Barbara Wiesner

# PRIVATE DATEN

## Unsere Spuren in der digitalen Welt

[transcript] Digitale Gesellschaft

Barbara Wiesner
Private Daten

**Digitale Gesellschaft** | Band 35

**Barbara Wiesner** war Professorin für Datensicherheitstechnik im Fachbereich Informatik an der Technischen Hochschule Brandenburg.

Barbara Wiesner

# Private Daten

Unsere Spuren in der digitalen Welt

[transcript]

Diese Publikation wurde im Rahmen des Fördervorhabens 16TOA002 mit Mitteln des Bundesministerium für Bildung und Forschung im Open Access bereitgestellt.

**Bibliografische Information der Deutschen Nationalbibliothek**
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.




**Erschienen 2021 im transcript Verlag, Bielefeld**


Umschlaggestaltung: Maria Arndt, Bielefeld, nach einer Idee von Christof Isopp
Umschlagabbildung: Christof Isopp
Korrektorat: Marina Lukin
Druck: Majuskel Medienproduktion GmbH, Wetzlar
Print-ISBN 978-3-8376-5605-3
PDF-ISBN 978-3-8394-5605-7
EPUB-ISBN 978-3-7328-5605-3
https://doi.org/10.14361/9783839456057
Buchreihen-ISSN: 2702-8852
Buchreihen-eISSN: 2702-8860

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.
Besuchen Sie uns im Internet: *https://www.transcript-verlag.de*
Unsere aktuelle Vorschau finden Sie unter *www.transcript-verlag.de/vorschau-download*

# Inhalt

# Einleitung

## Zum Inhalt des Buches

»Zitate sind verdichtete Informationen.«[1]

Zitate sind bekanntermaßen kurz, einprägsam und aussagekräftig. Sie dienen in diesem Buch als Motto, d.h. als knappe Leitgedanken, die den einzelnen Kapiteln vorangestellt werden. Darüber hinaus dienen sie dazu, die Aufmerksamkeit des Lesers auf bestimmte Aspekte zu lenken und ihm dadurch die komplexe Thematik des Buches verständlich zu machen.

Wenn im Folgenden von Privatheit die Rede ist, so ist damit *informationelle Privatheit* gemeint, d.h. der Anspruch auf den Schutz von persönlichen Daten, die man nicht in den falschen Händen sehen will.[2]

Privatheit ist ein Thema, das heute jeden betrifft. Jeder von uns hinterlässt Datenspuren; diese werden gesammelt, analysiert und für die unterschiedlichsten Zwecke verwendet. Dabei werden ständig neue Geräte, Anwendungen usw. entwickelt, die immer mehr und immer detailliertere Daten erzeugen. Gleichzeitig werden die Methoden zur Analyse der Daten immer leistungsfähiger. Das führt zu einem spannenden Prozess: Auf der einen Seite stehen diejenigen, die diese Daten für ihre Zwecke einsetzen, deren Geschäftsmodell auf diesen Datensammlungen basiert. Auf der anderen Seite befindet sich der Nutzer, dem ständig technische Neuerungen mit größerem Komfort

1 Eigenes Zitat der Autorin.

2 Vgl. Rössler 2001, S. 25.

angeboten werden – natürlich um den Preis der Weitergabe von noch mehr Daten – und der zugleich sein Bedürfnis nach einer Privatsphäre nicht vergessen sollte, um nicht völlig gläsern und manipulierbar zu sein. Das vorliegende Bändchen will diese Diskrepanz aufzeigen, sodass sie für jeden Einzelnen sichtbar und nachvollziehbar wird. Es nimmt den Leser auf eine Reise durch verschiedene Aspekte von Privatheit mit. Es zeigt Vorteile, die eine geschützte Privatheit bietet, und verdeutlicht, was ihr Verlust bedeuten kann. Privatheit erweist sich als ein bedrohtes und doch schützenswertes Gut.

## Zum Aufbau des Buches

Ausgehend von der Frage, wie das Konzept einer schützenswerten Privatheit entstand (»Privatheit gestern und heute«), wird in den folgenden zwei Kapiteln (»Unsere Daten: Status quo«, »Unsere Daten: Pro und Contra«) die gegenwärtige Situation untersucht und nach dem Wert und Nutzen unserer Datenspuren gefragt.

Welche Datenspuren wir hinterlassen und welche Gefahren für uns und das Gemeinwesen davon ausgehen (»Unsere Daten: Was verraten sie über uns?«), welche Möglichkeiten Technologien wie Verschlüsselung bieten (»Schutz der Privatsphäre durch Verschlüsselung und Anonymisierung«), diskutieren die daran anschließenden Kapitel, bevor die soziale Dimension von Privatheit und ihre Bedrohung durch die Datensammelwut von Firmen und Staatsorganen (»Die gesellschaftliche Dimension von Privatheit«) erörtert wird.

Das letzte Kapitel (»Freiheit versus Sicherheit«) widmet sich dem Spannungsverhältnis zwischen Privatheit und Sicherheit.

Die einzelnen Kapitel sind weitgehend unabhängig voneinander. Dem Leser steht es somit frei, mit welchem Kapitel er die Lektüre dieses Buches beginnen möchte. Er kann auch erstmal den Text durchblättern und nur die Zitate lesen. Damit bekommt er einen ersten Einblick in die Thematik des Buches.

