Name und Anschrift des Anschlussinhabers. Jedoch besteht keine Pflicht zur Überprüfung der Identität.[25] Diensteanbieter mit mehr als 10.000 Nutzern sind darüber hinaus verpflichtet, Verbindungsdaten wie Angaben zur Kennung des Nutzers, gewählte Rufnummern oder andere Adressierungsangaben (z.B. Nutzernamen), Zeit, Beginn und Ende des Kommunikationsvorgangs, oder Angaben zum Standort des Endgeräts bereitzuhalten.[26] Das Telekommunikationsgesetz verpflichtet jedoch

nur den Diensteanbieter; für den Nutzer entsteht keine Pflicht, auf die Nutzung von Anonymisierungs- und Verschlüsselungstechniken zu verzichten, um die Erhebung personenbezogener Daten zu ermöglichen. Sowohl Bundesnachrichtendienst als auch das Bundesamt für Verfassungsschutz haben Auskunftsrechte hinsichtlich bestimmter Daten gegenüber Telekommunikations- und Telemediendiensteanbietern.[27]
Durch den USA PATRIOT Act[28] erhalten auch US-amerikanische Behörden und Geheimdienste Zugriff auf personenbezogene Daten bzw. Kommunikationsinhalte von EU-Bürgern. Dies kann auf zwei Art und Weisen geschehen: Zum einen findet der USA PATRIOT Act auf alle Unternehmen mit Sitz oder Niederlassung in den USA – also auch auf Filialen deutscher Unternehmen – Anwendung. Zum anderen müssen alle US-amerikanischen Unternehmen, auch solche, die sich nicht auf US-amerikanischem Territorium befinden, dem FBI, der CIA und NSA Zugang zu all ihren Servern gewährleisten.[29] Ähnlich wie im deutschen Recht darf die anfragende Behörde zudem das angefragte Unternehmen verpflichten, Stillschweigen über die Weitergabe der Daten zu bewahren.[30] Des Weiteren gelten in den USA eine Reihe von speziellen Telekommunikationsüberwachungsgesetzen, z.B. der Communications Assistance for Law Enforcement Act (CALEA), der Betreiber und Ausrüster von Telekommunikationsnetzen verpflichtet, Schnittstellen zu Überwachungszwecken bereitzustellen oder in ihre Produkte zu integrieren.[31]
Jenseits dessen können Maßnahmen des Selbstdatenschutzes auch mit urheberrechtlichen Vorschriften in Konflikt geraten, wenn die eingesetzte Software oder das Betriebssystem verändert werden soll, um das Übermitteln personenbezogener Daten zu verhindern.[32]

Kernpunkte

- Das Recht auf informationelle Selbstbestimmung eröffnet jedem Einzelnen die Möglichkeit, sich mittels Maßnahmen des Selbstdatenschutzes gegen Eingriffe in seine Privatsphäre durch staatliche, wirtschaftliche oder private Akteure zu schützen.
- Zudem verpflichtet das Recht auf informationelle Selbstbestimmung den Staat, mittels geeigneter Maßnahmen die Wahrnehmung des Selbstdatenschutzes zu ermöglichen.
- Privatheitsschutz gilt nicht absolut, sondern ist durch Rechte und berechtigte Interessen anderer oder der Allgemeinheit begrenzt, weshalb Diensteanbieter unter bestimmten Voraussetzungen zur Aufzeichnung von Kommunikationsdaten gesetzlich verpflichtet sind.
- Solche Vorschriften hindern den Einzelnen jedoch nicht, selbst Maßnahmen zum Selbstdatenschutz zu ergreifen.

3
Wer hat ein Interesse an Selbstdatenschutz und warum?

Im Folgenden erfolgt eine knappe Analyse des Diskurses um Selbstdatenschutz, wie er sich bei fünf Gruppen beobachten lässt: Bei den sog. Cypherpunks, selbstorganisierten Initiativen und Aktivisten, institutionalisierten Datenschutzorganisationen, in der Politik sowie bei wirtschaftlichen Interessenverbänden.[33]

3.1
Libertäre Technikoptimisten (Cypherpunks)

Populäre Auseinandersetzungen mit dem Thema Selbstdatenschutz beziehen sich oftmals auf die sogenannten „Cypherpunks" der 1990er Jahre als „Urheber" des aktiven Selbstdatenschutzes. Während dessen Herkunft nicht eindeutig zu bestimmen ist,[34] wählen auch wir hier das „Cypherpunk Manifesto" als Einstiegspunkt, da dieses Anfang der 1990er Jahre im Kontext der sich ausbreitenden Internetnutzung formuliert wurde, und weil die Cypherpunks im Rahmen der internationalen „Kryptokontroverse" eine gewisse Bekanntheit erlangten.[35] Im Cypherpunk-Umfeld erfreuen sich Ideen wie Libertarismus und Anarchismus in unterschiedlichen Spielarten großer Beliebtheit.[36] Grundlegende Positionen finden sich in einem Manifest, das der Mathematiker Erich Hughes 1993 verfasste.[37] Explizit drückt sich darin eine ausgeprägte Skepsis in Bezug auf große staatliche und wirtschaftliche Organisationen aus, denen gegenüber eine Schutzhaltung eingenommen werden müsse. „Elektronische Technologien", wie Verschlüsselungstools, Anonymisierungsdienste, digitale Signaturen und elektronische Geldwährungen seien geeignet einen starken Privatheitsschutz zu gewährleisten. Die Nutzung dieser Techniken wird dabei als Voraussetzung einer libertaristischen Ordnung interpretiert. Im Cypherpunk-Diskurs findet sich somit ein ausgeprägter Individualismus und ein Verständnis von Privatheit als intrinsischem, zentralem Wert. Dies ist nicht zuletzt dem libertaristischen Weltbild geschuldet, welches seinerseits auf dem Konzept des „Selbsteigentums" gründet. Sofern es sich bei sehr vielen Cypherpunks um technische Experten handelt, weisen sie ein überdurchschnittliches Maß an technischer (mathematischer, informatischer) Kompetenz und Expertise auf. In diesem Sinne stellen sie gewissermaßen die „perfekten Selbstdatenschützer" dar: Die Wertschätzung von Privatheit ist tief in ihrem Weltbild verankert und sie verfügen über die entsprechenden Mittel, diese auch zu schützen. Allerdings hingen die Cypherpunks der Illusion an, Selbstdatenschutzkompetenzen würden sich „von selbst verbreiten."[38] Dies scheint jedoch kaum der Fall zu sein,[39] so dass der radikale Individualismus sowie die ablehnende Haltung der Cypherpunks gegenüber größeren Kollektiven (Staat, Wirtschaft) von vornherein einen nachhaltigen Beitrag zur kollektiven Aufgabe der Erzeugung von Selbstdatenschutzpraktiken verhindern.

3.2
Selbstorganisierte Initiativen & Aktivisten

Im bundesdeutschen Diskurs finden sich unter den Verfechtern des Selbstdatenschutzes auch zahlreiche selbstorganisierte Initiativen[40] und Aktivisten.[41] Bezugspunkt dieser Akteure bilden zumeist die Auseinandersetzungen um die Volkszählung der 1980er Jahre. Wiederholt finden sich Verweise auf das Urteil des Bundesverfassungsgerichtes von 1983 und das in diesem Zuge formulierte Recht auf informationelle Selbstbestimmung.[42] Herkunftsmäßig entstammen einige der Protagonisten dem linken, zuweilen staatskritischen Milieu, und es findet sich eine ausdrückliche Bezugnahme auf die Demokratie als Form der politischen Praxis.[43] Gleichzeitig sieht man sich mitunter der Ha-

cker-Ethik verpflichtet, wobei eines der Leitmotive dieses normativen Rahmens lautet: „Mißtraue Autoritäten – fördere Dezentralisierung."[44] Der politische Impetus der selbstorganisierten Akteure und Initiativen fußt auf einem normativen Aufklärungsgebot, welches seinerseits auf eine Entschleierung der eigentlichen Interessen und Überwachungspraktiken staatlicher und wirtschaftlicher Organisationen abzielt. Der wiederholte Bezug auf Bürgerrechte[45] zeigt indes nicht nur die ambivalent-distanzierte Haltung zum Staat an, sondern verdeutlicht auch das Akteursverständnis, das der Positionierung zugrundeliegt: Soziale Akteure werden hier als aufgeklärte oder aufzuklärende, engagierte Bürger der Zivilgesellschaft verstanden – und eben dies erfordere Eigeninitiative.[46] Den Kern des Privatheitsverständnisses bildet folgerichtig der Grad an „Kontrolle über die eigenen Daten im Internet",[47] den Bürger noch ausüben können. Während dies zwar als generell rechtlich garantiert angesehen wird, herrscht mitunter Zweifel vor, ob darauf noch als Ressource zurückgegriffen werden könne.[48] Dies führt zum Fazit: „Alles muss mensch selber machen. Selbstdatenschutz und digitale Selbstverteidigung ist nötig!"[49]

Vor diesem Hintergrund propagieren die Initiativen und Aktivisten, die sich selbst zumeist – zumindest implizit – als technikaffin beschreiben, zahlreiche Techniken und Technologien, die der Entwicklung von Selbstdatenschutzpraktiken dienen sollen. Genau wie den Cypherpunks gilt den selbstorganisierten Akteuren und Initiativen also die informationelle Privatheit als zentraler Wert, und genau wie diese verfügen sie über das erforderliche technische Know-how. Zudem weisen sie eine zwar skeptische, aber nicht völlig ablehnende Haltung gegenüber staatlichen/wirtschaftlichen Organisationen auf.[50] Um zur Bildung von Selbstdatenschutzpraktiken auf breiter Ebene beizutragen, fehlen ihnen jedoch die Mittel – sie verfügen nicht über die institutionelle Macht, um die Bedingungen zur Ausbildung solcher Praktiken herzustellen.

3.3 Institutionalisierter Datenschutz

Für die Gruppe der institutionalisierten Datenschützer (staatliche Datenschutzbeauftragte, Behörden, Stiftungen) bildet das Recht auf informationelle Selbstbestimmung den unverrückbaren normativen Rahmen.[51] Dieses Recht soll eine Situation gewährleisten, in der der Einzelne stets selbst darüber bestimmen kann, wer was wann und bei welcher Gelegenheit über sie oder ihn weiß.[52] Der institutionalisierte Datenschutz spielt gegenüber dem Staat eine Doppelrolle. So agieren Behörden (etwa das Bundesamt für Sicherheit in der Informationstechnik), staatliche Datenschutzbeauftragte (z. B. die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) und Stiftungen (z. B. die Stiftung Datenschutz) als staatliche Institutionen. Andererseits gehört es zum Auftrag dieser Institutionen, die Bürger u.a. gegen Organe eben dieses Staates zu schützen: Schutz der Staatsbürger *durch* den Staat vor „externen" Gefahren, gleichzeitig Schutz der Staatsbürger *vor* dem Staat durch Verteidigung von Grundrechten.[53] Aus diesem Grund ist die Unabhängigkeit der staatlichen Datenschutzbeauftragten gesetzlich vorgeschrieben und durch ein wegweisendes Urteil des Europäischen Gerichtshofs weiter gestärkt worden.[54]

In dem Maße, in dem der institutionalisierte Datenschutz dem staatlich vorgegebenen normativen Rahmen verpflichtet ist, orientiert er sich insbesondere am geltenden Recht. Diesbezüglich fallen nun vor allem zwei Dinge auf: Erstens erfolgt der Verweis auf das Recht üblicherweise gemeinsam mit einem *auf das Individuum bezogenen Selbstaktivierungsimperativ*.[55] Zweitens wird wiederholt in Rechnung gestellt, *dass das Recht im Bereich Datenschutz selbst an deutliche Grenzen stößt*.[56] Folgerichtig finden sich im Selbstdatenschutzdiskurs der Datenschützer wiederholt Aufforderungen technische Selbstdatenschutzpraktiken auszubilden,[57] sowie der Verweis auf Initiativen zur Bewusstseinsschaffung und Stärkung von Medienkompetenz. Auch hier treten wiederum zwei Problematiken auf. Sowohl die Bundesdatenschutzbeauftragte als auch eine Reihe von Datenschutzbeauftragten der Länder stehen strukturell den jeweils verantwortli-

Wer hat ein Interesse an Selbstdatenschutz und warum?

chen Innenministerien sehr nahe. Diese politische Nähe zur Innen- und Sicherheitspolitik lässt vermuten, dass einige Datenschützer die Ausbildung von Selbstdatenschutzpraktiken immer nur unter Vorbehalt und bis zu einem gewissen Grad propagieren können. Verschlüsselungstechniken lassen sich etwa auch für Kommunikationen einsetzen, die der Organisation krimineller oder staatsgefährdender Aktivitäten dienen, und dies steht in offensichtlichem Widerspruch zum innenpolitischen Kontrollanspruch.[58] Die zweite Problematik besteht in der Nicht-Zuständigkeit einiger Datenschützer für die Vermittlung jener Kompetenzen und Techniken, welche für die Entwicklung von Selbstdatenschutzpraktiken erforderlich sind. Hier nehmen sie ausdrücklich den Staat in die Pflicht,[59] jedoch beschränkt sich die Macht der Datenschützer – zumindest in dieser Hinsicht – eben weitgehend auf solche Appelle. In diesem Sinne sehen sich die institutionellen Datenschützer zwar dem Datenschutz verpflichtet und bekommen bis zu einem gewissen Grad auch die notwendig kollektive Anstrengung in den Blick, die die Gewährleistung desselben erfordert; die Ausbildung von Selbstdatenschutzpraktiken können sie aufgrund ihrer ambivalenten Rolle aber nur bedingt propagieren, und die erforderliche institutionelle Macht haben sie nicht inne.

3.4 Politik: Regierung und parlamentarisch vertretene Parteien

Die im Parlament vertretenen Parteien[60] verfügen über die institutionelle Macht, die Bildung von Selbstdatenschutzpraktiken zu fördern, sind jedoch in zwei Typen von strukturellen Widersprüchen verstrickt, die einer solchen Förderung grundsätzlich entgegenstehen. Der erste betrifft den interessenvermittelnden Charakter der Politik. Die informationelle Privatheit der Bürger wird gegenüber anderen Gütern abgewogen, und hierbei sind vor allem wirtschaftliche Interessen entscheidend. Dies zeigt sich etwa auf parteipolitischer Ebene: Zwar erkennen alle Parteien ein „Recht auf Privatsphäre" an, geben diverse Maßnahmen zu dessen Wahrung an und treten rhetorisch für die Stärkung von Medienkompetenz ein, doch unterscheiden sie sich bei der normativen Gewichtung der Privatheit in Bezug auf Wirtschaftsinteressen. So deutet die CDU in ihrem Wahlprogramm das Spannungsverhältnis an,[61] und setzt ausdrücklich auf Selbstregulierung, Eigenverantwortung – und eben Selbstdatenschutz.[62] Diese Betonung nimmt dann über SPD, Bündnis 90/GRÜNE bis zu DIE LINKE immer weiter ab.[63] Dennoch ist zu erwarten, dass Parteien mit Regierungsverantwortung der Abwägung zwischen Privatheitsschutz und Wirtschaftsinteressen größeres Gewicht im Sinne letzterer einräumen (siehe dazu weiter unten).

Der zweite strukturelle Widerspruch betrifft das Spannungsverhältnis zwischen den Interessen des Staates selbst und der Gesellschaft. Auf Regierungsebene tritt der Widerspruch vor allem in Form von Konflikten zwischen einzelnen Ressorts auf, die sich mitunter die Wahrung unterschiedlicher Interessen zur Aufgabe gemacht haben. Während sich das Bundesministerium des Innern für die Gewährleistung der inneren Sicherheit zuständig sieht, gilt das Interesse des Ministeriums der Justiz und für Verbraucherschutz verstärkt letzterem – und damit auch dem „Recht auf Privatheit."[64] Dass das Spannungsverhältnis in der Tat ein strukturelles ist, wird daran ersichtlich, dass der moderne Staat seine Existenz nicht zuletzt dem Einsatz differenzierter Überwachungstechniken verdankt,[65] da diese den administrativen Zugriff auf, und so wiederum die Verwaltung großer Populationen ermöglichen.[66] Nicht zuletzt gründet sich darin das *Sicherheitsinteresse* des Staates und im Diskurs wird oftmals angenommen, dass weit verbreiteter aktiver Selbstdatenschutz diesem Interesse zuwiderlaufe.[67] Sofern Selbstdatenschutz zumindest dann in Spannung zu ökonomischem und staatlichem Überwachungsinteresse geriete, wenn er tatsächlich flächendeckend praktiziert würde, ist die ernst gemeinte Förderung des Selbstdatenschutz durch Parlamente und daraus hervorgehende Regierungen sowohl auf Bundes- als auch Landesebene alles andere als wahrscheinlich. Aus diesem Grund lässt sich davon ausgehen, dass insbesondere ein Großteil der an Regierungen beteiligten Akteure, während sie über die Mittel (institutionelle

Macht) zur Erzeugung von effektiven Selbstdatenschutzpraktiken verfügen, im Gesamten betrachtet kein ernsthaftes Interesse daran haben.[68]

Wer hat ein Interesse an Selbstdatenschutz und warum?