# Privatheit gestern und heute

Es gibt einige wichtige Meilensteine bei der Entwicklung von Privatheit. Der erste ist der berühmte Aufsatz »The Right to Privacy« von Warren und Brandeis in einer amerikanischen juristischen Zeitschrift, der dann letztendlich zu entsprechenden Gesetzesänderungen in den USA geführt hat. Des Weiteren gibt es zwei bahnbrechende Urteile des deutschen Bundesverfassungsgerichtes (BVerfG) zu diesem Thema. Diese Urteile haben das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und das Recht auf informationelle Selbstbestimmung eingeführt. Heute ist das Recht auf Schutz der Privatsphäre vor allem in den nationalen Datenschutzgesetzen verankert bzw. in der Datenschutzgrundverordnung, die seit dem 25. Mai 2018 anzuwenden ist.

## Recht auf Privatheit

> »Das Recht auf Privatheit – das Recht in Ruhe gelassen zu werden.«[1]

Das Recht auf Privatheit wurde 1890 erstmals von Samuel D. Warren, einem amerikanischen Rechtsanwalt, und Louis D. Brandeis, ebenfalls ein amerikanischer Rechtsanwalt und später Richter am Supreme

1 »The right to privacy – the right to be let alone.« (Warren/Brandeis 1890).

Court, eingeführt. In ihrem berühmten Aufsatz *The Right to Privacy*[2] sprechen sie von »*the right to be let alone*«, dem Recht, in Ruhe gelassen zu werden.

Es wurde viel spekuliert, was Warren und Brandeis veranlasst haben könnte, diesen Artikel zu schreiben. Nach Rössler war Warrens Ärger über Presseberichte, die von der Hochzeit seiner Tochter private Details öffentlich gemacht hatten, der Anlass für den Artikel in der Harvard Law Review.[3]

Ein großes Ärgernis insbesondere für Warren dürften zudem Zeitungsberichte gewesen sein, die persönliche Details über die Partys seiner Frau enthielten.[4]

Tatsächlich erschienen zwischen 1882 und 1890 an die 60 Zeitungsartikel mit Klatsch und Tratsch über Warrens Familie, davon allein zwei Titelgeschichten über die Beerdigungen seiner Schwiegermutter und Warrens Schwägerin, die Schwester seiner Frau.[5]

Das besondere Interesse der Presse an Warren und seiner Familie erklärt sich aus der Tatsache, dass seine Frau die Tochter von Thomas F. Bayard war, eines amerikanischen Senators von Delaware und ehemaligen Präsidentschaftskandidaten. Die Presse interessierte sich vor allem deswegen für sie, weil sie aus einer politisch bedeutsamen Familie stammte und somit im Rampenlicht der Öffentlichkeit stand.[6]

Ermöglicht wurde diese ausführliche Berichterstattung durch die am Ende des 19. Jahrhunderts beginnende enorme Verbreitung der Klatschpresse, die zudem durch die neuesten Entwicklungen auf dem Gebiet der Fotografie über die Möglichkeit verfügte, Schnappschüsse zu erstellen.[7]

---

2 Ebd.

3 Vgl. Rössler 2001, S. 20; Prosser 1960.

4 Vgl. Gajda 2008; Prosser 1960.

5 Vgl. Lepore 2013.

6 Vgl. Gajda 2008.

7 »Es waren die Kameras der Marke Kodak und deren Rollfilme, durch die Schnappschüsse möglich wurden.« Geschichte der Fotografie 2017. Vgl. dazu auch Rössler 2001, S. 13.

Mit dem Artikel von Warren und Brandeis wird das Thema ›Privatheit‹ erstmals Gegenstand einer juristischen Abhandlung. Sie fordern, dass jeder das Recht haben soll zu entscheiden, was über ihn in der Öffentlichkeit berichtet wird.

Anwendung fanden die Überlegungen der Autoren mehr als 30 Jahre später, während der Prohibition (Alkoholverbot), bei einem Verfahren gegen den Alkoholdealer Roy Olmstead, dessen Telefonleitungen angezapft wurden, ohne dass eine richterliche Genehmigung vorlag.[8] Aus diesem Gerichtsverfahren stammt der bekannte Satz, dass vor Gericht offengelegt wird, was im Geheimen geflüstert wird.[9] Genau gegen solche Vorgehensweisen wenden sich die Autoren Warren und Brandeis.

> »Das Recht, in Ruhe gelassen zu werden [ist] das umfassendste aller Rechte und dasjenige, dem ein freies Volk den größten Wert beimisst.«[10]

Diese berühmte Formulierung ist enthalten in der Stellungnahme von Brandeis zu diesem Verfahren.

Der Jurist Louis Brandeis konnte sich damals mit seiner Auffassung, dass das heimliche Anzapfen von Telefonleitungen gegen den 4. oder 5. Verfassungszusatz (Fourth or Fifth Amendment) der amerikanischen Verfassung verstoße und damit die durch die Zusätze garantierten Rechte (Fourth and Fifth Amendment rights) verletze, nicht durchsetzen. Wäre man seiner Argumentation gefolgt, dann hätte Olmstead auf der Grundlage der Informationen, die aus dem heimlichen Anzapfen von Telefonleitungen gewonnen wurden, nicht verurteilt werden können. Fünf der neun Richter vertraten jedoch

8 Olmstead v. United States 1928.

9 »[…] to obtain disclosure in court of what is whispered in the closet.« Olmstead v. United States 1928.

10 »The right to be let alone – the most comprehensive of rights, and the most valued by civilized men.« Olmstead v. United States 1928.

die Auffassung, dass das heimliche Anzapfen der Leitungen zwar unethisch, aber als Beweismittel zulässig sei, da es nicht gegen das Fourth or Fifth Amendment der amerikanischen Verfassung verstoße.[11] Damit konnte Olmstead auf Grund der Informationen aus den angezapften Leitungen verurteilt werden. Er verbrachte vier Jahre im Gefängnis. 1935 wurde er von Präsident Roosevelt begnadigt.[12]

Ungefähr zehn Jahre später vermied der Oberste Gerichtshof verfassungsrechtliche Fragen und nahm den Federal Communications Act als Grundlage, um Abhörmaßnahmen ohne richterliche Genehmigung als illegal festzulegen.[13]

In späteren Regelungen verbot der Gerichtshof den Einsatz jeglicher Art von Überwachungsmaßnahmen ohne richterliche Genehmigung.[14]

Eine späte Auswirkung des Rechts auf Privatheit findet sich in dem berühmten Urteil *Roe v. Wade* von 1973. Darin wurde festgelegt, dass das Recht auf Privatheit impliziert, dass Frauen über eine Abtreibung selber entscheiden dürfen. Damit wurde die Kriminalisierung der Abtreibung als verfassungswidrig eingestuft.[15] Gerade dieses Recht auf Abtreibung droht nach dem Tod von Ruth Bader Ginsburg, Richterin am Obersten Gerichtshof der Vereinigten Staaten, gekippt zu werden.[16]

## Recht auf informationelle Selbstbestimmung

Dieses Recht basiert auf einer Entscheidung des deutschen Bundesverfassungsgerichtes von 1983. In dieser Entscheidung wird das Recht auf informationelle Selbstbestimmung wie folgt definiert:

11 Vgl. Olmstead v. United States 1928.

12 Vgl. Olmstead v. United States 2020.

13 Vgl. Nardone v. United States 1937.

14 Vgl. Whitfield/Landau 2007, S. 150.

15 Vgl. Roe v. Wade 1973.

16 Vgl. Steffens 2020.

> »Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art. 2 Abs. 1 in Verbindung mit GG Art. 1 Abs. 1 umfasst. Das Grundrecht [auf informationelle Selbstbestimmung] gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.«[17]

Anlass für diese Entscheidung war die für 1983 geplante Volkszählung. Es sollten sämtliche Einwohner der Bundesrepublik Deutschland statistisch erfasst werden. Dagegen wurde Beschwerde beim Bundesverfassungsgericht (BVerfG) eingelegt.

> »Der Protest drehte sich um die Frage, ob die Volkszählung nicht doch die Grundlage für eine schrankenlose, durch die automatisierte Verarbeitung begünstigte Verknüpfung der unzähligen, von den verschiedensten staatlichen und privaten Stellen bereits gespeicherten Daten abgeben könnte […].«[18]

Mit dem sogenannten Volkszählungsurteil setzte das Bundesverfassungsgericht die Volkszählung zunächst aus, erlaubte sie dann aber, mit Einschränkungen bezüglich der Verwendung der erhobenen Daten. So wurde der Melderegisterabgleich verboten. Hingegen durften anonymisierte Daten zu wissenschaftlichen Zwecken weitergegeben werden.

17 BVerfG 1983.

18 Simitis 2003.

Wichtigstes Ergebnis dieses Volkszählungsurteils ist das Recht auf informationelle Selbstbestimmung, das hier zum ersten Mal Erwähnung findet. Es beinhaltet das Recht, dass jeder Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann.

## Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Mit Bezug auf das allgemeine Persönlichkeitsrecht hat das Bundesverfassungsgericht in seinem Urteil von 2008 die Vertraulichkeit und Integrität informationstechnischer Systeme als Grundrecht eingeführt. Die Infiltration informationstechnischer Systeme ist damit nur noch unter sehr restriktiven Bedingungen möglich.

> »Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.«[19]

Bei diesem Verfahren vor dem Bundesverfassungsgericht ging es um die sogenannte Online-Durchsuchung, d.h. die heimliche Infiltration eines informationstechnischen Systems. Diese Befugnis hatte der nordrhein-westfälische Verfassungsschutz durch das am 30. Dezember 2006 in Kraft getretene Änderungsgesetz zum nordrhein-westfälischen Verfassungsschutzgesetz erhalten.

Dagegen reichten eine Journalistin, ein Mitglied des Landesverbandes Nordrhein-Westfalen der Partei DIE LINKE und drei Rechtsanwälte Verfassungsklage ein. Diese Klage war erfolgreich.[20] Die heimliche Online-Durchsuchung war danach nur noch unter starken

19 BVerfG 2008.

20 Vgl. BVerfG Pressemitteilung 2008.

Einschränkungen zulässig. So ist sie grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.

Gleichzeitig hat das Bundesverfassungsgericht mit dieser Entscheidung ein neues Grundrecht eingeführt, nämlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Damit sind alle Daten, die den Kernbereich privater Lebensgestaltung enthalten, vor Zugriff und Manipulation zu schützen. Dies betrifft Daten auf Computern, im Internet, in Netzwerken, auf Mobiltelefonen und auf vergleichbaren Systemen.[21]

21 Vgl. BVerfG 2008.

# Unsere Daten: Status quo

## Die großen Konzerne sammeln unsere Daten

> »Unternehmen und nicht mehr die Staaten sind in den freien Demokratien der Welt die eigentliche Gefahr für den Datenschutz. Sie stellen die größte unmittelbare Herausforderung für den Datenschutz dar. (Michael Sandel)«[1]

Es sind vor allem unsere Daten, die in unvorstellbarem Umfang gesammelt und verwertet werden, die unsere Privatsphäre erodieren lassen. Gesammelt werden sie sowohl von den großen Konzernen als auch vom Staat.