3.5 Wirtschaftliche Interessenverbände

Die Vertreter der wirtschaftlichen Interessenverbände einschlägiger Industriebereiche, wie z. B. der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) e. V. oder der Bundesverband Digitale Wirtschaft (BVDW) e. V. tendieren dazu, soziale Akteure als Kunden innerhalb datengetriebener Märkte zu verstehen.[69] Allerdings ist hinter den Kulissen als Folge des NSA-Spähskandals ein interner Machtkampf im BITKOM zwischen Vertretern US-amerikanischer und deutscher Konzerne entbrannt, der richtungsweisend für die Ausrichtung des Interessenverbandes sein könnte.[70]
Im Diskurs dieser Verbände geht es um Selbstbestimmung, jedoch bezieht sich diese folglich in erster Linie auf das Treffen von Entscheidungen über die Inanspruchnahme von Konsumangeboten.[71] Sofern sich die von den Verbänden vertretenen Interessen auf marktwirtschaftliche Praktiken beziehen, lässt sich als zentraler Wert die Kategorie des Vertrauens identifizieren:[72] Die Abwesenheit von Vertrauen wirke sich schädlich auf Techniknutzung und damit auch auf Wirtschaft und Gesellschaft aus.[73] Datenschutz stelle dementsprechend das Mittel der Wahl dar, für das erforderliche Vertrauen zu sorgen.[74] Doch spielt der Datenschutz als solcher für die Wirtschaftsvertreter eine generell zweischneidige Rolle, da viele der Geschäftsmodelle der datenverarbeitenden Industrie auf der Gewinnung und Verarbeitung personenbezogener Daten basieren. Folgerichtig fordern sie eine „Balance zwischen der Sicherheit auf der einen und Freiheit des Einzelnen sowie der Berufsausübungsfreiheit der betroffenen Unternehmen auf der anderen Seite";[75] der Ausbau des „Erlaubnisgrund[s] der Wahrung berechtigter Interessen der Anbieter" sowie eine „Eingrenzung des Begriffs der 'personenbezogenen Daten'" sei angeraten.[76]
Damit wird die Aufweichung eines zentralen Eckpfeilers der informationellen Selbstbestimmung eingefordert.[77] Vor diesem Hintergrund, und mit Blick auf den Umstand, dass die Industrie die technischen Strukturen und deren Funktionsweise – also auch deren „Privatheitsfreundlichkeit" – maßgeblich gestaltet, muss auch der offizielle Aufruf zur „Befähigung zum Selbstschutz" der Nutzer[78] gesehen werden: An flächendeckenden Selbstdatenschutzpraktiken hat die Industrie aufgrund der bestehenden Geschäftsmodelle momentan größtenteils kein Interesse. Da solche Praktiken zum gegenwärtigen Zeitpunkt jedoch kaum in nennenswerter Breite etabliert sind, birgt der Selbstdatenschutz für sie – aktuell – jedoch auch wenig Konfliktpotential.

Kernpunkte

- Selbstdatenschutzpraktiken sind kollektiv gebildete, verfestigte Schutzroutinen, die 1) von menschlichen und technischen Komponenten gemeinsam geformt werden, und 2) eng mit soziokulturellen Verhaltensregeln, Werthaltungen, Wahrnehmungsweisen, Kompetenzen usw. verwoben sind.
- Der geringe Durchdringungsgrad von Selbstdatenschutzpraktiken in der Gesellschaft weist darauf hin, dass der allergrößte Teil der die Gesellschaft konstituierenden sozialen Welten – aus welchen Gründen auch immer – Selbstdatenschutzpraktiken nicht selbstorganisiert ausbildet.
- Sofern Praktiken generell kollektiv, d.h. in Sozialformationen, wie etwa der sozialen Welt der Cypherpunks gebildet, stabilisiert und erhalten werden, erfordert auch die Bildung von Selbstdatenschutzpraktiken in einer Vielzahl anderer sozialer Welten kollektive Anstrengungen.

Wer hat ein Interesse an Selbstdatenschutz und warum?	▪ Es ist allerdings unwahrscheinlich, dass jene Gruppen, auf die der Selbstdatenschutzdiskurs zurückgeht bzw. die an diesem Diskurs aktuell beteiligt sind, zur tatsächlichen Ausbildung von Selbstdatenschutzpraktiken in der Gesellschaft maßgeblich beitragen, weil diese Gruppen *entweder* nicht über die erforderlichen Strukturressourcen verfügen *oder* aufgrund struktureller Widersprüche kein Interesse an der Ausbildung besagter Praktiken haben.

4

Was denken und was tun Internetnutzer?

Da Selbstdatenschutz beschreibt, wie ein Einzelner die Erhebung seiner Daten durch öffentliche oder nicht-öffentliche Stellen begrenzt,[79] kommt man bei diesem Thema nicht umhin zu fragen, inwiefern Bürger mögliche technische, organisatorische und/oder rechtliche Maßnahmen auch tatsächlich umsetzen bzw. umsetzen können. Das folgende Kapitel widmet sich dieser Frage aus medienpsychologischer Perspektive. Es soll aufzeigen, wie Menschen im Hinblick auf Selbstdatenschutz denken und welche Hürden auftreten, wenn Selbstdatenschutz als individuelle Verantwortung jedes Einzelnen begriffen wird.

4.1 Sorgen um Privatheitsverletzungen und Maßnahmen des Selbstdatenschutzes

Aktuell macht sich die Bevölkerung zum Teil erhebliche Sorgen um ihre informationelle Privatheit im Internet.[80] Laut einer aktuellen, repräsentativen Umfrage sind 37 Prozent der deutschen Bevölkerung besorgt bis sehr besorgt um ihre Privatsphäre, wenn sie das Internet nutzen. Dabei fürchten 61 Prozent der Bürger, nicht ausreichend Einblick darüber zu haben, was Organisationen oder Websitebetreiber mit ihren Daten tun.[81] Gleichzeitig liefern verschiedene Studien Hinweise darauf, dass die partizipativen Möglichkeiten des Internets eine erhöhte Preisgabe privater Informationen wahrscheinlich machen.[82] In der medienpsychologischen Forschung ist deshalb immer wieder von einem sogenannten *Privacy Paradox*[83] die Rede, das unterstellt, Nutzer seien zwar um ihre informationelle Privatheit besorgt, würden aber nicht in gleicher Weise Maßnahmen zum Schutz dieser Privatheit ergreifen. Obwohl einige Studien vereinzelte Hinweise auf die Existenz jenes Paradoxons liefern,[84] ist bei einer Verallgemeinerung einer solchen angenommenen Einstellungs-Verhaltens-Diskrepanz dennoch Vorsicht geboten. Insbesondere ist sie an jeweilige situative Bedingungen gebunden und impliziert daher nicht, dass ein Schutz persönlicher Daten durch den Einzelnen überhaupt immer vollumfänglich möglich ist.

Zudem setzen Bürger einzelne Maßnahmen des Privatheitsschutzes durchaus bereits heute erfolgreich um. Dies scheint vor allem dann der Fall zu sein, wenn es darum geht, personenbezogene Inhalte vor Zugriffen anderer *Nutzer* zu schützen. Dies ist etwa am Nutzerverhalten auf Social Network Sites (SNS) zu beobachten. Obwohl der Großteil der bisherigen Untersuchungen in diesem Bereich auf nicht-repräsentativen Stichproben beruht, deren Erkenntnisgewinn vor allem bei deskriptiven Daten eingeschränkt ist, liefern sie erste Hinweise darauf, welche Möglichkeiten von Nutzern sozialer Netzwerkseiten überhaupt in Anspruch genommen werden, um die Preisgabe ihrer Daten zu kontrollieren. Hierzu zählt zum Beispiel die Verwendung von Pseudonymen anstatt des richtigen Namens[85] oder das Führen von Freundeslisten, um die Sichtbarkeit einzelner Statusupdates gegenüber bestimmten Kontakten einzuschränken.[86] Auch gibt es erste Hinweise darauf, dass deutsche Nutzer vor allem nach negativen Erfahrungen auf SNS seltener Informationen angeben, die sie identifizierbar machen.[87] Aus diesen Analysen lässt sich schließen, dass Menschen die ihnen zur Verfügung stehenden Maßnahmen des Selbstdatenschutzes vor allem dann ergreifen, wenn sie bereits Erfahrungen mit Übergriffen auf private Informationen gesammelt haben.[88]

Während Nutzer von den Strategien des Selbstdatenschutzes in interpersonellen – also horizontalen – Kontexten zumindest teilweise Gebrauch machen, unterliegen Selbstdatenschutzmaßnahmen im Hinblick auf vertikale Beziehungen zwischen Nutzern und *Organisationen* (z. B. Regierungen, Privatunternehmen, Internetdiensteanbietern etc.)

größeren Beschränkungen. Dies betrifft nicht nur Schutzmaßnahmen gegenüber Anbietern von Netzwerkplattformen, Messaging-Diensten, Internettelefonie oder E-Mail-Portalen, die häufig erst durch die Preisgabe personenbezogener Daten ihre „kostenlose" Nutzung möglich machen; es betrifft auch Situationen, in denen es primär um das Abrufen von Informationen oder den Kauf von Waren geht. Oftmals wird den Nutzern in jenen Kontexten vermutlich nicht einmal bewusst, dass ihre Daten gespeichert und weiterverarbeitet werden. Hinzu kommt, dass es die vielfältigen technischen Varianten des Datenzugriffs erschweren, informationelle Privatheit gezielt zu steuern. Diesem Problem begegnen die Bürger jedoch nicht mit Tatenlosigkeit (wie es das Privacy Paradox möglicherweise nahelegen würde), sondern mit ‚Generalmaßnahmen', die über verschiedene mögliche Gefahrensituationen hinweg einen gewissen Schutz der Privatheit versprechen. Laut einer repräsentativen Umfrage im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) gaben im vergangenen Jahr beispielsweise fast neun von zehn deutschen Internetnutzern an, eine Software installiert zu haben, die ihren Computer vor Viren schützen soll, und immerhin jeder dritte Befragte erklärte, regelmäßig seine Passwörter zu ändern, um Sicherheitslücken vorzubeugen. Ein weiteres Viertel der Befragten verschlüsselt regelmäßig personenbezogenen Daten. Derartige Sicherheitsvorkehrungen sind jedoch stark vom Alter der Nutzer abhängig: Je jünger die Nutzer – und je intensiver und vielfältiger damit auch die Inanspruchnahme des Internets als Informations- und Kommunikationsmedium – umso unbefangener gehen sie mit ihren Daten im Internet um, und dies obwohl sich jüngere Personen hinsichtlich ihrer Privatheitsbedenken kaum von älteren Personen unterscheiden.[89]

Auf Basis dieser Studien lässt sich vermuten, dass Nutzer dem Schutz ihrer Daten gegenüber anderen Nutzern einen hohen Stellenwert einräumen und auch Maßnahmen ergreifen, um der Erhebung, Auswertung und Analyse der eigenen Daten durch öffentliche und nicht-öffentliche Organisationen entgegenzuwirken. Warum dennoch von einer gewissen Kluft zwischen den Sorgen um informationelle Privatheit einerseits und der Umsetzung von Selbstdatenschutzmaßnahmen andererseits auszugehen ist, soll im Folgenden näher diskutiert werden.

4.2 Erklärungen für Einstellungs-Verhaltens-Diskrepanzen

In der medienpsychologischen Forschung existieren unterschiedliche Annahmen darüber, warum sich mögliche Privatheitssorgen in der Bevölkerung nicht eins zu eins in individuell ergriffene Schutzmaßnahmen überführen lassen. Sabine Trepte und ihre Kollegen formulierten dazu u. a. drei Hypothesen, die wir kurz vorstellen und kritisch diskutieren wollen:[90]

Die *Gratifikationshypothese* nimmt an, dass Internetanwendungen oftmals eine Vielzahl an Gratifikationen erfüllen. Im Bereich sozialer Netzwerke sind dies zum Beispiel soziale Anerkennung, Akzeptanz, soziale Unterstützung oder effektive Selbstdarstellung.[91] Hier erhalten Nutzer konkrete Belohnungen, wenn sie private Informationen preisgeben. Außerhalb des SNS-Kontextes spielen sicherlich auch die oft diskutierten Convenience-Aspekte eine wichtige Rolle: Der einfache und bequeme Zugriff auf Informationen oder die schnelle Abwicklung von Transaktionen im Internet könnten Gratifikationen darstellen, die dem Selbstdatenschutz – auch aufgrund bereits angesprochener Geschäftsmodelle und trotz bestehender Besorgnisse auf Nutzerseite – entgegenstehen. Aus Sicht der Gratifikationshypothese wird daher vermutet, dass bei der Nutzung von Online-Services durchaus eine Abwägung von Vorteilen und Risiken vorgenommen wird.[92]

Dabei ist jedoch zu bedenken, dass die Risiken nur schwer kalkulierbar und dem Nutzer daher mitunter nicht in all ihren Facetten bewusst sind bzw. sein können.

Die *Soziale Erwünschtheitshypothese* nimmt dagegen an, dass Nutzer die Probleme, die im Hinblick auf Privatheitsmanagement entstehen, durchaus kennen, wobei ihre Sorgen und Einstellungen jedoch vor allem einen Spiegel der medialen Berichterstattung darstellen.[93] Die Ergebnisse von Umfragen unter Mediennutzern reflektieren laut dieser Hypothese tendenziell eher die im massenmedialen Diskurs verhandelten Ansichten zu Datenschutz und informationeller Privatheit als die tatsächlichen, individuellen Sorgen und Wünsche innerhalb einer spezifischen Nutzungssituation.
Inwiefern es sich hierbei tatsächlich um soziale Erwünschtheit (oder doch eher Sekundärerfahrungen) handelt, ist noch zu prüfen, da Bürger in globalisierten, hoch diversifizierten Sozialstrukturen nur beschränkt außerhalb medialer Diskurse auf mögliche Risiken aufmerksam werden können. Dies trifft vermutlich besonders stark auf Privatheitsverletzungen zu, da deren Auswirkungen für den Einzelnen oft nicht unmittelbar spürbar und selbst für Experten schwierig zu kalkulieren sind.

Die *Kompetenzhypothese* besagt, dass Nutzer ihre Daten zwar schützen wollen, ihnen dazu aber häufig die notwendige Kompetenz fehlt. Entsprechend dieser Hypothese entsteht aufgrund fehlenden Wissens im Hinblick auf Datenschutzmöglichkeiten eine Einstellungs-Verhaltens-Diskrepanz. Privatheitskompetenz (engl. privacy literacy) verstehen Trepte et al. dabei als eine Kombination aus deklarativem und prozeduralem Wissen über Privatheit im Internet.[94] Unter deklarativem Wissen wird das Wissen über institutionelle Praktiken (z. B. Tracking, Datensammlung, -speicherung, -auswertung, -weitergabe), technische und rechtliche Aspekte (z. B. deutsche und EU-Gesetzgebung) von Datenschutz zusammengefasst. Prozedurales Wissen umfasst die Fähigkeit, individuelle Privatheitseinstellungen und Datenschutzstrategien auch tatsächlich umsetzen zu können.
Die Kompetenzhypothese nimmt also an, dass Bürger nur ein begrenztes Wissen und begrenzte Fähigkeiten besitzen, um einen effektiven Selbstdatenschutz zu gewährleisten. In der Tat zeigt eine repräsentative Bevölkerungsbefragung, die vom Fachbereich für Medienpsychologie von Mai bis Juni 2014 durchgeführt wurde, dass – trotz des aktuellen Mediendiskurses – 27% der Deutschen fälschlicherweise glauben, die NSA greife nur auf Daten zu, die öffentlich und sowieso für jedermann zugänglich sind. Auch wussten 56 Prozent der Befragten nicht, dass sie ein Recht darauf haben, bei Online-Anbietern die über sie gespeicherten Daten einzusehen.[95]
Viele Nutzer spüren auch selbst eine gewisse Unsicherheit in Bezug auf die Möglichkeiten des Selbstdatenschutzes. So schreiben sich momentan nur 35 Prozent der deutschen Internetnutzer die Kompetenz zu, E-Mails verschlüsselt versenden zu können; nur 17 Prozent trauen sich eine Einschätzung darüber zu, welche Informationen in Suchmaschinen, Online-Shops etc. über sie gespeichert werden.[96]

Die Ergebnisse der hier vorgestellten Studien legen die Vermutung nahe, dass Bürger derzeit nur begrenzt über die Infrastruktur und die Praktiken datensammelnder Akteure im Internet Kenntnis haben – ein Umstand, der vermutlich einem Wandel unterworfen ist, je nachdem wie deutlich derartige Praktiken in der Öffentlichkeit diskutiert werden. Weiterhin lässt sich aufgrund der bisherigen Erkenntnisse vermuten, dass technische wie auch rechtliche Datenschutzlösungen umso erfolgreicher angewendet werden können, je geringer die Anforderungen an die Nutzer, diese zu verstehen und einzusetzen, sind. Wie die Rahmenbedingungen für optimalen Selbstdatenschutz aus Nutzersicht aber konkret aussehen könnten und wo individueller Selbstdatenschutz seine Schranken findet, ist bislang noch weitestgehend unklar und bedarf weiterer Forschung.

Was denken und was tun Internetnutzer?

Kernpunkte

- Nutzer äußern ein verstärktes Interesse am Schutz ihrer informationellen Privatheit.
- Gleichzeitig wachsen die Sorgen - auch bedingt durch eine zunehmende Berichterstattung - vor unerwünschten Eingriffen in eben jene Privatheit.
- Nutzer setzen bereits heute vereinzelt Selbstdatenschutzmaßnahmen um.
- Der individuelle Selbstdatenschutz stößt dennoch an Grenzen. Mögliche Erklärungen hierfür sind zum Beispiel:
  - konkurrierende Bedürfnisse der Nutzer, die häufig mit einer Weitergabe personenbezogener Daten verbunden sind, und
  - begrenzte Fähigkeiten und Möglichkeiten, diesen Gefährdungen individuell entgegenzuwirken.

5
Technische Grundlagen

Im Zuge dieses Abschnitts wird ein Überblick technischer Ausspähmöglichkeiten von Nutzerdaten gegeben. Dabei werden potenzielle Angriffswege skizziert, die ausgenutzt werden können, um informationelle Privatheit zu kompromittieren.

5.1
Abstraktes Systemmodell

Abbildung 1 beschreibt die drei wichtigsten Dimensionen, die personenbezogene Daten bei ihrer Verarbeitung im Internet durchlaufen. Diese sind:

- (Mobile) Endgeräte der Nutzer,
- heterogene Kommunikationsnetze und
- Server der Diensteanbieter (Cloud of Clouds).

Die Endgeräte der Nutzer sind typischerweise mit verschiedenen Arten von Sensoren bestückt und in der Lage, Daten über Off- und Online-Aktivitäten zu erfassen und an Online-Diensteanbieter weiterzuleiten. Die Daten werden bei den Diensteanbietern verarbeitet, mit dem Ziel Produkte, die auf prognostizierbaren Bedürfnissen, Vorlieben, und Verhalten jedes Einzelnen zugeschnitten sind, anzubieten.

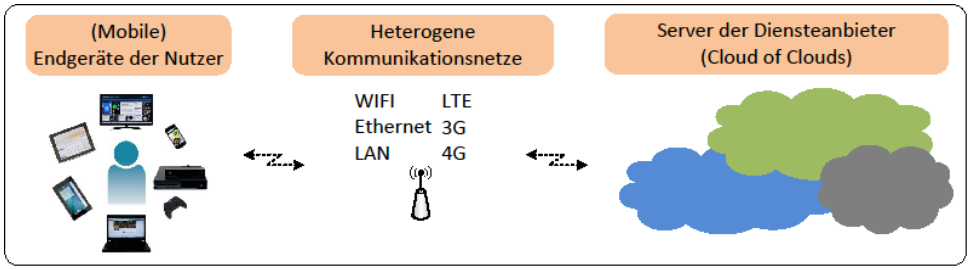

Abb. 01 Abstraktes Modell eines typischen IKT-Systems

Hier hat es einen Paradigmenwechsel hinsichtlich der Zugriffsrechte von Anbietern auf personenbezogene Daten gegeben: Im Gegensatz zu klassischen Computergeräten wie PCs und Laptops hat sich die Software-Architektur auf Smartphones und Tablets dahingehend verändert, dass weit mehr Zugriffsmöglichkeiten der Anbieter von Firmware, Betriebssystem und Apps auf personenbezogene und teilweise höchst private Daten wie Bilder, Videos, Kontakte, SMS, Kalenderdaten, usw. bestehen. Durch eingebaute Netzwerkschnittstellen sind diese Geräte in der Lage, die erfassten Daten entweder miteinander oder mit Komponenten auf Seiten der Diensteanbieter auszutauschen. Dies geschieht überwiegend über zwei Kommunikationsmodelle (Client-Server und Peer-to-Peer) sowie unter Verwendung unterschiedlicher (drahtloser) Übertragungstechnologien wie TCP/IP, 3G, Bluetooth, usw. Die an die Diensteanbieter übermittelten Daten werden i.d.R. verwendet, um eine Vielzahl personalisierter Online-Dienste zu ermöglichen. Die gesammelten Daten werden in großem Umfang auf ganz unterschiedlichen Systemen vorgehalten, die wir im Systemmodell als ‚Cloud' zusammenfassen. Obwohl heute existierende bzw. entstehende IT-Systeme ganz verschiedene Anwendungen ermöglichen und zweifellos komplexer als die obige Beschreibung sind, bietet das abstrakte Systemmodell eine Basis, um mögliche Angriffspunkte und Einfallstore aufzuzeigen.

5.2 Angriffe auf (mobile) Endgeräte der Nutzer

Smarte Objekte – seien es persönliche Kommunikationsgeräte oder „intelligente" Alltagsgegenstände wie Auto, Heizung, Fernseher – tragen zur Digitalisierung und Vernetzung unseres öffentlichen und privaten Lebens bei. Das weitverbreitetste Gerät dieser Art ist momentan das Smartphone. Zahlreiche Komponenten in Smartphones machen es möglich, Nutzerdaten über logische und physische Angriffswege abzugreifen.[97] Zum einen gibt es Angriffsmöglichkeiten auf die Software wie Apps, mobile Browser, Kommunikationsdienste (z.B. E-Mail) oder gar das Betriebssystem des Benutzergerätes. Ein typischer Angriff auf die Software ist das Einschleusen von Schadprogrammen (Trojaner, Spyware, etc.).[98] Daneben wird standardmäßig von Software-Anbietern auf eine Vielzahl von Online-Tracking-Techniken zurückgegriffen, um Nutzerdaten zu sammeln und auszuwerten. Dies passiert häufig über Techniken im Browser sowie Funktionen und Methoden der Web-Protokolle, die z.T. auch durch Dritte zweckentfremdet werden können. In den meisten Fällen geschieht dies ohne Wissen und Einwilligung der betroffenen Nutzer.[99] Ähnliche Tracking-Techniken finden auch Anwendung bei Smartphone-Apps[100] und im Bereich der Unterhaltungselektronik.[101] Physische Angriffe - also direkt auf die Hardware - können nur durchgeführt werden, wenn der Angreifer nah genug am Gerät ist, um auf Schnittstellen wie USB, Bluetooth oder NFC zuzugreifen. Über diese Schnittstellen findet dann die Schadsoftware für Datendiebstahl und/oder Überwachung ihre Wege auf das Benutzergerät.
In der Praxis gibt es meist eine Kombination aus Angriffen auf Software und Hardware verbunden mit einer gezielten Beeinflussung des Nutzers (sog. „social engineering"), damit dieser vertrauliche Informationen preisgibt.[102]

5.3 Angriffe auf Kommunikationsnetze

Die Kommunikation im Internet und anderen Formen von Computernetzwerken wird i.d.R. durch das Zusammenspiel zwischen unterschiedlichen aufeinander aufbauenden Protokollschichten geregelt. Eine wesentliche Rolle spielen hierbei Protokolle der TCP/IP-Familie, die den Umgang mit den Datenpaketen bzw. Datenströmen regeln. Beim Einsatz von TCP/IP-Protokollen können Nutzerdaten (wie etwa die IP-Adresse des Absenders, des Empfängers und ggf. Inhaltsdaten) gesammelt und ausgewertet werden. Eine IP-Adresse ist über Umwege eindeutig einem Gerät bzw. einer Person zuordenbar. Zudem können Dritte aus Datenpaketen, die über TCP/IP-Protokolle ausgetauscht werden, weitere Informationen über den Nutzer des Dienstes - wie etwa wann, wo, und wie lange bestimmte Dienste genutzt wurden - erlangen. Diese Möglichkeiten beschränken sich nicht auf die Internetnutzung. Auch Schwachstellen in Protokollen[103] und Architektur[104] der Mobilfunkkommunikation sind Einfallstore für ein systematisches Sammeln von Nutzerdaten.
Im Zusammenhang mit der Bekämpfung von Terrorismus und organisierter Kriminalität ist derartiges Sammeln personenbezogener Daten in vielen Teilen der Welt gesetzlich legitimiert. Hierbei werden vor allem zwei Strategien verfolgt:
Zum einen speichern Mobilfunkanbieter bzw. Internet Service Provider (ISPs) auch ohne konkreten Verdacht auf strafbare Handlungen alle Daten, die bei der Nutzung von Telekommunikations- und Internetdiensten anfallen, und stellen diese den Ermittlungsbehörden zur Verfügung. Hierzu werden in den meisten demokratischen Ländern ausschließlich sogenannte Metadaten – also Ort, Zeit, Dauer, Teilnehmer und Art der Dienste (E-Mail, SMS, Telefonie, etc.) und des Mediums (IP, Mobilfunk, etc.) – gesammelt und ausgewertet. Der Inhalt der Kommunikation wird ausdrücklich nicht aufbewahrt, kann aber mit umstrittenen Techniken wie der „*Deep Packet Inspection*" (DPI) analysiert werden.[105] Allerdings ermöglichen bereits die gesammelten Metadaten sehr exakte Rückschlüsse auf das Privatleben einzelner Personen. So können über Bewe-

gungsprofile, Aufenthaltsorte und Gewohnheiten teilweise sehr exakte Aussagen über soziale Beziehungen, sexuelle Orientierung oder politische Einstellungen getätigt werden.[106]
Zum anderen findet ein systematisches Abhören und Auswerten des Internetverkehrs über 1) die weltweit verteilten Austauschknoten der Internetkommunikation, an die alle ISPs eines Landes angeschlossen sind, und 2) die (inter-)kontinentalen Unterwasserkabel, über die ein großer Teil des weltweit verteilten Internetdatenverkehrs läuft, statt.[107] Hierbei bekommt der Angreifer auch Zugriff auf die Inhaltsdaten. Schließlich nutzen Strafverfolgungsbehörden und Geheimdienste beim Abhören von Kommunikation gezielt Sicherheitsschwachstellen in weitverbreiteten Übertragungsprotokollen (aber bspw. auch bei Krypto-Standards) aus, um sogenannte Hintertüren einzubauen, mit denen unter Umgehung installierter Sicherungsmechanismen auf die Kommunikation (oder weitere Funktionen des Endgeräts) zugegriffen werden kann.

5.4 Angriffsmöglichkeiten auf Server der Diensteanbieter

Cloud Computing als neues Paradigma zur Bereitstellung und Nutzung von IT-Diensten trägt dazu bei, dass immer mehr Webdiensteanbieter auf eine starre und z.T. kostenintensive hausinterne IT verzichten, um stattdessen ihre IT-Leistungen bedarfsgerecht und flexibel über das Internet beziehen zu können.[108] Greift ein Nutzer auf einen in der Cloud gehosteten Dienst etwa für E-Mail oder die Verwaltung von privaten Fotos zurück, so verliert er nach heutigem Stand der Technik damit auch i.d.R. die volle Kontrolle über diese Daten. Angriffsvehikel bei Cloud-basierten Diensten sind zahlreich.[109]

Kernpunkte:

- Internetbasierte IT-Systeme und Anwendungen werden immer komplexer und durchdringen jeden Aspekt unseres Lebens.
- Zahlreiche Komponenten in solchen Systemen und Anwendungen bieten Angreifern ideale Voraussetzungen, um unautorisiert und oft unbemerkt Zugriff auf personenbezogene Daten zu erhalten.
- Dabei kann zwischen Angriffsmöglichkeiten in drei Systemabschnitten unterschieden werden:
  - (Mobile) Endgeräte der Nutzer
  - Heterogene Kommunikationsnetze
  - Server von Diensteanbietern (Cloud of Clouds).

6
Technischer Selbstdatenschutz

Im Folgenden werden anhand des in 5.1 skizzierten abstrakten Systemmodells technische Lösungen für die jeweiligen Systemabschnitte (mobile) Endgeräte der Nutzer, Kommunikationsnetze und Server der Diensteanbieter (Cloud of Clouds) diskutiert.

6.1
Sicherheitslösungen für (mobile) Endgeräte der Nutzer

Selbstdatenschutztechniken, die Nutzer einsetzen können, um ihre in (mobilen) Endgeräten erfassten und zum Teil verarbeiteten Daten zu schützen, werden typischerweise in zwei Kategorien aufgeteilt: Maßnahmen zur Datenverschlüsselung und Sicherung des Endgerätes sowie Maßnahmen zum Schutz vor Tracking.

6.1.1 Maßnahmen zum Schutz sensibler Daten in Smartphone und PC

Auf Kommunikationsgeräten gespeicherte sensible Daten können mit Hilfe von Trojanern oder nach Verlust bzw. Diebstahl des Gerätes in falsche Hände geraten. Um sich gegen derartige Datenverluste zu schützen, können Nutzer die Daten verschlüsseln. Anwender können dazu entweder ihre gesamte Festplatte oder lediglich einzelne Dateien oder Ordner verschlüsseln. Man unterscheidet software- und hardwarebasierte Verschlüsselungslösungen.
Mit Pretty Good Privacy (PGP) Desktop und GNU Privacy Guard (GnuPG)[110] stehen Notebook- und PC-Nutzern zwei effektive (im Fall von GnuPG sogar kostenlose) Software-Lösungen zur Verfügung. Zu diesen gehörte bis vor Kurzem auch TrueCrypt. Allerdings wurde im Mai 2014 überraschend die Einstellung des TrueCrypt Projekts bekannt gegeben. IT-Sicherheitsexperten sind sich nun uneins, ob bisherige Versionen weiter als sicher gelten können. Hinlänglich bekannt ist hingegen, dass eine Weiterentwicklung der Software insbesondere aus lizenzrechtlichen Gründen nur unter erschwerten Bedingungen stattfinden kann.[111]
Hardware-Ansätze hingegen greifen auf spezielle Baugruppen des Computers zurück, die die Ver- und Entschlüsselung der Nutzerdaten vornehmen und ein sicheres Schlüsselmanagement ermöglichen. Heute weit verbreitete Hardware-Lösungen wie Bitlocker[112] oder Festplatten mit speziell eingebautem Krypto-Chip zielen primär auf eine Verschlüsselung der gesamten Festplatte und weniger auf den Schutz einzelner Dateien ab.
Für den Schutz sensibler Daten auf Smartphones und anderen mobilen Endgeräten steht Anwendern eine Vielzahl von Software-Lösungen zur Verfügung. Angeboten werden diese als eingeschränkte Maßnahmen auf Betriebssystemebene[113] oder durch Apps von Drittanbietern wie z.B. EDS Lite[114] oder Cryptonite,[115] mit denen sich beliebige Dateien auf dem mobilen Endgerät verschlüsseln lassen. Obwohl die technischen Grundlagen schon vor Jahren entwickelt wurden und in Situationen wie etwa beim Schutz von Regierung- bzw. Firmendaten zum Einsatz gekommen sind, wurden erst mit den Snowden-Enthüllungen Hardware-basierte Datenverschlüsselungs-Tools für eine breiteren Öffentlichkeit zugänglich.
Die verschlüsselten Daten sind sowohl bei Hardware- als auch bei Software-Lösungen durch ein Passwort oder ein biometrisches Merkmal (wie einen Fingerabdruck) geschützt. Ist das Passwort allerdings schlecht gewählt, so kann es von Unbefugten mit einfachen Mitteln geknackt werden. Verschlüsselung ist ein wichtiges Werkzeug, um persönliche Daten zu sichern. Da sie aber keinen vollständigen Schutz bieten kann, sollten Nutzer zusätzliche Maßnahmen ergreifen. So sollte der Nutzer den Zugriff von Programmen (insbesondere von Anbietern, deren Vertrauenswürdigkeit unklar ist) auf

Daten restriktiv einschränken. Darüber hinaus ist der Einsatz eines sicheren Passwort-Management Tools ,[116] die Nutzung von Anti-Malware („Virenscanner") und Anti-Tracking Tools zu empfehlen. Es gibt schließlich auch Betriebssysteme, die speziell für den Schutz von Privatsphäre und Anonymität entwickelt wurden. Für den Laien ist der Einsatz solcher Betriebssysteme allerdings aus verschiedenen Gründen (Gewährleistung des Herstellers, Kompatibilität mit Anwendungen, Nutzerfreundlichkeit) wenig realistisch.