### Die Global Player unter den Datensammlern

Will man mehr über diese Gefährdung wissen, muss man sich diese Unternehmen und deren Praktiken genauer ansehen. Exemplarisch seien hier Google, Apple, Facebook, Amazon und Microsoft herausgegriffen, fünf große Konzerne, die für ihre Datensammlungen berüchtigt sind.[2]

1 Bohsem 2016.

2 Für die Konzerne Google, Apple, Facebook, Amazon und Microsoft wird häufig das Akronym GAFAM verwendet.

## Google

> »Google ist zuallererst ein global agierender Werbekonzern. Kommerzielle Anzeigen sind das Business, mit dem Google seine Milliarden macht.«[3]

Die Datensammelwut von Google zeigt sehr schön das folgende Beispiel:

> »Französische Sicherheitsforscher des Unternehmens Eurecom haben 2000 Gratis-Apps für Android-Smartphones aus 25 verschiedenen Kategorien im Google Play Store geladen und auf einem Samsung-Smartphone ausgeführt. Der Netzwerkverkehr der Apps nach außen wurde abgefangen und analysiert. Demnach steuerten die Programme heimlich insgesamt 250 000 verschiedene Webadressen an und gaben Daten weiter.«[4]

Neuere Untersuchungen bestätigen diesen Trend. Die Datensammelwut nimmt stetig zu, wie nachstehendes Beispiel zeigt.

> »Forscher der Universität Oxford betrachteten fast eine Million Apps, die im ›Google Play Store‹ bereitgestellt sind. So gut wie alle haben Tracker eingebaut, die von amerikanischen Unternehmen sind. Siebenhunderttausend der Apps verbinden sich ausschließlich mit verschiedenen Profilbildungsfirmen in den Vereinigten Staaten. Mehr als hunderttausend Apps senden ihre Tracking-Daten zusätzlich in andere Länder, in denen Profilfirmen sitzen.«[5]

3 BigBrotherAward, 2013.

4 Spehr 2015.

5 Kurz 2018.

Larry Page, Sergey Brin und Eric Schmidt, Gründer und Verwaltungsrat der Google Inc., Mountain View, Kalifornien, USA, erhielten 2013 den BigBrotherAward in der Kategorie Globales Datensammeln.

> »Bei diesem Preisträger kritisieren wir nicht einen einzelnen Datenschutzverstoß. Wir prangern auch nicht einzelne Sätze in seinen Geschäftsbedingungen an. – Nein, der Konzern selbst, sein globales, allumfassendes Datensammeln, die Ausforschung der Nutzerinnen und Nutzer als Wesenskern seines Geschäftsmodells und sein de facto Monopol – das ist das Problem.«[6]

> »Google weiß, wer wir sind, wo wir gerade sind und was uns wichtig ist. Google weiß nicht nur, nach welchen Begriffen wir vorher gesucht haben, sondern auch, welche davon wir tatsächlich angeklickt haben. Google weiß minutiös, an welchem Tag wir zu welcher Zeit wach waren, für welche Personen, Nachrichten, Bücher wir uns interessiert haben, nach welchen Krankheiten wir recherchiert haben, welche Orte wir besucht haben, welche Videos wir uns angeschaut haben, welche Werbung uns angesprochen hat.«[7]

## Apple

Der Gewinn von Apple basiert nicht primär auf Werbung, sondern zunächst einmal auf dem Verkauf von Produkten. Doch sollte das nicht darüber hinwegtäuschen, dass Apple sich durchaus für die Daten seiner Kunden interessiert und diese auch in großem Stil sammelt.

Wenn man in irgendeiner Form Kontakt mit Apple aufnimmt, sei es, dass man eine Apple ID erstellt, einen Konsumentenkredit beantragt, ein Produkt kauft, oder ein Softwareupdate herunterlädt: Es werden stets alle anfallenden Daten gespeichert. Das sind beispiels-

6 BigBrotherAward, 2013.

7 Ebd.

weise Name, Adresse, Telefonnummer, E-Mail-Adresse, Informationen zur bevorzugten Kontaktaufnahme, Gerätekennungen, IP-Adressen, Standortinformationen, Kreditkarteninformationen und Profilinformationen, wenn der Kontakt über ein soziales Netzwerk erfolgt.[8]

Im Handy wird der Aufenthaltsort gespeichert mit Tages- und Uhrzeit, sofern man diese Option nicht abgeschaltet hat. Man kann also genau verfolgen, wo man sich wann aufgehalten hat.[9]

> »Siri [Sprachassistent von Apple] weiß noch nach zwei Jahren, was Nutzer den Sprachassistenten von Apple fragen. Denn so lange werden die Daten auf dem Server festgehalten.«[10]

Diese Daten werden nicht nur gespeichert.