6.1.2 Anti-Tracking-Maßnahmen

Anti-Tracking-Maßnahmen sollen den Nutzer davor schützen, dass sein Surfverhalten im Internet ungewollt und teilweise sogar unbemerkt aufgezeichnet wird. Dabei unterscheidet man zwischen 1) Einstellungen im Browser,[117] mit denen sich die Funktionsweisen von Trackinginstrumenten wie z. B. Cookies und JavaScript regulieren lassen, und 2) sogenannten Tracking-Blockern wie Disconnect.me,[118] Do Not Track Plus[119] oder Ghostery,[120] die überwiegend als Browser Plug-ins angeboten werden. Tracking-Blocker nutzen Techniken zum Aufspüren von Skripten auf Webseiten, die mit Negativlisten abgeglichen werden.[121] Das Blockieren von Tracking im Browser kann allerdings dazu führen, dass Webseiten nicht mehr richtig dargestellt werden.

6.2 Lösungen für sichere und anonyme Kommunikation

Die einfachste Möglichkeit, um vertrauliche Kommunikation sicherzustellen ist die Verwendung gängiger Verschlüsselungsprotokolle im Internet wie SSL/TLS (Secure Sockets Layer/Transport Layer Security) oder die Nutzung virtueller privater Netzwerke (VPN). Trotz Sicherheitsbedenken bzgl. der Implementierung solcher Protokolle[122] ist eine Übertragung vertraulicher Daten über SSL- bzw. VPN-Verbindungen in den meisten Fällen ratsam. Abhilfe in diesem Zusammenhang bieten u.a. Cloak[123] und HTTPS Everywhere[124], mit denen eine verschlüsselte Verbindung zu der besuchten Internetseite möglich ist. Andere Lösungsansätze sind häufig anwendungsspezifisch und integrieren unterschiedliche Kommunikationsprotokolle und kryptographische Funktionen. Beispiele solch anwendungsspezifischer Selbstdatenschutztools sind u.a. die E-Mail-Verschlüsselungstools PGP/GnuPG[125] bzw. S/MIME, Instant Messaging Software mit Ende-zu-Ende-Verschlüsselung wie Threema[126] und TextSecure,[127] sowie sichere (Video-)Telefoniedienste wie Jitsi[128] und Tox.[129]
Es fällt auf, dass vielfältige Möglichkeiten, digitale Kommunikation zu schützen, existieren. Allerdings erlauben anfallende Verbindungsdaten nichtsdestotrotz Rückschlüsse auf den Inhalt der Kommunikation.[130] Ein wirksamer Schutz kann zudem nur dann gewährleistet werden, wenn Schutztechniken in allen drei Dimension des vorher beschriebenen Systemmodells – also sowohl auf Nutzerendgeräten als auch auf Servern der Diensteanbieter - eingesetzt werden. Neben dem Schutzniveau sind vor allem Aspekte der Nutzerfreundlichkeit zu berücksichtigen. Denn jenseits des in Kapitel 2 beschriebenen fehlenden Interesses zentraler Akteure an einem effektiven Selbstdatenschutz von Bürgern gilt die komplizierte Handhabung von Verschlüsselungsdiensten als einer der wichtigsten Gründe für deren geringen Verbreitungsgrad.[131]
Im Folgenden werden zwei Beispiele präsentiert, die einen praktischen Eindruck von verfügbaren Selbstdatenschutztools für die verschlüsselte Kommunikation vermitteln sollen.

6.2.1 Beispiel – E-Mail-Verschlüsselung mit OpenPGP und S/MIME

Als sicher angesehene E-Mail-Kommunikation wird häufig mit einer sogenannten Ende-zu-Ende-Verschlüsselung versehen, d.h. Nachrichten werden, nachdem sie auf dem

Endgerät des Absender verschlüsselt wurden, erst auf dem Endgerät des Empfängers wieder entschlüsselt.[132]
Die Verschlüsselung kann auf verschiedene Arten erfolgen. Die Kryptographiesysteme OpenPGP[133] und S/MIME bauen bei der Emailverschlüsselung sowohl auf dem Prinzip der sogenannten symmetrischen als auch asymmetrischen Verschlüsselung auf. Bei der Kontaktaufnahme mit einem Kommunikationspartner benötigt man lediglich den sogenannten *öffentlichen Schlüssel* dieser Person. Dieser Schlüssel dient dazu, die Botschaft zu verschlüsseln, kann diese also nicht entschlüsseln. Das Entschlüsseln der Botschaft funktioniert hingegen nur mit dem sogenannten *privaten Schlüssel* des Adressaten. Da der Schutz des privaten Schlüssels zentral ist, wird dieser auf dem eigenen Endgerät aufbewahrt und niemals weitergegeben.[134]

> In jedem Fall ist es am Sichersten, wenn mir mein Kommunikationspartner seinen öffentlichen Schlüssel persönlich übergibt und mir zudem bestätigt, dass die verwendete E-Mail-Adresse auch wirklich seine E-Mail-Adresse ist. Damit soll verhindert werden, dass sich ein Angreifer mir gegenüber als mein befreundeter Kommunikationspartner ausgibt, mir einen gefälschten öffentlichen Schlüssel zuschickt und dasselbe gegenüber meinem befreundeten Kommunikationspartner tut: sich also als ich ausgibt. Ein solches Angriffsszenario wird als *Man-in-the-Middle Attacke* bezeichnet und kann die gesamte verschlüsselte Kommunikation kompromittieren. Wenn also eine persönliche Schlüsselübergabe nicht stattfinden kann, sind alle Kommunikationspartner darauf angewiesen die öffentlichen Schlüssel auf eine Weise auszutauschen, bei der sich alle Seiten sicher sein können, dass der Schlüssel auch tatsächlich einer bestimmten Person gehört, also authentisch ist.[135]

Was wird (nicht) geschützt?

Ein vollständiger Schutz ist erst dann gegeben, wenn alle drei sensiblen Komponenten einer E-Mail (Kopfzeile, Inhalt und Anhang) auf allen Ebenen (Endgeräte-, Übertragungs- und Cloud-Ebene) geschützt würden. Die Kopfzeile ist die erste sensible Komponente. Sie enthält Metadaten wie Absenderadresse, Betreff und Empfängeradresse. Die Kopfzeile bleibt bei der E-Mail-Verschlüsselung mit PGP und S/Mime unverschlüsselt. Die zweite sensible Komponente ist der Inhalt (body) einer E-Mail. Vollständig geschützt ist dieser Bestandteil einer E-Mail lediglich auf der Übertragungsebene. Die Endgeräte der Nutzer bleiben bei diesem Verfahren ungeschützt. Wenn ein Angreifer Zugriff auf das Nutzerendgerät und somit Zugang zum privaten Schlüssel erlangt, kann jede verschlüsselte Botschaft mithilfe des privaten Schlüssels entschlüsselt werden. Metadaten der Kopfzeile bleiben innerhalb der Cloud-Infrasktruktur (dritte Dimension) ungeschützt während für den Inhalt und den Anhang von E-Mails keine unmittelbare Gefahr ausgeht, da durch die Ende-zu-Ende-Verschlüsselung unterwegs abgefangene Daten - sofern der private Schlüssel nicht abhandenkommt oder gar in eine Cloud geladen und ausgelagert wird - für Angreifer unleserlich bleiben. Die dritte sensible Komponente bildet der Anhang einer E-Mail. Diese Komponente wird sowohl bei der Verschlüsselung mit OpenPGP als auch mit S/Mime geschützt.[136]

Eigenverantwortung oder Delegation von Verantwortung?

Zentraler Aspekt funktionierender E-Mail-Verschlüsselung ist die Herstellung von Glaubwürdigkeit hinsichtlich der öffentlichen Schlüssel. Diese Beglaubigung erfolgt über digitale Zertifikate, die an den öffentlichen Schlüssel geheftet werden, um deren Glaubwürdigkeit zu bestätigen. Während die Schlüsselbeglaubigung bei OpenPGP über eine dezentrale Struktur erfolgt, basiert sie bei S/MIME auf einer zentralen Struktur.

Bei **OpenPGP** erfolgt die Beglaubigung des öffentlichen Schlüssels beispielsweise über das „Web of Trust"-Prinzip (WoT). Dabei kann jeder Nutzer seinen Schlüssel veröffentlichen, indem dieser in eine öffentliche Schlüsseldatenbank[137] (Keyserver) eingetragen wird. In der Datenbank können Nutzer wiederum nach dem öffentlichen Schlüssel ihres Kommunikationspartners suchen, und wenn sie die Authentizität des Schlüssels bestätigen möchten, diesen Schlüssel durch ihre eigene digitale Unterschrift beglaubigen bzw. zertifizieren.[138]

> Wenn ich also einem mir bisher unbekannten Kommunikationspartner D eine Botschaft senden möchte, besteht die Möglichkeit, auf einem Keyserver zunächst nach dessen öffentlichem Schlüssel zu suchen. Prinzipiell kann sich hier ein Angreifer als D ausgeben, der öffentliche Schlüssel also gar nicht zu D gehören. Doch wenn ich sehe, dass mein befreundeter Kommunikationspartner A mit seiner digitalen Unterschrift den öffentlichen Schlüssel von D beglaubigt hat - also u.a. mir gegenüber versichert, dass der Schlüssel auch tatsächlich zu D gehört - sinken die Chancen dafür, dass der öffentliche Schlüssel von D kompromittiert ist. Und je mehr Personen die Authentizität von Person D und dessen öffentlichem Schlüssel beglaubigen, umso eher kann ich auf die Authentizität vertrauen, so dass ich dann bspw. nach erfolgreicher Kontaktaufnahme mit D die Glaubwürdigkeit seines Schlüssels mit meiner eigenen digitalen Unterschrift bestätige, sprich zertifiziere.[139] Je größer dieses Netz des Vertrauens ist, umso größer jedoch das Risiko, dass Nutzer allzu leichtfertig und ohne ausreichende Überprüfung fremde Schlüssel signieren und damit potentiellen Angreifern Tür und Tor öffnen.[140]

Bei **S/MIME** erfolgt die Beglaubigung bzw. Zertifizierung des öffentlichen Schlüssels nicht durch die Nutzer selbst, sondern durch eine als vertrauenswürdig geltende Zertifizierungsstelle bzw. Certificate Authority (CA). CAs (Firmen wie z.B. Verisign oder StartCom) beglaubigen über öffentliche Schlüssel hinaus auch Webseiten. Dabei wird den CAs vertraut, dass sie in der Lage und willens sind, die Glaubwürdigkeit eines Schlüssels zu überprüfen. Je nach Gründlichkeit der Prüfung werden Zertifikate in verschiedenen Qualitätsstufen ausgestellt.[141] Die Zertifizierungsstellen geben innerhalb ihrer Sicherheitsleitlinien die Regeln an, nach denen die Ausgabe der Zertifikate erfolgt, woraus sich die Aussagekraft und das Sicherheitsniveau der ausgestellten Zertifikate ableiten lassen. Allerdings entziehen sich die Zertifizierungsstellen einer unmittelbaren Kontrolle durch die Nutzer. Schließlich können technische Fehler oder fahrlässiges Verhalten durch die Mitarbeiter der CAs zu Sicherheitsproblemen führen, wie in der Vergangenheit mehrmals geschehen.[142]

Geschäftsmodell

OpenPGP ist ein an sich kostenloser Kryptographiestandard, der auf dem Idealismus einer freiwilligen Partizipation am WoT gründet. Viele Anwendungen die auf dem OpenPGP Standard basieren – wie GnuPGP – sind ebenfalls kostenlos. Es können jedoch Kosten entstehen, wenn OpenPGP in kommerzielle Anwendungen integriert wird. Eine **S/MIME**-Schnittstelle ist im Gegensatz zu PGP/GnuPG bei vielen Systemen bereits implementiert, so dass in der Regel keine Kosten durch kostenpflichtige Zusatzdienste entstehen. Durch die zentrale Beglaubigungsstruktur bzw. die damit zusammenhängende Abhängigkeit von CA- Zertifikaten entstehen jedoch Kosten bei der Zertifikatserstellung. Zertifikate können in verschiedenen (meistens drei) Qualitätsstufen ausgestellt werden, die sich auch im Preis unterscheiden.[143]

6.2.2 Beispiel – Sicheres Instant Messaging

Instant Messaging ermöglicht das weitgehend kostenlose Versenden von beliebig vielen Kurznachrichten (inkl. Fotos und Videos) über das Internet. Folgende Fallbeispiele wurden ausgewählt und analysiert:

- *WhatsApp* hat sich hier als größter Anbieter mit einer Nutzerzahl von über 450 Millionen Nutzer (Stand Feb. 2014) etabliert, wurde allerdings auch oftmals kritisiert aufgrund mangelnder Datensicherheit – hier insbesondere aufgrund fehlender Verschlüsselung – und Unklarheit, was mit den massenhaft gesammelten Kommunikations- und Inhaltsdaten passiere.[145]
- Beflügelt durch die WhatsApp-Übernahme durch Facebook stellt *Threema* momentan eines der größten Konkurrenzprodukte in Deutschland dar, wo der auf Ende-zu-Ende-Verschlüsselungstechnik zurückgreifende Dienst insbesondere im Februar 2014 einen massiven Anstieg seiner Nutzerzahlen verzeichnen konnte.[146]
- *TextSecure* ist ein quelloffener, verschlüsselt arbeitender Instant Messaging Dienst, der kostenlos angeboten wird und vor allem dadurch Berühmtheit erlangte, dass Edward Snowden ihn 2014 ausdrücklich empfahl.[147]

Verschlüsselung und deren rechtliche Grenzen

Während WhatsApp keine Ende-zu-Ende-Verschlüsselung einsetzt – der Anbieter (aber auch Dritte) also mitlesen können – bieten sowohl Threema als auch TextSecure dieses Feature an. Allerdings müssen Diensteanbieter sowohl in den USA als auch in der Schweiz (Serverstandort von Threema) auf Anfrage von Strafermittlungsbehörden Zugang zu gespeicherten Kommunikationsinhalten gewähren. Während hier in den USA bereits erwähnte Gesetze wie der USA PATRIOT Act oder CALEA einschlägig sind, unterliegt die Threema GmbH als Schweizer Unternehmen insbesondere dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF).[148]

Offener Quellcode

Im Gegensatz zu WhatsApp und Threema liegt TextSecure ein offener Quellcode zugrunde, was nicht nur dazu führt, dass die Qualität der eingesetzten Verschlüsselung von unabhängigen Experten überprüft[149], sondern auch nachvollzogen werden kann, was das Programm de facto mit den gesammelten und verarbeiteten Daten macht.[150] Obwohl IT-Sicherheitsexperten Threema das Einsetzen sicherer Verschlüsselungstechnik bescheinigen[151], kann nicht überprüft werden, wie gut diese Verschlüsselung in die Software eingebettet worden ist und was mit den Kommunikationsdaten geschieht, bevor sie verschlüsselt werden.[152] Während deswegen einem kommerziellen Anbieter von verschlüsselten Kommunikationsdiensten, der den Quellcode der angebotenen Programme nicht veröffentlicht, auf Grundlage der rechtsverbindlichen Zusicherungen in den AGB und in der Datenschutzerklärung vertraut werden muss,[153] ist der Nutzer beim Einsatz quelloffener Software wie TextSecure auf die Fähigkeit und Motivation der Entwickler-Community[154] angewiesen. Allerdings zeigt der jahrelang unentdeckt gebliebene Heartbleed-Programmierfehler: Theoretische Kontrollierbarkeit heißt nicht, dass dies auch jemand tut oder Sicherheitslücken tatsächlich gefunden werden.[155] Zudem gibt es häufig keine Garantie dafür, dass die angebotene Instant Messaging Software auf dem Server des Anbieters mit demselben der Öffentlichkeit zur Verfügung gestellten Quellcode arbeitet.
Der Threema-Entwickler Manuel Kaspar gibt schließlich zu bedenken, dass letztendlich auch die beste (Privacy) App nichts nütze, wenn das Betriebssystem dahinter nicht vertrauenswürdig sei.[156]

Privacy by default

Threemas Alleinstellungsmerkmal im Vergleich zu WhatsApp und TextSecure ist, dass Kontaktdaten nicht automatisch mit denen auf dem Server des Anbieters abgeglichen werden, sondern manuell und offline durch die ID eines Kommunikationspartners (eine achtstellige Kombination aus Buchstaben und Zahlen) hinzugefügt werden können. Eine ähnliche Funktion bietet auch TextSecure an, allerdings ohne das automatische Übertragen von Adressbuchdaten auf den TextSecure Server zu unterbinden. Die Verifizierung der Schlüssel wird bei Threema durch das manuelle (offline) Scannen des QR-Codes des Kommunikationspartners vom Nutzer selbst übernommen, wodurch insbesondere einer Man-in-the-middle-Attacke vorgebeugt werden soll.

Geschäftsmodelle

Obwohl das Geschäftsmodell von Whatsapp nicht wie bei Facebook und Google originär auf Werbung und dem damit verbundenen Sammeln und Verarbeiten von Nutzerdaten gründet, sondern sich vor allem aus Abogebühren der App speist[157], so hat die massive Datensammelwut (von Meta- und Adressdaten, Bild- und Videomaterial, Kommunikationsinhalte, etc.) des Unternehmens doch schon vielfältig für Kritik gesorgt. Mit der Übernahme durch Facebook wurde nun auch eine häufig kritisierte Klausel in den AGB von WhatsApp relevant, die im Falle einer Übernahme des Unternehmens dem Käufer den Zugriff und die weitere Verwendung aller bis dahin erhobenen Daten ermöglicht.[158] Der Konkurrent Threema setzt auf Datensicherheit und Vertraulichkeit als zentrales Verkaufsargument. Im Gegensatz zu WhatsApp finanziert sich Threema durch eine einmalige Gebühr (1,69 – 1,79 €). Die Threema GmbH beschreibt sich selbst als sogenannter *Zero Knowledge Provider*, der zum einen keinerlei Zugriffsmöglichkeiten auf die verschlüsselten Kommunikationsinhalte hat[159], und zum anderen keine Metadaten aufzeichnet.[160] Allerdings ist nicht abschließend geklärt, welche Daten bspw. an Strafermittlungsbehörden weitergereicht werden müssen. Die Open-Source Variante TextSecure wurde vom Unternehmen Whisper Systems (um den angesehenen IT-Sicherheitsexperten Moxie Marlinspike), das 2011 von Twitter gekauft wurde, entwickelt.[161] Kurz darauf wurde beschlossen TextSecure und RedPhone (eine App für verschlüsselte IP-Telefonie) in Form des Open Whisper Systems Projektes, das zumindest formal unabhängig von Twitter ist, als Open-Source Software weiter zu führen und zu entwickeln. Die Finanzierung von TextSecure basiert größtenteils auf Spenden, da die App kostenlos ist.[162] Insbesondere Entwickler- und Serverkosten müssen jedoch gedeckt werden, so dass sich auch hier die Frage einer langfristigen Finanzierungsstrategie stellt, die nicht die Unabhängigkeit des Projektes gefährdet.[163]

6.3 Anonymisierungstools und –dienste

Während der Entstehung des Internets war einer der Treiber der Vernetzung von Netzen das Prinzip der Offenheit. Wesentliche Protokolle des Internets wurden so gestaltet, dass eine möglichst reibungslose Kommunikation erfolgen kann.[164] Wer also Internetdienste nutzt, hinterlässt digitale Spuren, mit denen sich sehr exakte Rückschlüsse auf das Privatleben der Nutzer ziehen lassen. Eine anschauliche Demonstration, wie viele und welche Daten über den Nutzer bei der nichtanonymen Verwendung eines Webbrowsers anfallen, lässt sich beispielsweise auf der Website von JonDonym durchführen.[165] Was und wie viel diese Informationen über einen Nutzer verraten können, zeigen verschiedene Experimente.[166] Ein effektiver Schutz derartiger Spuren im Netz kann durch Anonymisierungsdienste erreicht werden. Mit Tor und JonDonym sollen im Folgenden zwei Anonymisierungsdienste vorgestellt und diskutiert werden, die eine weitgehende Anonymisierung erlauben.

In der Kopfzeile jedes Datenpakets, das im Internet zirkuliert, ist neben der Zieladresse auch die Absenderadresse angegeben, in der die spezifische IP-Adresse des Absenders enthalten ist. Die IP-Adresse kann bei diesem Vorgang nicht weggelassen, sondern nur verschleiert werden. Das Prinzip der Verschleierung folgt dem Prinzip einer sog. Proxy-Kaskade, d.h. das Datenpaket, dessen IP-Adresse verschleiert werden soll, wird auf dem Weg zur Zieladresse verschlüsselt und an mehrere Zwischenstationen umgeleitet. Das Datenpaket übernimmt beim Erreichen jeder Zwischenstation deren jeweilige IP-Adresse, die fortan als Absender erscheint, wodurch die Zugehörigkeit des Datenpakets zum eigentlichen Absender verschleiert wird. Bei Erreichen der Zieladresse wird nun lediglich die IP-Adresse der letzten Zwischenstation als Absender angezeigt, während alle zuvor angesteuerten Zwischenstationen dazu dienen, die Verschleierung zu verbessern.[167]
Ein wesentlicher Unterschied zwischen dem Tor-Netzwerk und JonDonym besteht in der Art und Weise, wie die Zwischenstationen angesteuert werden. Zudem verbindet Tor den Nutzer alle 10 Minuten über eine neue Proxy-Kaskade, während JonDonym jeden Website-Zugriff einzeln anonymisiert.[168]
Dokumente, die von Edward Snowden bereitgestellt wurden, legen nahe, dass die NSA nach dem derzeitigen Stand der Technik weder dazu in der Lage ist, eine großflächige Echtzeitüberwachung aller Tor-Nutzer zu realisieren, noch einzelne Tor-Nutzer gezielt ausfindig machen kann. Überwachbar durch mühevolle, manuelle Analyse sei lediglich ein kleiner Anteil von Tor-Nutzern.[169]

6.3.1 Beispiel – Freies Anoymisierungsnetzwerk „Tor"

Was wird (nicht) geschützt?

Auf der Übertragungsebene wird die Information geschützt, wer mit wem und wann kommuniziert hat. Dies gilt aber nicht unbedingt für die Inhalte, die eine Identifikation des Nutzers ebenfalls möglich machen können. Während die Effektivität des Tor-Netzwerks einerseits vor allem vom spezifischen Surf-Verhalten eines jeden Nutzers abhängt[170] gibt es darüber hinaus eine Reihe an Möglichkeiten, den Nutzer trotz IP-Verschleierung durch Tor identifizierbar zu machen.[171] Während diese Möglichkeiten bisher nur unter Laborbedingungen realisierbar schienen, wird seit der im November 2014 von Europol, dem FBI und dem Heimatschutzministerium der Vereinigten Staaten durchgeführten „Operation Onymous" nicht mehr ausgeschlossen, dass eine großflächige Deanonymisierung von Tor-Nutzern möglich ist. Die Tor-Community diskutiert derweil über verschiedene Angriffsszenarien, doch wo genau die Schwachstellen liegen, ist bislang nicht geklärt.[172]

Eigenverantwortung der Community

Innerhalb des dezentralen Tor-Netzwerks kann jeder Nutzer als Zwischenstation fungieren und damit die Effektivität des Systems insgesamt erhöhen. Diese Knoten können je nach dem Standort des Nutzers, theoretisch auf dem gesamten Erdball verteilt sein. Um Schwachstellen wie Java Applets oder Flash-Objekte zu vermeiden, die bei einer unvorsichtigen Nutzung des Tor-Netzwerks eine Deanonymisierung zur Folge haben können, kann das Tor Browser Bundle verwendet werden.[173] Für Smartphones auf Android-Basis gibt es mit Orbot eine mobile Alternative zur Desktop-Variante.[174] Die Geschwindigkeit von Tor ist mit etwa 240 kBit/s recht langsam. Die meisten Aktivitäten im Internet können mit dieser Geschwindigkeit aber weiter durchgeführt werden. Lediglich größere Downloads und Live Video-Streaming bringen das Netzwerk an seine Grenzen.[175]

Geschäftsmodell

The Tor Project ist eine spendenbasierte Non-Profit Organisation, die im Jahr 2012 Einnahmen im Wert von über 2 Millionen US-Dollar generieren konnte. Ungefähr 60% dieser Einnahmen kommen aus dem US-amerikanischen Staatshaushalt. So wurde etwas mehr als 40% des TOR-Jahresbudgets 2012 über das *Stanford Research Institute* vom US-Verteidigungsministerium bereitgestellt. Weitere 20% verteilen sich auf *Internews Network*, die *New America Foundation* und die *National Science Foundation* mit dem US-Außenministerium im Hintergrund.[176] Die übrigen 40% der Einnahmen kommen durch Privat- und Unternehmensspenden zustande. Allerdings machte der Anteil privater Spenden im Jahr 2011 nur 4% der Gesamteinnahmen aus.[177]

Überwachungsschnittstellen

Nach derzeitigem Stand der Technik könne es bei Tor keinerlei Hintertüren bzw. offizielle Überwachungsschnittstellen geben - auch nicht zum Zwecke der Strafverfolgung. Jedoch stünden die Tor-Betreiber hier unter Druck. Denn Tor-Mitbegründer Roger Dingledine räumt durchaus ein, dass die US-Regierung als wichtigster Finanzier einen „gewichtigen Einflussfaktor auf Entscheidungen des Teams darstellen [könne]."[178] Jedoch bestünde die US-Regierung eben nicht nur aus NSA-Unterstützern. Teile der US-Regierung, von denen die Geldmittel stammten, hätten großes Interesse an einem Internet, innerhalb dessen Privatheit und Anonymität geschützt werden würden. So hätten Angehörige des US-Außen- und Verteidigungsministeriums ein ganz besonderes Interesse an TOR im Sinne eines US-amerikanischen Demokratie-Exports, damit oppositionelle Gruppen wie in Ägypten oder Syrien trotz Überwachung über das Internet kommunizieren könnten. Hier würden eingebaute Schwachstellen – die letztlich von jedem (Geheimdienst) gefunden werden könnten – über Leben oder Tod entscheiden.[179]

6.3.2 Beispiel – Kommerzieller Anonymisierungsdienstleister „JonDonym"

Delegation von Verantwortung

Bei JonDonym kann im Gegensatz zu Tor nicht jeder Nutzer als Zwischenstation (*Mix*) fungieren. Stattdessen vertraut der Dienst auf feste Betreiber und fungiert in Form der JonDonym Certification Authority selbst als Zertifizierungsstelle, um Betreiber zertifizieren zu können und somit eine hohe Qualität des Dienstes zu gewährleisten.[180] Die hohe Qualität ist jedoch nur in der Premium-Variante garantiert, während die kostenfreie Variante um wesentliche Funktionen reduziert ist.

Geschäftsmodell

Die Premium-Variante kostet je nach Laufzeit und Volumen zwischen 5 € und 100 €. Damit wird gegenüber der kostenfreien Variante und auch gegenüber Tor mit über 600 kBit/s eine weitaus höhere Übertragungsgeschwindigkeit, ein besserer Schutz gegen Website-Fingerprinting, die Gewährleistung einer internationalen Verteilung der Zwischenstationen in zwei bis drei Staaten und über drei Zwischenstationen gewährleistet.[181]
Angaben eines Entwicklers zufolge rentiert sich JonDonym bislang finanziell kaum. Die Einnahmen würden weder für einen zweiten Vollzeit-Programmierer, noch für ein Büro oder eine tarifähnliche Bezahlung reichen. Doch es wäre angesichts der Bedeutung von

Anonymität für das Leben von Menschen, die unter einer repressiven Diktatur wie im Iran leben, „zuviel, um JonDos sterben zu lassen."[182]

Überwachungsschnittstellen

Im Gegensatz zu Tor kann bei JonDonym eine Strafverfolgung im Internet stattfinden. Um einen einzelnen Nutzer zu deanonymisieren, müssen alle Betreiber einer Mix-Kaskade eine in ihrem jeweiligen Land gültige behördliche Anweisung dazu erhalten. Nach Angaben von JonDonym wurde diese Anforderung für Premium-Kaskaden bisher jedoch noch nie erfüllt. Zudem veröffentlicht JonDonym jedes Jahr einen Bericht über die durchgeführten behördlichen Überwachungsmaßnahmen.[183]

Kernpunkte:

- Um unbefugte Zugriffe auf sensible Daten zu verhindern, können Nutzer eine Reihe von günstig zu erwerbenden, jedoch nicht immer einfach anzuwendenden technischen Schutzmaßnahmen einsetzen.
- Allerdings garantieren diese Maßnahmen erst in ihrer Gesamtheit, d.h. angewendet in allen drei Systemabschnitten (Endgerät des Nutzers, Kommunikationsnetze und Server der Diensteanbieter) einen wirkungsvollen und effektiven Schutz.

7
Fazit

Bereits vor über 30 Jahren wurde im Rahmen des Volkszählungsurteils die staatliche Schutz- und Förderpflicht der informationellen Selbstbestimmung formuliert. Trotzdem wurden von staatlicher Seite seither kaum nennenswerte Anstrengungen unternommen dieser Schutzpflicht nachzukommen, so dass von verschiedenen Seiten Selbstdatenschutzpraktiken entwickelt und forciert wurden, die es jedoch allesamt nicht geschafft haben, eine faktische Durchsetzung der informationellen Selbstbestimmung (vor allem im Internet) zu bewerkstelligen. Da (informationelle) Privatheit aber keine Frage individueller Vorlieben ist, sondern vor allem einen gesellschaftlichen Wert konstituiert, der kennzeichnend für ein freiheitlich-demokratisches Gemeinwesen ist, birgt die Selbstdatenschutzdebatte um vermeintliche Verantwortlichkeiten des Individuums die Gefahr, die eigentliche Schutzpflicht des Staates in diesem Bereich zu verschleiern. Deswegen ist es wichtig festzuhalten, dass eine vollständige Verlagerung staatlicher Schutzpflichten auf das Individuum in keiner Art und Weise der gesellschaftlichen Bedeutung des Grundrechts auf informationelle Selbstbestimmung gerecht werden würde.

Gerade angesichts der im Zuge der Enthüllungen Edward Snowdens offenkundig gewordenen, weltweiten Überwachungsinfrastruktur von Geheimdiensten zeigt sich die Unmöglichkeit der Realisierung eines umfassenden, effektiven und durch den Nutzer gewissenhaft umgesetzten Selbstdatenschutzes. Obgleich einzelne Praktiken und Anwendungen existieren, mit deren Hilfe einzelne Aspekte des Selbstdatenschutzes realisiert werden können, gibt es kein Patentrezept für die Lösung allgegenwärtiger Datenschutzprobleme. Angesichts der fortschreitenden Digitalisierung weiterer Lebensbereiche, einer massiven Ausbreitung datengetriebener Geschäftsmodelle (auch über den IKT-Sektor hinaus) und dem Ziel der NSA und anderer Geheimdienste die Daten von *jedermann, jederzeit und überall* abgreifen zu können, kommt dem Staat - aber auch der Gesellschaft als Ganzer - die Aufgabe zu, oftmals bereits bestehende Konzepte zur Durchsetzung des Grundrechts auf informationelle Selbstbestimmung in die Praxis umzusetzen. Die politische Realisierung eines solchen Grundrechtschutzes wird nicht einfach sein, da weniger Überwachung auch immer mit einem geringeren Kontrollanspruch aller - auch europäischer und nationaler - staatlicher und privatwirtschaftlicher Akteure verbunden ist. Doch wird man sich zugleich die Frage stellen müssen, inwiefern die Kehrseite eines solchen Kontrollanspruchs - ein allwissender und damit potentiell allmächtiger Staat - sich mit der Vorstellung einer freien und selbstbestimmten Gesellschaft deckt.

Anhang

An dieser Stelle verweisen wir auf weitere Informationsquellen zum Thema (Selbst)Datenschutz sowie beispielhaft auf Anleitungen für die Einrichtung von E-Mail-Verschlüsselung für unterschiedliche Systeme.
Wie wir jedoch bereits im White-Paper problematisiert haben, gibt es kein Patentrezept für die Gewährleistung eines umfassenden und effektiven Datenschutzes. Auch die Verschlüsselung von E-Mails sollte hier nur als Teilaspekt im systemischen Ansatz des technischen Selbstdatenschutzes verstanden werden.