> »Apple und seine verbundenen Unternehmen können diese personenbezogenen Daten untereinander austauschen. Sie können solche Daten auch mit anderen Informationen verbinden, um Produkte, Dienstleistungen, Inhalte und Werbung anzubieten oder zu verbessern.«[11]

Dass von diesen Möglichkeiten der Datenweitergabe reichlich Gebrauch gemacht wird, zeigt ein Experiment der *Washington Post*. Es deckt auf, dass 5.400 versteckte App Tracker unsere Daten verschlungen haben – in einer einzigen Woche. Apple verspricht Datenschutz, aber iPhone-Apps geben die Daten ihrer Nutzer an Tracker, Werbefirmen und Forschungsunternehmen weiter.[12]

---

8 Vgl. Apple Datenschutzrichtlinie, 2019.

9 Vgl. Giordano 2018.

10 Apple speichert Siri-Daten bis zu zwei Jahre, 2013.

11 Apple Datenschutzrichtlinie, 2019.

12 Vgl. Fowler 2019.

2011 erhielt die Apple GmbH in München den BigBrotherAward in der Sparte Kommunikation »für die Geiselnahme ihrer Kunden mittels teurer Hardware und darauffolgende Erpressung, den firmeneigenen zweifelhaften Datenschutzbedingungen zuzustimmen.«[13]

> »Apples Firmenstrategie scheint darauf ausgelegt zu sein, möglichst viele Nutzerdaten zu erfassen, ähnlich wie es soziale Netzwerke auch tun. Werbepartner freuen sich darauf, mit Hilfe von Apple möglichst zielgruppengerechte und standortbezogene Werbung auf dem Telefon anzeigen zu können.«[14]

> »Damit die Werbung optimal auf deine Bedürfnisse abgestimmt ist, bietet dir Apple Anzeigen im App Store und in Apple News auf der Basis von Informationen wie deinem Suchverlauf im App Store oder den gelesenen Artikeln in Apple News.«[15]

> »Seit Mittwoch [17.10.2019] bietet Apple an, sämtliche Daten einsehen, herunterladen und löschen zu können, die die i-Geräte bisher über den jeweiligen User gesammelt haben.«[16]

Wer dies einmal ausprobiert und sich die gesammelten Daten angeschaut hat, für den ist klar, dass die Aussage von Apple, dass Privatheit ein fundamentales Menschenrecht ist,[17] hier ad absurdum geführt wird. Bemerkenswert ist auch, dass ein Löschen nur über ein Löschen

13 Der BigBrotherAward 2011 in der Kategorie »Kommunikation« geht an die Apple GmbH, 2011.

14 Ebd.

15 Apple Interessenbezogene Werbung im App Store und in Apple News deaktivieren, 2020.

16 Giordano 2018.

17 Vgl. Apple Privacy, 2020.

des Accounts möglich ist. Erkennbar ist dies an den Möglichkeiten, die Apple anbietet, wenn man sich in seinen Account eingeloggt hat.[18]

## Facebook

Die Nutzung von Facebook ist für Anwender kostenlos. Sie bezahlen die Nutzung dieser Plattform mit ihren Daten.

Jemand hat einmal gesagt: »Facebook ist eine Content-Fabrik.«[19] Der Rohstoff, der hier verarbeitet wird, ist Content, d h. Inhalte, also letztlich Daten. Zu diesen datenbezogenen Inhalten zählt alles, was auf Facebook erfasst wird, dazu gehört jede Information, jeder Like, jeder Share, jedes Selfie, jede aufgerufene Seite, jeder einzelne Klick, einfach alles. Diese Daten werden akribisch erfasst und analysiert. Sie dienen letztlich dazu, die Nutzer dahingehend zu beeinflussen, dass kommerzielle oder politische Werbung erfolgreich platziert werden kann.[20]

Facebook gibt die Daten seiner Nutzer an Werbekunden weiter. Das Tool ›Audience Insights‹ ist nichts anderes als eine riesige Datenbank mit den Daten der Nutzer von Facebook mit entsprechenden Abfragemöglichkeiten.

Dieses Tool steht allen Nutzern von Facebook zur Verfügung die einen Account für Werbeanzeigen haben. Diese Nutzer können damit Zielgruppen definieren, z.B. alle schwangeren Frauen im Bundesstaat New York mit Hochschulabschluss. Diese Zielgruppe können sie dann genauer analysieren, etwa wie viele dieser Frauen Single sind, wie viele in einer Partnerschaft leben, wie viele einer höheren Einkommensschicht angehören usw. An diese Zielgruppe können sie dann über den Werbeanzeigen-Manager die entsprechende Werbung schicken.[21]

2011 erhielt die Facebook Deutschland GmbH den BigBrother-Award in der Kategorie Kommunikation »für die gezielte Ausfor-

18 Vgl. Apple Daten und Datenschutz, 2020.

19 Kaeser 2018.

20 Vgl. ebd.

21 Vgl. Küchemann 2014; Roth 2020.

schung von Menschen und ihrer persönlichen Beziehungen hinter der netten Fassade eines vorgeblichen Gratisangebots.«[22]

> »Die Fakten: Facebook sammelt alles an Daten, was sie bekommen können. Nicht nur Name, Adresse, Profilbild, Telefon, Handynummer, Fotos, Texte, Statusupdates, Aufenthaltsort, Nachrichten an Freunde, besuchte Webseiten und und und …«[23]

## Amazon

Auch Amazon speichert die Daten seiner Kunden. Bei jedem Kontakt mit Amazon, sei es, dass man nach einem Produkt sucht, auf der Webseite von Amazon eine Bestellung aufgibt, mit dem Sprachdienst von Amazon spricht oder mit Amazon per Mail oder Telefon oder anderweitig kommuniziert: Alle dabei anfallenden Daten werden gespeichert. Das können z.B. Name, Adresse, Telefonnummer, E-Mail-Adresse, Passwörter, Zahlungsinformationen, Alter, Standort, Personen, an die Einkäufe versendet wurden, E-Mail-Adressen von Freunden und anderen Personen, IP-Adresse, Logins, und vieles mehr sein. Will man bei Amazon ein Produkt kaufen, muss man ein Amazon-Konto eröffnen. E-Mail-Adresse, Name, Adresse und Telefonnummer werden erfasst. Wählt man *Zahlung auf Rechnung*, muss man das Geburtsdatum angeben. Will man per Kreditkarte bezahlen, wird diese dauerhaft abgespeichert.