Informationsquellen

Stiftung Datenschutz http://stiftungdatenschutz.org/
BSI für Bürger https://www.bsi-fuer-buerger.de/
Verbraucher im Internet http://www.verbraucheriminternet.de/
Verbraucherzentrale Bundesverband http://www.vzbv.de/Datenschutz.htm
Projekt „Surfer haben Rechte" http://www.vzbv.de/surfer-haben-rechte.htm

Anleitungen zur Einrichtung von E-Mail-Verschlüsselung

Desktop:

Anleitung für die Verschlüsselung von E-Mails mit **S/Mime** in Thunderbird/Firefox
http://page.mi.fu-berlin.de/lohr/email/thunder/index.html

Anleitung für die Verschlüsselung von E-Mails mit **PGP** in Thunderbird
https://www.verbraucher-sicher-online.de/anleitung/e-mails-verschluesseln-in-mozilla-thunderbird-mit-enigmail-und-gnu-privacy-guard

Anleitung für die Verschlüsselung von E-Mails/Dateien mit **S/Mime** innerhalb von Windows/Explorer/Outlook (2010/2013) http://page.mi.fu-berlin.de/lohr/email/outlook/index.html

Anleitung für die Verschlüsselung von E-Mails/Dateien mit **PGP** bzw. dem Programm **GPG4win** in Windows/Explorer/Outlook https://www.der-webcode.de/dateien-verschluesseln-mit-gpg4win-installation-und-schluesselerzeugung/

Anleitung für die Verschlüsselung von E-Mails mit **S/Mime** und Apple Mac OS X 10
http://page.mi.fu-berlin.de/lohr/email/mac/index.html

Anleitung für die Verschlüsselung von E-Mails mit **PGP** (GPGTools) in Apple Mail
https://www.verbraucher-sicher-online.de/anleitung/bildfolge-e-mails-verschluesseln-in-apple-mail-mit-gpgmail

Mobil:

Anleitung für die Verschlüsselung von E-Mails mit **S/Mime** im Mail-Programm unter iOS http://www.heise.de/ct/artikel/Brief-mit-Siegel-1911842.html

Anleitung für die Verschlüsselung von E-Mails mit **PGP** mithilfe der App **oPenGP (Lite)** unter iOS https://www.der-webcode.de/pgpopenpgp-verschluesselung-auf-dem-ipad-nutzen/

Anleitung für die Verschlüsselung von E-Mails mit **S/Mime** mithilfe der App Djigzo unter Android: https://blog.netways.de/2013/07/05/smime-emailsicherheit-auf-android/

Anleitung für die Verschlüsselung von E-Mails mit **PGP** mithilfe der Apps **K9** und **APG** in Android: https://thomas-leister.de/allgemein/android-pgp-e-mail-verschluesselung-mit-k9-und-apg/

Anmerkungen

[1] Aus Gründen der Lesbarkeit wird im Folgenden auf das Gendern von Personengruppen verzichtet.
[2] Vgl. Giddens, Anthony (1995): Die Konstitution der Gesellschaft: Grundzüge einer Theorie der Strukturierung. 3. Aufl., Frankfurt, New York: Campus; Ochs, Carsten (2013): Digitale Glokalisierung das Paradox von weltweiter Sozialität und lokaler Kultur. Frankfurt am Main, New York: Campus (Campus Forschung, 963); Dourish, Paul / Anderson, Ken (2006): Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. In: Human-Computer Interaction 21, Nr. 3, S. 319-342.
[3] Vgl. http://www.saechsdsb.de/datenschutz-fuer-buerger/112-selbstdatenschutz (25.04.14).
[4] Vgl. Reißmann, Ole (2012): Cryptoparty-Bewegung: Verschlüsseln, verschleiern, verstecken. In: Spiegel-Online, abrufbar unter. http://www.spiegel.de/netzwelt/netzpolitik/cryptoparty-bewegung-die-cypherpunks-sind-zurueck-a859473. html; Peikert, Denise (2013): Cypto-Party: Anleitung zur digitalen Selbstverteidigung. In: FAZ.net, abrufbar unter: http://www.faz. net/aktuell/rhein-main/crypto-party-anleitung-zur-digitalen-selbstverteidigung-12309561.html; Bernold, Matthias (2012): Cypherpunk goes Mainstream, abrufbar unter: http://derbernold.com/2012/12/04/cypherpunk-goes-mainstream/; Beuth, Patrick (2013): Überwachung – Mein digitaler Schutzschild. In: ZEIT ONLINE, abrufbar unter: http://www. zeit.de/digital/datenschutz/2013-01/serie-mein-digitaler-schutzschild-einleitung; vgl. daneben die versch. Websites der Kryptoparty-Bewegung, z.B. unter http://www.cryptoparty.in/ (alle 25.04.14).
[5] Um informationelle Privatheit geht es, „wenn Personen den Anspruch haben, vor unerwünschtem Zugang im Sinne eines Eingriffs in persönliche Daten über sich geschützt zu werden". Vgl. Rössler, Beate (2001): Der Wert des Privaten. Frankfurt/M., S. 25.
[6] BVerfGE 65, 1 ff.
[7] BVerfGE 65, 1 (42 f.).
[8] BVerfGE 65, 1 (43).
[9] BVerfGE 65, 1 (43).
[10] BVerfG, NJW 1981, S. 1656.
[11] EuGH, Urt. v. 8.4.2014, Rs. C-293/12 und C-594/12; BVerfGE 125, 260; vgl. auch Roßnagel, Alexander (2014 i.E.): Neue Maßstäbe für den Datenschutz in Europa. In: Multimedia und Recht (MMR), S. 372-377.
[12] Das ergibt sich aus der Grundrechtsdogmatik (Abwehrrecht und Schutzpflicht) des BVerfG, aber vor allem aus der Natur der informationellen Selbstbestimmung an sich. Denn auf Grund des Grundrechts muss gewährleistet sein, dass der Einzelne in der Lage ist, seine Daten gegenüber Dritten zu schützen. Vgl.: BVerfGE 33, 303 (333); 46, S. 106 (164 f.).
[13] Siehe ausführlich Roßnagel, Alexander (2013), in: ders. (Hrsg.), Handbuch Datenschutzrecht, München, Kap. 3.4. Selbstdatenschutz umfasst auch die Wahrnehmung von Betroffenenrechten des TKG, TMG und BDSG. Anwendbar sind diese Gesetze gemäß § 1 Abs. 5 Satz 2 BDSG auch für Dienste mit Sitz im Ausland, da personenbezogene Daten der Nutzer im Inland durch eine verantwortliche Stelle mit Sitz in einem Drittland erhoben werden. Die Übermittlung der Daten in Drittländer wie die USA ist nur gestattet, wenn dieses ein dem europäischen Recht vergleichbares Datenschutzniveau bietet. Das zwischen der EU-Kommission und dem US-Handelsministerium geschlossene Safe-Harbor-Abkommen, zu dem sich US-amerikanische Firmen verpflichten können, soll ein solches angemessenes Schutzniveau bieten.
[14] Sokol, Bettina (2011), in: Spiros Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Aufl., München, § 13 BDSG, Rn. 26.

[15] Roßnagel, Alexander (o. Fußn. 13), Kap. 3.4, Rn. 69.
[16] Zum Beispiel die Funktion Do-Not-Track oder Plug-ins und Add-ons wie Ghostery, BetterPrivacy etc.
[17] Roßnagel (o. Fußn. 13), Kap. 3.4, Rn. 73 mwN.
[18] § 3 Abs. 6 Bundesdatenschutzgesetz (BDSG). Der unverhältnismäßige Aufwand ist relativ zu bestimmen, also danach, welches Wissen für eine Re-Identifizierung der datenverarbeitenden Stelle konkret zur Verfügung steht, Buchner, Benedikt (2013), in: Taeger, Jürgen / Gabel, Detlev, Kommentar zum BDSG, 2. Aufl., Frankfurt/Main, § 3 BDSG, Rn. 45.
[19] Roßnagel (o. Fußn. 13), Kap. 3.4, Rn. 58 f.
[20] Hansen, Marit (2011), in: Roßnagel (o. o. Fußn. 13), Kap. 3.3, Rn. 91; Spindler, Gerald / Nink, Judith (2011): Pflichten des Diensteanbieters. In: Spindler, Gerald / Schuster, Fabian (Hg.): Recht der elektronischen Medien, Kommentar, 2. Aufl., München, § 13 TMG, Rn. 12.
[21] Z.B. § 3a BDSG und § 13 Abs. 6 Telemediengesetz (TMG).
[22] Roßnagel (o. Fußn. 13), Kap. 3.4, Rn. 13.
[23] Telekommunikationsdienste sind gemäß § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Diensteanbieter ist gemäß § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Es kommt weder auf die Gewinnerzielungsabsicht an noch darauf, ob diese Dienste für jedermann oder nur einer bestimmten Gruppe, etwa Arbeitnehmern bei der privaten Mitbenutzung eines Firmennetzwerks, angeboten werden. Ob Instant-Messaging-Dienste Telekommunikationsdienste sind, ist umstritten, vgl. Schneider, Mathias (2014): WhatsApp & Co. - Dilemma um anwendbare Datenschutzregeln. In: Zeitschrift für Datenschutz (ZD), Mai 2014, S. 231 ff.
[24] §§ 111 ff. Telekommunikationsgesetzes (TKG)
[25] Eckhardt, Jens (2013): Daten für Auskunftsersuchen der Sicherheitsbehörden. In: Geppert, Martin / Schütz, Raimund (Hg.): Beck'scher TKG-Kommentar, 4. Aufl., § 111 TKG, Rn. 24, S. 2461-2473.
[26] § 3 Abs. 2, § 7 Abs. 1 Telekommunikationsüberwachungsverordnung (TKÜV).
[27] § 2a Bundesnachrichtendienstgesetz (BNDG) bzw. § 8a Bundesverfassungsschutzgesetz (BVerfSchG). Dazu ausführlich: Voigt, Paul (2014): Weltweiter Datenzugriff durch US-Behörden, MMR 2014, S. 161.
[28] Der PATRIOT Act umfasst eine Reihe von Änderungen bereits bestehender Gesetze und Verordnungen, wie dem Foreign Intelligence Surveillance Act (FISA), der zusammen mit dem Änderungsgesetz Foreign Intelligence Surveillance Amendments Act 2008 (FISAA) US-amerikanischen Behörden die Überwachung der Telekommunikation sowohl von US- als auch Nicht-US-Bürgern erlaubt und umfassende Auskunftserlangung ermöglicht; Becker, Philipp / Nikolaeva, Julia (2012): Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG. In: Computer und Recht (CR) 2012, 171; Voigt, Paul / Klein, David (2013): Deutsches Datenschutzrecht als "blocking statute"?, Auftragsdatenverarbeitung unter dem USA PATRIOT Act. In: Zeitschrift für Datenschutz (ZD) 1/2013, 17.
[29] Becker / Nikolaeva, CR 2012, S. 171 f.; Vogt / Klein, ZD 2013, S. 17; ein aktuelles Urteil eines Bundesgerichts in New York vom 25.4.2014 hat dies jüngst bestätigt, Roos, US-Internetunternehmen müssen im Ausland gespeicherte Daten herausgeben. In: heise online vom 28.4.2014, abrufbar unter: http://heise.de/-2178454 (29.07.2014).
[30] Lejeune, Mathias (2013): Datenschutz in den Vereinigten Staaten von Amerika. In: Computer und Recht (CR) 11/2013, S. 756.
[31] Section 103 i.V.m. 106 CALEA.
[32] Bodden, Eric / Rasthofer, Siegfried / Richter, Philipp /Roßnagel, Alexander (2013): Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps, Technische

Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps. In: Datenschutz und Datensicherheit (DuD) 11/2013, S. 720-725.

[33] Die Auswahl der ersten drei genannten Gruppen beruht auf einer Recherche zum Thema (welche Gruppen positionieren sich überhaupt im Selbstdatenschutzdiskurs?). Bei Politik und Wirtschaft wurde indes gezielt nach Positionierungen gesucht, da es sich bei diesen – als normativer Rahmensetzer bzw. als Anbieter von Anwendungen – um einflussreiche Akteure in Bezug auf die Ausgestaltung von Selbstdatenschutzpraktiken handelt.

[34] So machten sich bereits in den 1980er Jahren deutsche IT-Sicherheitsexperten Gedanken dazu, vgl. Pfitzmann, Andreas / Waidner, Michael (1986): Networks without user observability - design options. In: Pichler, Franz (Hg.): Advances in Cryptology - EUROCRYPT '85. Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques, Berlin, Heidelberg, S. 245-25; Pfitzmann, Andreas / Pfitzmann, Birgit / Waidner, Michael (1988): Datenschutz garantierende offene Kommunikationsnetze. In: Informatik Spektrum 11, Nr. 3, S. 118-142.

[35] Bei der Kontroverse ging es um die Aushandlung bindender Normen zum Gebrauch kryptographiebasierter Verschlüsselungstools, vgl. Winkel, Olaf (2000): Netzwerksicherheit – (k)ein Thema für Sozialwissenschaftler. In: Rubin 2/2000, S. 6-12, abrufbar unter: http://www.ruhr-uni-bochum.de/rubin/rbin2_00/pdf/artikel_g1_netzwerk.pdf (25.04.14).

[36] Vgl. http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ (25.04.14).

[37] Hughes, Eric (1993): A Cypherpunk's Manifesto, vgl. http://activism.net/cypherpunk/manifesto.html (25.04.14).

[38] So etwa Hughes in „A Cypherpunk's Manifesto."

[39] Vgl. http://www.bitkom.org/de/markt_statistik/64026_78217.aspx (25.04.14).

[40] Z.B. Chaos Computer Club, Digitalcourage e.V., Deutsche Vereinigung für Datenschutz e.V. usw.

[41] Z.B. die Betreiber von Websites wie etwa www.informationelle-selbstbestimmung-im-internet.de, www.selbstdatenschutz.info, www.netzausglas.de, www.daten-speicherung.de.

[42] Vgl. http://digitalcourage.de/themen/datenschutz-und-buergerrechte (25.04.14).

[43] Vgl. http://ccc.de/de/club (25.04.14).

[44] Vgl. http://ccc.de/de/hackerethik (25.04.14).

[45] Vgl. http://aktion-freiheitstattangst.org/ (25.04.14).

[46] Vgl. https://www.datenschutzverein.de/themen/datenschutz-im-internet/ (25.04.14).

[47] Vgl. http://informationelle-selbstbestimmung-im-internet.de/ (25.04.14).

[48] Vgl. http://www.selbstdatenschutz.info/ (25.04.14).

[49] Vgl. http://www.selbstdatenschutz.info/datenschutzprobleme (25.04.14).

[50] Vgl. http://ccc.de/de/club (25.04.14).

[51] Während uns völlig bewusst ist, dass wir hier Organisationen mit sehr unterschiedlichem rechtlichen Status (z.B. in puncto ministerieller Weisungsgebundenheit) zu einer einzigen Gruppe zusammenfügen, bildet das Hauptkriterium dafür eben die starke Bindung an staatlich vorgegebene Normsetzungen. Auch wenn der Grad stark variiert, weisen folglich alle hier aufgeführten Organisationen eine gewisse Staatsnähe auf, welche ihrerseits zu bestimmten diskursiven Positionierungen führt.

[52] Vgl. BVerfGE 65, 1 (43).

[53] Vgl. dazu etwa die Aussage der neuen BfDI im Rahmen eines Interviews unter http://www.dw.de/globales-netz-braucht-globalen-datenschutz/a-17421683 (25.04.14).

[54] Vgl. EuGH, Urteil vom 9. März 2010, Rs. C-518/07, Slg. 2010, I-1885. Vgl.: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=416862 (25.04.14).

Weiterführende Literatur: Schütz, Philip (2012): The Set Up of Data Protection Authorities as a New Regulatory Approach. In: Gutwirth, Serge / Leenes, Ronald / De Hert, Paul / Poullet, Yves (ed.): European Data Protection: In Good Health?, Dordrecht: Springer, 2012, S. 125-142.

[55] Vgl. http://www.datenschutz-berlin.de/content/service/selbstdatenschutz (25.04.14). In ähnlicher Weise äußert sich die Stiftung Datenschutz in der Broschüre „Ihr gutes Recht im Datenschutz" („Datenschutz – es liegt an ihnen", vgl. S. 17) unter http://stiftungdatenschutz.org/category/aktuelles/) und der BfDI in der Broschüre „Datenschutz – meine Rechte" http://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Datenschutz_MeineRechte.pdf?__blob=publicationFile (25.04.14).

[56] Vgl. http://www.dw.de/globales-netz-braucht-globalen-datenschutz/a-17421683 (25.04.14).

[57] So Voßhoff selbst, vgl. http://www.dw.de/wie-ist-die-privatsph%C3%A4re-zu-retten/a-17425091 (25.04.14).

[58] Darauf verweist etwa der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit auf seiner mit „Sicherheit mit Kryptographischen Verfahren" betitelten Website unter http://www.tlfdi.de/tlfdi/ themen/technischer_datenschutz/sicherheit/ (25.04.14).

[59] Vgl. die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. März 2010, unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile; vgl. des Weiteren die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. März 2013 unter http://www.bfdi.bund.de/SharedDocs/Publikationen/ Entschliessungssammlung/DSBundLaender/85DSK_EU Grundverordnung.pdf?__blob=publicationFile; vgl. ebenso die Äußerungen des Hamburger Datenschutzbeauftragten unter http://www.datenschutz-hamburg.de/news/detail/article/meine-daten-kriegt-ihr-nicht-projekt-tritt-in-2-phase-ein.html (alle 25.4.14).

[60] Die folgenden Aussagen basieren auf einer Analyse der Wahlprogramme von CDU/CSU, SPD, Die Linke und Bündnis 90/die Grünen; zusätzlich wurde der Koalitionsvertrag zwischen CDU/CSU und SPD ausgewertet. Hier die Quellenangaben (alle 25.04.14): http://www.cdu.de/sites/default/files/media/dokumente/regierungs programm-2013-2017-langfassung-20130911.pdf; http://www.spd.de/linkableblob/96686/data/20130415_regierungsprogramm_2013_2017.pdf; http://www.die-linke.de/fileadmin/download/wahlen2013/bundestagswahlprogramm/bundestagswahlprogramm2013_langfassung.pdf; http://www.gruene.de /fileadmin/user_upload/Dokumente/Gruenes-Bundestagswahlprogramm-2013.pdf; https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

[61] CDU-Regierungsprogramm „Gemeinsam erfolgreich für Deutschland", S. 35, vgl. http://www.cdu.de/ sites/default/files/media/dokumente/regierungsprogramm-2013-2017-langfassung-20130911.pdf (25.04.14).

[62] Vgl. die „Antworten der Christlich Demokratischen Union Deutschlands (CDU) und der Christlich-Sozialen Union in Bayern (CSU) auf die Fragen des Bundesverbandes Digitale Wirtschaft (BVDW) e.V.", S. 5-6, abrufbar unter www.bvdw.org/ mybvdw/media/ download/ 02-bvdw-cdu-csu-antworten-wahlpruefsteine.pdf?file=2946 (25.04.14).

[63] Dies deckt sich weitgehend mit der gründlichen Analyse der Parteipositionierungen zum politischen Diskurs über Privatsphäre in Sozialen Netzwerken, die Baumann vorgelegt hat. Zwar bezieht er sich auf die letzte Legislaturperiode und einen leicht abweichenden Gegenstand, es finden sich darin jedoch nahezu dieselben Muster wieder. Vgl. Baumann, Max-Otto (2013): Datenschutz im Web 2.0: Der politische Diskurs über Pri-

vatsphäre in sozialen Netzwerken. In: Ackermann, Ulrike (Hg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter. Frankfurt/M., S. 15-52.
[64] Vgl. die Eröffnungsrede von Heiko Maas zur Eröffnung des Safer Internet Day am 11.2.14 in Berlin unter http://www.bmj.de/SharedDocs/Reden/DE/2014/20140211_Rede_Safer_Internet_Day.html?nn=2708420 (25.4.14); vgl. des Weiteren die Ressortkontroverse um die Vorratsdatenspeicherung unter http://www.n24.de/n24/Nachrichten/Politik/d/4562650/heiko-maas-hat-keine-eile--thomas-de-maizi%C3%A8re-schon.html (25.04.14).
[65] Giddens, Anthony (1995): Die Konstitution der Gesellschaft. Grundzüge einer Theorie der Strukturierung. Frankfurt/M., S. 180.
[66] Ebd., S. 238.
[67] Vgl. hierzu Fußnote 9.
[68] „Je mehr politische Macht ein Akteur besitzt, d.h. je mehr er den Staat verwaltet, desto geringer dürfte seine Bereitschaft zum Datenschutz sein." Baumann, Max-Otto (2013): Datenschutz im Web 2.0: Der politische Diskurs über Privatsphäre in sozialen Netzwerken. In: Ackermann, Ulrike (Hg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter. Frankfurt/M., S. 15-52, Zitat S. 47.
[69] BVDW (2013): Goslarer Programm: Medien- und netzpolitisches Grundsatzpapier des Bundesverband digitale Wirtschaft (BVDW) e.V., S. 4, abrufbar unter: www.bvdw.org/mybvdw/ media/ download/ leitfaden-mepo-goslarer-programm-2013.pdf?file=2789 (25.04.14).
[70] Berke, Jürgen (2014): Echte Zerreißprobe. In: WirtschaftsWoche, Nr. 8, 17.2.2014.
[71] Ebd., S. 5.
[72] Vgl. http://www.bitkom.org/de/themen/50790.aspx; in diesem sinne auch der BITKOM-Präsident unter http://www.dw.de/wie-ist-die-privatsph%C3%A4re-zu-retten/a-17425091 (25.04.14).
[73] BITKOM-Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit 2013, S. 1, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Positionspapier_Abhoermassnahmen.pdf (25.4.14).
[74] BVDW (2013): Goslarer Programm, S. 7.
[75] BITKOM-Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden 2013, S. 5.
[76] BVDW (2013): Goslarer Programm, S. 7.
[77] Vgl. die Definition „personenbezogener Daten" durch den BfDI unter http://www.bfdi.bund.de/SharedDocs/ Publikationen/Faltblaetter/Datenschutz-ist.pdf?__blob=publicationFile (25.4.14).
[78] BITKOM-Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden 2013, S. 6.
[79] Der Sächsische Datenschutzbeauftragte (2013): Selbstdatenschutz, Was ist Selbstdatenschutz? Vgl. http://www.saechsdsb.de/datenschutz-fuer-buerger/112-selbstdatenschutz (01.08.2014) .
[80] Vgl. Eurobarometer (2010): E-communications household survey. Brussels, unter: http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf; Eurobarometer (2011): Attitudes on data protection and electronic identity in the European Union. Brussels, unter: http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf; DIVSI (2013): DIVSI Studie zu Freiheit versus Regulierung im Internet. Hamburg, unter: https://www.divsi.de/wp-content/uploads/2013/12/divsi-studie-freiheit-v-regulierung-2013.pdf.
[81] Trepte, Sabine / Masur, Philip K. / Dienlin, Tobias (2014 i.E.). Eine repräsentative Umfrage zu Privatheit im Internet, Manuskript in Vorbereitung.

[82] vgl. z.B. Leung, Louis (2009): User-generated content on the internet: An examination of gratifications, civic engagement and psychological empowerment. New Media & Society, 11, S. 1327-1347.
[83] Barnes, S. B. (2006): A privacy paradox: Social networking in the Unites States. In: First Monday, 11(9). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312
[84] z. B. Acquisti, A. / Gross, R. (2006, June): Awareness, information sharing, and privacy on the facebook. Paper presented at the 6th Workshop on privacy enhancing technologies, June 28 - June 30 2006, Cambridge; Taddei, S. / Contena, B. (2013): Privacy, trust and control: Which relationships with online self-disclosure? Computers in Human Behavior, 29(3), 821–826. doi: 10.1016/j.chb.2012.11.022; Tufekci, Z. (2008): Can you see me now? Audience and disclosure regulation in online social network sites. In: Bulletin of Science, Technology & Society, 28(1), 20-36.
[85] Dienlin, T. / Trepte, S. (in press): Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. In: European Journal of Social Psychology.
[86] Trepte, S. / Dienlin, T. / Reinecke, L. (2013): Privacy, self-disclosure, social support, and social network site use. Research Report of a three-year panel study. Stuttgart.
[87] Trepte, S. / Dienlin, T. / Reinecke, L. (2014): Risky behaviors: How online experiences influence privacy behaviors. In B. Stark, O. Quiring & N. Jackob (Hg.): Von der Gutenberg-Galaxis zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy. Surveying old and new frontiers after 50 years of DGPuK (S. 225-244). Wiesbaden.
[88] Dienlin, T., / Trepte, S. (in press): Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. In: European Journal of Social Psychology.
[89] DIVSI (2013): DIVSI Studie zu Freiheit versus Regulierung im Internet. Hamburg, unter: https://www.divsi.de/wp-content/uploads/2013/12/divsi-studie-freiheit-v-regulierung-2013.pdf.
[90] Trepte, S. / Teutsch, D. / Masur, P. K. / Eicher, C. / Fischer, M. / Hennhöfer, A. / Lind, F. (in press): Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In. S. Gutwirth et al. (Hrsg.). Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective. Dordrecht/New York: Springer.
[91] Ellison, N. B. / Steinfield, C. / Lampe, C. (2007): The benefits of Facebook ‘‘friends:’’ Social capital and college students’ use of online social network sites. In: Journal of Computer-Mediated Communication, 12(4), 1143-1168. doi: 10.1111/j.1083-6101.2007.00367.x; Joinson, A. N. (2008): 'Looking at', 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook. Paper presented at the CHI 2008, New York; Papacharissi, Z. / Mendelsohn, A. (2011): Toward a new(er) sociability: Uses, gratifications, and social capital on Facebook. In: S. Papathanassopoulos (Hg.): Communication and Society. Media perspectives for the 21st century. Concepts, topics and issues (pp. 212-230). New York. Smock, A. D. / Ellison, N. B. / Lampe, C. / Wohn, D. Y. (2011): Facebook as toolkit: A uses and gratifications approach to unbundling feature use. In: Computers in Human Behavior, 27, 2322-2329.
[92] Ellison, N. B. / Vitak, J. / Steinfield, C. / Gray, R. / Lampe, C. (2011): Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte / L. Reinecke (Hg.): Privacy online. Perspectives on privacy and self-disclosure in the social web (pp. 19-32). Berlin Taddicken, M. / Jers, C. (2011): The uses of privacy online: Trading a loss of privacy for social web gratifications? In S. Trepte & L. Reinecke (Hg.): Privacy online. Perspectives on privacy and self-disclosure in the social web (pp. 143-158). Berlin.
[93] Trepte, S. / Dienlin, T. / Reinecke, L. (2014): Risky behaviors: How online experiences influence privacy behaviors. In B. Stark, O. Quiring & N. Jackob (Hg.): Von der Guten-

berg-Galaxis zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy. Surveying old and new frontiers after 50 years of DGPuK (S. 225-244). Wiesbaden.
[94] Trepte, S. / Teutsch, D. / Masur, P. K. / Eicher, C. / Fischer, M. / Hennhöfer, A. / Lind, F. (in press): Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In. S. Gutwirth et al. (Hrsg.). Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective. Dordrecht/New York: Springer.
[95] Trepte, Sabine / Masur, Philip K. / Dienlin, Tobias (2014 i.E.). Eine repräsentative Umfrage zu Privatheit im Internet, Manuskript in Vorbereitung.
[96] DIVSI (2013): DIVSI Studie zu Freiheit versus Regulierung im Internet. Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet, unter: https://www.divsi.de/wp-content/uploads/2013/12/divsi-studie-freiheit-v-regulierung-2013.pdf. Für Deutschland besteht hinsichtlich des Wissens um Privatheits-Gefährdungen und individuelle Datenschutz-Maßnahmen noch immer hoher Forschungsbedarf. Daher führt der Lehrstuhl für Medienpsychologie an der Universität Hohenheim derzeit mehrere Projekte durch, die sich mit der Erfassung von Privatheitskompetenzen sowie den Entstehungsbedingungen und Hürden beim Ausbau dieser Kompetenzen beschäftigen (Trepte, Masur & Teutsch (in prep): Measuring Internet Users' Online Privacy Literacy. Development and Validation of the Online Privacy Literacy Scale (OPLIS).)
[97] Biermann, Kai (2014): Der Spion in der Tasche, Die ZEIT, Nr. 23; Einen guten graphischen Überblick liefert hierzu: Heider, Jens / El Khayari, Rachid (2012): Geht Ihr Smartphone fremd? In: Datenschutz und Datensicherheit - DuD 36, 3/2012.
[98] Snowden-Enthüllungen: NSA plant Schadsoftware für die Massen: http://www.spiegel.de/netzwelt/netzpolitik/snowden-enthuellungen-nsa-setzt-auf-automatisierte-ueberwachung-a-958324.html (29.07.2014); Bickford, Jeffrey / O'Hare, Ryan / Baliga, Arati / Ganapathy, Vinod / Iftode, Liviu (2010): Rootkits on Smart Phones: Attacks, Implications and Opportunities. In: HotMobile '10 Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, Feb. 2010, S. 49-54.
[99] Ur, Blasé / Leon, Pedro G. / Cranor, Lorrie Faith / Shay, Richard / Wang, Yang (2012): Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In: Technical Report CMU-CyLab-12-007, April 2, 2012. SOUPS 2012.
[100] Zhou, Xiaoyong / Demetriou, Soteris / He, Dongjing / Naveed, Muhammad / Pan, Xiaorui / Wang, XiaoFeng / Gunter, Carl A. / Nahrstedt, Klara (2013): Identity, location, disease and more: inferring your secrets from android public resources. In: Proceedings of the 2013 ACM SIGSAC CCS '13. ACM, New York, NY, USA, S. 1017-1028.
[101] Ghiglieri, Marco / Oswald, Florian / Tews, Erik (2013): HbbTV - I Know What You Are Watching. In: 13. Deutschen IT-Sicherheitskongresses, SecuMedia Verlags-GmbH, May 2013, abrufbar unter: http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html#comment-form (29.07.2014).
[102] Mitnick, Kevin D. (2003): Die Kunst der Täuschung, mitp-Verlag.
[103] Weidman, Georgia (2011): Transparent Botnet Control for Smartphones over SMS, abrufbar unter: http://www.undernews.fr/wp-content/uploads/2011/05/Shmoocon2011_SmartphoneBotnets_GeorgiaW.pdf (29.07.2014).
[104] Gellman, Barton / Soltani, Ashkan (2013): NSA tracking cellphone locations worldwide, Snowden documents show. In: The Washington Post, erschienen am: 04.12.2014, abrufbar unter: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (29.07.2014).
[105] Body of European Regulators for Electronic Communications (2012): A view of traffic management and other practices resulting in restrictions to the open Internet in

Europe, 29 May 2012, abrufbar unter: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf (29.07.2014).
[106] Mayer, Jane (2013): What's the matter with metadata. In: The New Yorker, abrufbar unter: http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html; Biermann, Kai (2011): Was Vorratsdaten über uns verraten. In: ZEIT ONLINE, 24.01.2011, abrufbar unter: http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz (29.07.2014).
[107] http://www.heise.de/newsticker/meldung/NSA-Abhoerskandal-PRISM-Internet-Austauschknoten-als-Abhoerziele-1909604.html; Meister, Andre (2013): Glasfaserkabel und Spionage-U-Boote: Wie die NSA die Nervenzentren der Internet-Kommunikation anzapft. In: Netzpolitik.org, erschienen am: 20.06.2013, abrufbar unter: https://netzpolitik.org/2013/glasfaserkabel-und-spionage-u-boote-wie-die-nsa-die-nervenzentren-der-internet-kommunikation-anzapft/ (29.07.2014).
[108] Vgl. Bitkom - https://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf (29.07.2014).
[109] Herfert, Michael et al. (2012): On the Security of Cloud Storage Services. Technical report SIT-TR-2012-001, abrufbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf (29.07.2014); The Notorious Nine: Cloud Computing Top Threats in 2013. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/ (29.07.2014).
[110] Vgl. http://www.gnupg.org/ (29.07.2014).
[111] Schmidt, Jürgen (2014): Kommentar: Truecrypt ist unsicher – und jetzt? In: heise online, erschienen am: 30.05.2014, abrufbar unter: http://www.heise.de/security/artikel/Truecrypt-ist-unsicher-und-jetzt-2211475.html (29.07.2014).
[112] Vgl. Bitlocker: http://windows.microsoft.com/en-us/windows7/products/features/bitlocker (29.07.2014).
[113] Schmidt, Jürgen (2013): iPhone-Verschlüsselung durchleuchtet. In: heise online, erschienen am: 17.12.2013, abrufbar unter: http://www.heise.de/security/artikel/iOS-Verschluesselung-durchleuchtet-2066500.html (29.07.2014).
[114] Vgl. https://play.google.com/store/apps/details?id=com.sovworks.edslite (29.07.2014).
[115] Vgl. https://play.google.com/store/apps/details?id=csh.cryptonite (29.07.2014).
[116] Vgl. http://www.mobilesitter.de/index_de.php (29.07.2014).
[117] Mylonas, Alexios / Tsalis, Nikolaos / Gritzalis, Dimitris (2013): Evaluating the Manageability of Web Browsers Controls. In: Accorsi, Rafael / Ranise, Silvio (Hrsg.); Security and Trust Management, STM 2013, S. 82-98, abrufbar unter: http://link.springer.com/chapter/10.1007%2F978-3-642-41098-7_6 (29.07.2014).
[118] Vgl. https://disconnect.me/ (29.07.2014).
[119] Vgl. http://www.abine.com/index.html (29.07.2014).
[120] Vgl. https://www.ghostery.com/de/ (29.07.2014).
[121] Fraunhofer Tracking Protection List. vgl.: https://www.sit.fraunhofer.de/de/angebote/projekte/tracking-protection-list/ (29.07.2014).
[122] Vgl. http://heartbleed.com/ (29.07.2014).
[123] Vgl. https://www.getcloak.com/ (29.07.2014).
[124] Vgl. Electronic Frontier Foundation (EFF). https://www.eff.org/https-everywhere (29.07.2014).
[125] The GNU Privacy Guard. http://www.gnu.org/software/gnupg/gnupg.html (29.07.2014).
[126] Vgl. https://threema.ch/de/ (29.07.2014).
[127] Vgl. https://whispersystems.org/ (29.07.2014).