Amazon kennt damit unsere emotionalen Vorlieben und unsere finanziellen Möglichkeiten. Amazon verfügt u.a. über exakte und umfangreiche Bonitätsdaten. All diese Daten werden unter anderem zur Einblendung zielgruppengenauer Werbung genutzt.[24]

---

22 Der BigBrotherAward 2011 in der Kategorie »Kommunikation« geht an die Facebook Deutschland GmbH, 2011.

23 Ebd.

24 Vgl. Amazon Datenschutzerklärung, 2019; Wer weiß was über die Nutzer: Die wirkliche Datenkrake heißt Amazon, 2011; Daten-Speicherung.de – minimum data, maximum privacy, o.J.

Amazon bietet seinen Kunden in den USA 10 Dollar dafür, dass sie eine Browser-Erweiterung installieren (Amazon Assistant for Chrome). Diese soll den Nutzern dabei helfen, Preise im Internet zu vergleichen. Erst im Kleingedruckten erfährt man, dass das Programm das komplette Surfverhalten des Nutzers auswertet.[25]

## Microsoft

Auch Microsoft sammelt die Daten seiner Kunden. Groß war die Aufregung nach der Einführung von Windows 10. Denn man stellte fest, dass dieses Betriebssystem umfangreiche System- und Nutzungsinformationen an Microsoft sendet. Verschiedene Datenschutzbehörden wurden aktiv.

So mahnte die französische Datenschutzbehörde CNIL Microsoft wegen Windows 10 ab. »Sie kritisiert vor allem eine ›übermäßige‹ Datensammlung ohne Einwilligung der Nutzer. Außerdem seien Anwenderdaten nicht ausreichend geschützt.«[26]

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) führte eine groß angelegte Studie zu Systemaufbau, Protokollierung, Härtung und der Sicherheitsfunktionen in Windows 10, kurz »SiSyPHuS Win10«, durch. Ein Teilergebnis dieser Untersuchung ist, dass zwar die Möglichkeit besteht, die Datenerfassung und -übermittlung vollständig zu deaktivieren. Das ist aber nur unter hohem Aufwand möglich und zwingt Nutzer dazu, bestimmte Dienste abzuschalten.[27]

Das niederländische Ministerium für Sicherheit und Justiz befasste sich damit, dass Microsoft Office noch mehr Telemetriedaten (das sind z.B. Daten über die individuelle Nutzung von Word, Excel, PowerPoint und Outlook) als Windows 10 sammelt. Es beauftragte die u.a. auf Datenschutz spezialisierte Firma Privacy Company mit einer

25 Vgl. Langer 2019.

26 Greif 2016.

27 Vgl. Matthes/Dachwitz 2018; Vgl. BSI untersucht Sicherheitseigenschaften von Windows 10, 2018.

Datenschutz-Folgenabschätzung für Microsoft Office. Die Ergebnisse zeigen u.a., dass personenbezogene Daten wie Metadaten und Inhalte illegal gespeichert werden, die im Falle von Behörden sogar geheimhaltungsbedürftiges Material betreffen können. Riskant ist darüber hinaus die Speicherung der Daten außerhalb der EU wegen des umstrittenen Privacy-Shield-Abkommens sowie die fehlende Kontrolle über die Art der übertragenen Daten und deren spätere Löschung.[28]

Mittlerweile befasst sich auch der Europäische Datenschutzbeauftragte mit Microsoft. Grund dafür ist, dass die EU-Institutionen sich bei ihren täglichen Aktivitäten auf Microsoft Dienste und Produkte verlassen. Dies schließt die Verarbeitung großer Mengen personenbezogener Daten ein. Es soll deshalb geprüft werden, ob die zwischen Microsoft und den EU-Institutionen geschlossenen vertraglichen Vereinbarungen in vollem Umfang mit den Datenschutzbestimmungen vereinbar sind.[29]

Inzwischen wurde bekannt, dass Microsoft die Office-Suite 365 um Funktionen erweitert (Stand 24.11.2020), mit denen Unternehmen die Arbeitsgepflogenheiten ihrer Belegschaft detailliert beobachten können. Bertold Brücher, Rechtsexperte beim DGB, hält einen rechtskonformen Einsatz für ausgeschlossen. Das Beispiel zeigt sehr deutlich, dass es bisher nicht gelungen ist, Microsoft hier Einhalt zu gebieten.[30]

2020 kommt eine Arbeitsgruppe der deutschen Datenschutzkonferenz zu dem Schluss, dass kein datenschutzgerechter Einsatz von Microsoft 365 möglich sei. Außerdem fordert sie dazu auf, das Problem der Abhängigkeit von Microsoft anzugehen. Immerhin verwenden 96 Prozent aller Behörden Produkte aus dem Microsoft-Office-Paket.[31]

Diese fünf hier aufgezählten Unternehmen Google, Apple, Facebook, Amazon und Microsoft stehen exemplarisch für die vielen an-

28 Vgl. Beiersmann 2018; Bordel 2018; Boehring 2018.

29 Vgl. Der Europäische Datenschutzbeauftragte, 2019.

30 Vgl. Schüler 2020.

31 Vgl. Ballweber 2020.

deren, die die Daten ihrer Kunden in ganz großem Stil sammeln. Die Liste dieser Unternehmen ließe sich beliebig fortsetzen.