[128] Vgl. https://jitsi.org/ (29.07.2014).
[129] Vgl. http://tox.im/en (29.07.2014).
[130] Auf die besondere Wichtigkeit des Schutzes der Endgeräte weist nicht zuletzt auch Edward Snowden hin: „[P]roperly implemented strong encryption works. What you have to worry about are the endpoints. If someone can steal you [sic!] keys (or the pre-encryption plaintext), no amount of cryptography will protect you. However, that doesn't mean end-to-end crypto is a lost cause. By combining robust endpoint security with transport security, people can have much greater confidence in their day to day communications." Snowden, Edward (2014): Live Q&A with Edward Snowden. In: Free Snowden, In Support of Edward Snowden, The Courage Foundation, abrufbar unter: http://freesnowden.is/asksnowden.html#midwire-how-quickly-can-the-nsa-et-al-decrypt-aes-messages-with-strong-keys-asksnowden-does-encrypting-our-emails-even-work (28.02.2014).
[131] Wirth, Stephan (2013): Praxislösungen zum sicheren Versand von E-Mails. In: Helmke, Stefan / Uebel, Matthias (Hrsg.): Management orientiertes IT-Controlling und IT-Governance, Springer Fachmedien Wiesbaden, S. 227–236, abrufbar unter: http://www.springerlink.com/index/10.1007/978-3-8349-7055-8_15 (29.07.2014).
[132] Bleich, Holger (2013): Vertrauenswürdige Kommunikation. In: c't Security 2013, S. 150-153.
[133] Siehe u.a.: Callas, J.; Donnerhacke, L.; Finney, H.; Shaw, D.; R. Thayer (2007): OpenPGP Message Format, RFC 4880, November 2007; siehe ebenfalls: http://www.openpgp.org/ (29.07.2014).
[134] Vgl. Bleich 2013.
[135] Paar, Christof / Pelzl, Jan (2010): Understanding Cryptography. Berlin, Heidelberg: Springer, S. 149-172 und S. 331-358.
[136] Schwenk, Jörg (2010): Sicherheit und Kryptographie im Internet: von sicherer E-Mail bis zu IP-Verschlüsselung, Wiesbaden: Vieweg + Teubner, S. 29-82.
[137]Vgl. http://www.heise.de/security/dienste/Keyserver-474468.html (29.07.2014).
[138] Weltweit gibt es zwar eine Vielzahl an Schlüsselservern, doch diese synchronisieren sich wechselseitig, was die Benutzung sehr erleichtert. Weiterführende Informationen auf: http://www.gnupg.org/gph/de/manual/x569.html (29.07.2014).
[139] Vgl. Bleich 2013: 151.
[140] Vgl. Schwenk 2010, S. 40.
[141] Bleich, Holger / Neuhaus, Sven (2013): Mail-Verschlüsselung auf dem Rechner und mobil. In: c't Security 2013, S. 154-157. Auch Online: http://www.heise.de/ct/artikel/Brief-mit-Siegel-1911842.html (02.04.2014).
[142] Aufsehenerregend war ein Angriff auf die niederländische Zertifizierungsstelle DigiNotar, bei der die Angreifer mehr als 500 Zertifikate für gefälschte Seiten, darunter Google-Mail und die CIA-Homepage, erfolgreich erstellen und über längere Zeit auf den gefälschten Seiten verwenden konnten. Vgl.: Thomsen, Sven (2012): Verschlüsselung – Nutzen und Hindernisse in der Praxis. In: Schmidt, Jan-Hinrik / Weichert, Thilo (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung Schriftenreihe Band 1190, Bonn, S. 381-389.
[143] Beispielhafte Preisübersicht bei GlobalSign: https://www.globalsign.com/de-de/personalsign/vergleichen.html (29.07.2014).
[145] Beuth, Patrick (2014a): WhatsApp-Gründer verspricht mehr, als er hält. In: Zeit Online, erschienen am: 18.03.2014, abrufbar unter: http://www.zeit.de/digital/mobil/2014-03/whatsapp-nutzerdaten-weitergabe-facebook/komplettansicht (29.07.2014).
[146] Im Feburar 2014 konnte Threema innerhalb weniger Tage seine Nutzerzahlen von 200.000 auf 400.000 Nutzer verdoppeln. Vgl.: Tanriverdi, Hakan (2014): Whatsapp-Konkurrent Threema verdoppelt Nutzerzahl. In: Süddeutsche.de, erschienen am: 21.02.2014, abrufbar unter: http://www.sueddeutsche.de/digital/seit-facebook-deal-whatsapp-konkurrent-threema-verdoppelt-nutzerzahl-1.1894768 (29.07.2014).

[147] Böck, Hanno (2014): Snowden empfiehlt TextSecure and Redphone. In: www.golem.de, erschienen am: 11.03.2014, abrufbar unter: http://www.golem.de/news/verschluesselung-snowden-empfiehlt-textsecure-und-redphone-1403-105052.html (29.07.2014).
[148] Auch in Deutschland müssen Komunikationsdiensteanbieter Strafermittlungsbehörden die Möglichkeit geben auf Meta- und Inhaltsdaten zugreifen zu können, falls diese über einen richterlichen Beschluss zur Überwachung verfügen (vgl. § 100a der Strafprozessordnung). Bei Diensten mit mehr als 9.999 Nutzern muss dafür eine sogenannte SINA-Box auf Kosten des Anbieters eingerichtet werden. Die durch eine Überwachungsanforderung betroffenen E-Mails werden dann über das VPN der SINA-Box an die entsprechenden Behörden weitergeleitet. Vgl. Ermert, Monika (2006): Lauschverhalten unter der Lupe. In: c't 1/06, abrufbar unter: http://www.heise.de/ct/artikel/Lauschverhalten-unter-der-Lupe-290250.html (29.07.2014). Es konnte abschließend allerdings nicht geklärt werden, inwieweit ein *Zero Knowledge Provider*, der aufgrund des fehlenden Zugriffs auf private Schlüssel keinen Zugang zu den Inhaltsdaten seiner Kunden hat, einer solchen Verpflichtung nachkommen soll und ob er somit vielleicht sogar gegen geltendes US-amerikanisches, schweizerisches oder deutsches Recht verstößt.
[149] Wood, Molly (2014): Privacy Please: Tools to Shield Your Smartphone. In: The New York Times, erschienen am: 19.02.2014, abrufbar unter: http://www.nytimes.com/2014/02/20/technology/personaltech/privacy-please-tools-to-shield-your-smartphone-from-snoopers.html?_r=1 (29.07.2014).
[150] Beuth, Patrick (2014b): App Weg von WhatsApp – aber wohin? In: Zeit Online, erschienen am: 20.02.2014, abrufbar unter: http://www.zeit.de/digital/mobil/2014-02/threema-telegram-surespot-chatsecure-vergleich (29.07.2014).
[151] Da eine fertige und als sicher anerkannte Open-Source Kryptografie-Lösung (NaCl Cryptography Library) eingesetzt wird, ist von einer sicheren Verschlüsselungsmethode auszugehen. Vgl.: Dimitrov, Hristo et al. (2013): Threema security assessment, Research project for Security of Systems and Networks, Master Thesis in System and Network Engineering, abrufbar unter.: https://www.os3.nl/_media/2013-2014/courses/ssn/projects/threema_report.pdf (29.07.2014); Beuth, Patrick (2013): Eine App, um die NSA zu ärgern. In: Zeit Online, erschienen am: 14.08.2013, abrufbar unter: http://www.zeit.de/digital/mobil/2013-07/threema-app-manuel-kasper/komplettansicht (29.07.2014).
[152] Diese fehlende Transparenz und Überprüfbarkeit ist Grund für vielfältige Kritik. Allerdings gibt der Threema-Entwickler zu bedenken, dass nur so das IT-Produkt Threema kommerziell nutzbar sei.
[153] Da die AGB oder auch Datenschutzerklärung eines Unternehmens jedoch geltendem Recht (hier bspw. BÜPF und VÜPF) unterliegt, kann hier nicht abschließend geklärt werden, inwieweit Rechtsverbindlichkeit gegenüber der Threema GmbH bei der Zusicherung, keinen Zugriff auf Inhaltsdaten zu haben, herrscht. Generell wäre hier die Frage zu prüfen, ob sogenannte Zero Knowledge Provider mit geltendem Recht vereinbar sind. Einen interessanten Vergleichsfall stellt hier der nach einem juristischen Streit mit US-Sicherheitsbehörden eingestellte US-Dienst Lavabit dar.
[154] Free and Open Source Software (FOSS).
[155] Fuest, Benedikt (2014): „Heartbleed"-Programmierer spricht von Versehen. In: Die Welt Online, erschienen am: 11.04.2014, abrufbar unter: http://www.welt.de/wirtschaft/webwelt/article126814584/Heartbleed-Programmierer-spricht-von-Versehen.html (29.07.2014).
[156] Er könne nicht garantieren, dass „es z.B. in iOS eine Hintertür gibt, über die Apple alle Tastatureingaben oder den Bildschirminhalt mitschneiden kann." Vgl. Beuth, 2013.
[157] WhatsApp ist das erste Jahr umsonst und kostet jedes darauffolgende Jahr 0,89 €. Vgl.: http://www.whatsapp.com/faq/de/general/23014681 (29.07.2014).

[158] „In the event that WhatsApp is acquired by or merged with a third party entity, we reserve the right to transfer or assign the information we have collected from our users as part of such merger, acquisition, sale, or other change of control." Vgl.: http://www.whatsapp.com/legal/ sowie http://www.huffingtonpost.com/mark-weinstein/whatsapp-with-whatsapp_b_4856338.html (beide 29.07.2014). Obwohl WhatsApp-Gründer Jan Koum immer bestritten hat, dass Nutzerdaten jenseits von Zwecken der Serviceverbesserung weiterverarbeitet und analysiert werden, scheint dies nun nicht mehr der Fall zu sein.
[159] „[Die] Threema GmbH als Betreiber der Threema-Server hat keine Möglichkeit, Nachrichten der Benutzer zu entschlüsseln, da sie keinerlei Kenntnis der privaten Schlüssel hat." Datenschutzerklärung der Threema GmbH. Vgl.: https://threema.ch/de/privacy.html (29.07.2014).
[160] „Unsere Server müssen natürlich wissen, wer wem eine Nachricht schickt, damit sie diese dem richtigen Empfänger zustellen können. Diese Information wird aber nicht geloggt […]." Häufige Fragen. Vgl.: https://threema.ch/de/faq.html (29.07.2014).
[161] Ähnlich wie Facebook finanziert sich auch Twitter durch Werbung, die allerdings in Form von eigenen Tweets und Accounts der Werbetreibenden dem Nutzer eingeblendet wird.
[162] Vgl.: http://support.whispersystems.org/customer/portal/questions/5836104-how-is-openwhispersystems-paying-for-the-its-server-costs- (29.07.2014).
[163] Vgl.: https://github.com/WhisperSystems/TextSecure/issues/819 (29.07.2014).
[164] Warnke, Martin (2011): Theorien des Internet zur Einführung. Hamburg, Junius Verlag.
[165] „Anonymitätstest" unter Menüpunkt „IP-Check" auf: http://ip-check.info/?lang=de (28.04.2014)
[166] Vgl. z.B. Biermann, Kai (2011): Was Vorratsdaten über uns verraten. In: Zeit Online, erschienen am 24.02.2011, abrufbar unter: http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz/komplettansicht (30.07.2014)
[167] Endres, Johannes (2013): Dienste und Software zum Verbergen der IP-Adresse. In: c't Security 2013, S. 120-122.
[168] Vorteile von JonDonym. In: JonDonym: JonDonym im Vergleich. abrufbar unter: https://www.anonym-surfen.de/vorteile.html (29.04.2014)
[169] Ball, James; Schneier, Bruce; Greenwald, Glenn (2013): NSA and GCHQ target Tor network that protects anonymity ob web users. In: the guardian, erschienen am: 04.10.2013, 15:50, abrufbar unter: http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (21.03.2014).
[170] „Sieht man sich die Ratschläge der Tor-Entwickler zur sicheren Nutzung ihres Dienstes an, wird klar, wohin die Reise geht. […] Also nix mit ‚noch n bisschen rumsurfen, spielen und Spaß haben' – ohne Helm, Gasmaske und kugelsichere Weste hat man im Tor-Netz nichts zu suchen." In: Schmidt, Jürgen (2013): Eigen-Tor: Gefahren der Tor-Nutzung im Alltag. c't, 20.
[171] Johnson, Aaron et al (2013): Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries, ACM Press, S. 337–348; Wang, Tao / Goldberg, Ian (2013): Improved Website Fingerprinting on Tor. ACM Press, S. 201–212; Hoffman, Chris (2013): HTG Explains: Is Tor Really Anonymous and Secure? In: How-To-Geek, erschienen am: 04.02.2013, abrufbar unter: http://www.howtogeek.com/142380/htg-explains-is-tor-really-anonymous-and-secure/ (03.04.2014); Perry, Mike (2013): A Critique of Website Traffic Fingerprinting Attacks. In: Tor, abrufbar unter: https://blog.torproject.org/blog/critique-website-traffic-fingerprinting-attacks (04.04.2014).

Zudem sind weder Tor noch JonDonym in der Lage VoIP und P2P-Filesharing sicher zu anonymisieren. Aus Gründen des Spamschutzes wird außerdem der SMTP-Port 25 blockiert Vgl. Vorteile von JonDonym.

[172] Vgl. https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous (17.11.2014).

[173] Vgl. https://www.torproject.org/projects/torbrowser.html.en (29.07.2014).

[174] Vgl. https://www.torproject.org/docs/android.html.en (29.07.2014).

[175] Vgl. Endres, 2013; Kasanmascheff, Markus (2013): Anonym Surfen: Tor, JonDo, VPN und Web-Proxies im Vergleich. In: softonic erschienen am 31.07.2013, abrufbar unter: http://artikel.softonic.de/anonym-surfen-tor-jondo-vpn-und-web-proxies-im-vergleich (03.04.2014).

[176] Moody, Famiglietti & Andronico (2013): The Tor Project, Inc. And Affiliate, Consolidated Financial Statements and reports required for audits in accordance with government auditing standards and omb circular A-133. December 31, 2012 and 2011, S. 11. abrufbar unter: https://www.torproject.org/about/findoc/2012-TorProject-FinancialStatements.pdf (20.03.2014).

[177] Zu den aufgezählten spendenden Unternehmen in 2011 gehörten u.a. Google, die Knight Foundation und the Swedish International Development Cooperative Agency. Auf weitere Spender wird im Annual Report zwar hingewiesen, doch keine weiteren Namen angegeben und auch eine genauere Auflistung der Spendenhöhen erfolgt nicht. Vgl. The Tor Project (2013): Tor Annual Report 2012, S. 6, abrufbar unter: https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf (20.03.2014).

[178] Vgl. Krempl, 2013.

[179] Arma (2012): Trip report, October FBI conference. In: Tor Blog, erschienen am 16.12.2012, abrufbar unter: https://blog.torproject.org/blog/trip-report-october-fbi-conference (29.04.2014).

[180] JonDonym (2010): Der Weg zum Mix Betreiber. In: JonDonym Wiki, abrufbar unter: https://anonymous-proxy-servers.net/wiki/index.php/Der_Weg_zum_Mix_Betreiber#JonDonym_Certification_Authority (30.04.2014).

[181] Die kostenfreie Variante ist dagegen auf zwei Zwischenstationen und eine Übertragungsgeschwindigkeit von 50 kBit/s beschränkt. Vgl.: JonDonym: Auswahl des Premium Tarifs. In: JonDonym. abrufbar unter: https://shop.anonymous-proxy-servers.net/bin/payment?lang=de (30.04.2014).

[182] Cane (2014): Post subject: Re: geringe Nutzerzahl für die kostenpflichtigen Kaskaden. In: JonDonym forum, Beitrag vom 11.02.2014 um 18:34 Uhr, abrufbar unter: https://anonymous-proxy-servers.net/forum/viewtopic.php?f=6&t=8230 (30.04.2014).

[183] „JonDonym und Strafverfolgung". In: JonDonym, abrufbar unter: https://www.anonym-surfen.de/strafverfolgung.html (03.04.2014).

Abkürzungen

AGB	Allgemeine Geschäftsbedingungen
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BVDW	Bundesverband Digitale Wirtschaft
CA	Certificate Authority
CALEA	Communications Assistance for Law Enforcement Act
DIVSI	Deutsches Institut für Vertrauen und Sicherheit im Internet
DPI	Deep Packet Inspection
EUGH	Europäischer Gerichtshof
GnuPG	GNU Privacy Guard
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISP	Internet Service Provider
NSA	National Security Agency
PGP	Pretty Good Privacy
SINA	Sichere Inter-Netzwerk Architektur
S/MIME	Secure / Multipurpose Internet Mail Extensions
SNS	Social Network Sites
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKÜV	Telekommunikationsüberwachungsverordnung
TLS	Transport Layer Security
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
VPN	virtuelles privates Netzwerk
WoT	Web of Trust

IMPRESSUM

Kontakt:
Peter Zoche
Koordinator Sicherheitsforschung und
Technikfolgenabschätzung
Telefon +49 721 6809-152
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und
Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes
Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

2. Auflage: 500 Stück
November 2014

Druck
Stober GmbH Druck und Verlag, Eggenstein

Dieses Werk ist lizensiert unter einer Creative
Commons Namensnennung – Nicht kommerziell
– Keine Bearbeitungen 4.0 International Lizenz.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

WWW.FORUM-PRIVATHEIT.DE

View publication stats