## Der Staat sammelt unsere Daten

> »Wenn es zu einer Katastrophe kommt, besteht die Tendenz möglichst schnell zu reagieren, um die Dinge sofort zu beheben. (Susan Landau)«[32]

Diese oft sehr wenig durchdachten Reaktionen auf Katastrophen beinhalten in den meisten Fällen den Ruf nach noch mehr Daten. Zwar benötigt der Staat Daten seiner Bürger, um diese verwalten zu können, wie z.B. die Daten der Melderegister, Daten zur Rentenversicherung, Steuerdaten usw. Doch gerade im Zuge der Bedrohung durch Terror und Kriminalität verlangt der Staat den Zugriff auf immer weitere Daten.

Hierzu einige Beispiele:[33]

> »Die Attacken in Paris im November 2015 und in San Bernardino im Dezember 2015 haben die Forderung der Regierung nach weiterem Zugriff auf elektronische Kommunikation – Telefone, EMails und Browser Chronik – neu entfacht, um Terrorismus zu verhindern.«[34]

---

32 »Whenever there's a disaster, there's a tendency to do a knee-jerk reaction to fix things right away. (Susan Landau)« Sadeghi/Dessouki 2016.

33 Es sei hier angemerkt, dass bei einigen dieser Beispiele die sogenannte Vorratsdatenspeicherung erwähnt wird, auf die später noch genauer eingegangen wird.

34 »These recent attacks (attacks in Paris in November 2015 and in San Bernardino in December 2015) reignited calls for more government access to people's electronic communications-phones, emails and Internet browsing history – to prevent terrorism.« Jasen 2016.

»Nach den Terroranschlägen auf ›Charlie Hebdo‹ [07.01.2015] fordern Politiker und Behörden schon wieder die Vorratsdatenspeicherung.«[35]

»Innenpolitiker verschiedener Parteien, Vertreter des Bundesinnenministeriums und der Chef des Bundesamts für Verfassungsschutz fordern dieser Tage einen verbesserten Zugriff auf Daten aus sozialen Netzwerken. Sie berufen sich dabei auf den Amoklauf in München und auf terroristisch motivierte Straftaten in den letzten Wochen.«[36]

»[Am 30. Juli 2016] wird das Telekommunikationsgesetz abgeändert, so dass die Daten der Käufer der mehr als sechzehn Millionen SIM-Karten für Mobiltelefone, die in Deutschland pro Jahr ohne Vertrag verkauft werden, demnächst mit Identitätsdokumenten abgeglichen werden müssen. Die Informationen sind jeweils zu speichern und sicher zu verwahren, falls ein behördlicher ›Bedarfsträger‹ einen Blick darauf werfen möchte.«[37] Dies soll einer verbesserten Terrorismusbekämpfung dienen.

»Die Niederlande planen eine Verschärfung der Massenüberwachung von Internet und Kommunikation durch ihre Geheimdienste. […] Zukünftig soll es den Geheimdiensten erlaubt sein, jeglichen Internetverkehr abzuhören, Computer und Handys zu hacken und Rohdaten ungefiltert an befreundete Dienste weiterzugeben. […] Wie auch in Deutschland wird die nun angestrengte Reform mit der gestiegenen Gefahr von Cyberkriminalität und Terroranschlägen begründet.«[38]

35 Lobo 2015.

36 Schaar 2016.

37 Kurz 2016.

38 Rebiger 2016.

> »Nach den Ausschreitungen vor dem Reichstagsgebäude [im August 2020] will die CDU die Kompetenzen der Polizei erweitern – vor allem um die Vorratsdatenspeicherung.«[39]

Diese Vorratsdatenspeicherung – von Politikern immer wieder gefordert, von Bürgerrechtlern und Datenschutzexperten vehement bekämpft – beinhaltet, dass alle bei Telekommunikationsvorgängen anfallenden Verbindungsdaten vorsorglich aufbewahrt werden. Damit ist nachvollziehbar, wer mit wem per Telefon oder Handy in Verbindung gestanden oder das Internet genutzt hat. Man spricht hier auch von einer anlasslosen, d.h. ohne konkreten Verdacht erfolgenden Überwachung der gesamten Bevölkerung. Denn diese Verbindungsdaten sind weit aussagekräftiger als mancher sich das vorstellen mag. Sie sagen oft mehr über Menschen aus als die eigentlichen Inhalte der Kommunikation.[40]

Die Vorratsdatenspeicherung hat eine wechselvolle Geschichte. Immer wieder wurde sie eingeführt, um danach wieder aufgehoben zu werden.

Ihren Beginn hat sie mit der EU-Richtlinie zur Vorratsdatenspeicherung (2006/24/EG), die am 15. März 2006 in Kraft trat.

> »Mit ihr wurden die EU-Mitgliedstaaten verpflichtet, die Speicherung von Verkehrs- und Standortdaten sowie Daten zur Feststellung der Identität der jeweiligen Teilnehmer nach nationalem Recht sicherzustellen. Den Providern wurde auferlegt, die Verbindungsdaten nahezu aller Kommunikationsvorgänge für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten aufzubewahren.«[41]

---

39 CDU-Spitze fordert nach Corona-Demo mehr Befugnisse für Polizei, 2020.

40 Vgl. Vorratsdatenspeicherung: Alle Menschen unter Generalverdacht, o.J.

41 Ebd.

Die Vorratsdatenspeicherung wurde dann mit Urteil vom 2. März 2010 vom Bundesverfassungsgericht verboten. Mit Wirkung vom 18.12.2015 ist sie jedoch wieder in Kraft gesetzt worden.

> »[Danach] soll spätestens ab 1. Juli 2017 zehn Wochen lang nachvollziehbar sein, wer mit wem per Telefon oder Handy in Verbindung gestanden oder das Internet genutzt hat. Bei Handy-Telefonaten und SMS wird auch der jeweilige Standort des Benutzers festgehalten und vier Wochen lang gespeichert. In Verbindung mit anderen Daten wird auch die Internetnutzung nachvollziehbar.«[42]

Derzeitiger Stand: Das Bundesverwaltungsgericht in Leipzig hatte am 25. September 2019

> »entschieden, dem Gerichtshof der Europäischen Union (EuGH) eine Frage zur Auslegung der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) vorzulegen. Von der Klärung dieser Frage hängt die Anwendbarkeit der im Telekommunikationsgesetz enthaltenen Regelungen zur Vorratsdatenspeicherung ab.«[43]

Bis zur endgültigen Entscheidung ist damit die Pflicht zur Datenspeicherung ausgesetzt.

Anlass für dieses Urteil waren die Klagen der Telekom und des Münchener Internet-Service-Provider SpaceNet gegen die Pflicht zur Datenspeicherung.[44]

Auch wenn die Speicherpflicht derzeit ausgesetzt ist, hat die Vorratsdatenspeicherung noch immer viele Befürworter. Jüngstes Beispiel ist Manuela Schwesig, Ministerpräsidentin von Mecklen-

42 Stoppt die Vorratsdatenspeicherung, o.J.

43 VBVerwG. Pressemitteilung 2019

44 Vgl. Schäfer 2019.

burg-Vorpommern, die sich mit Datum vom 08.09.2020 für die Wiedereinführung der Vorratsdatenspeicherung aussprach.[45] Dies soll der verstärkten Bekämpfung von Kinderpornografie und extremistischen Straftaten dienen. Dazu hat sie einen Antrag an den Bundesrat gestellt, man möge die Einführung der Mindestspeicherpflicht soweit möglich bereits jetzt vorbereiten, um bei einem entsprechenden Urteil des Europäischen Gerichtshofes sofort handlungsfähig zu sein.[46]

Am 6. Oktober 2020 hat der Europäische Gerichtshof seine Urteile zu drei Klagen gegen die Vorratsdatenspeicherung aus dem Vereinigten Königreich, Frankreich und Belgien verkündet. Danach ist eine flächendeckende und pauschale Speicherung von Internet- und Telefon-Verbindungsdaten *nicht* zulässig. Ausnahmen sind aber möglich, wenn es um die Bekämpfung schwerer Kriminalität oder den konkreten Fall einer Bedrohung der nationalen Sicherheit geht.[47] Das Urteil für Deutschland liegt zwar noch nicht vor. Es dürfte aber kaum anders ausfallen. Die Aktion von Manuela Schwesig erweist sich damit im Nachhinein als sinnloser und wenig durchdachter Aktionismus.

Eine weitere sehr umstrittene Regelung ist die Regelung über die Weitergabe von Flugpassagierdaten.

> »Das [EU] Parlament hat [am 14.04.2016] die neue Richtlinie zur Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität verabschiedet. Die Regeln verpflichten Luftfahrtgesellschaften dazu, ihre Fluggastdaten für Flüge von der EU in Drittländer und andersherum den nationalen Behörden zur Verfügung zu stellen.«[48]

45 Vgl. Schwesig 2020.

46 Vgl. ebd.

47 Vgl. EuGH verbietet Vorratsdatenspeicherung erneut, 2020; Vorratsdatenspeicherung ist nur in Ausnahmen zulässig, 2020.

48 Parlament stimmt EU-Richtlinie über Verwendung von Fluggastdaten zu, 2016.

> »Diese Informationen müssen für einen Zeitraum von fünf Jahren vorgehalten werden. Sechs Monate nach der Übermittlung allerdings müssen die Daten unkenntlich gemacht werden, d.h. Datenelemente wie zum Beispiel der Name, die Anschrift oder Kontaktdaten dürfen nicht mehr sichtbar sein.«[49]

> »Ich will nicht so weit gehen zu sagen, die Unschuldsvermutung würde außer Kraft gesetzt. Aber sie wird abgeschwächt in ihrer Bedeutung für den Rechtsstaat. Und das halte ich wirklich für fatal.«[50]

Dies ist eine Warnung der Philosophin Beate Rössler vor all diesen Datensammlungen. Denn in den meisten Fällen werden die Daten aller Bürger erfasst, unabhängig davon, ob ein Verdachtsmoment vorliegt oder nicht. Zudem bedeuten diese Datensammlungen immer auch eine Überwachung der Bevölkerung.

Völlig verändert hat sich die Situation seit Beginn der Corona-Pandemie. Auf einmal wird alles dem Schutz der Gesundheit untergeordnet. Was umgekehrt bedeutet, dass alle Urteile diesen Jahres bezüglich Datensicherheit, Personenrechte und das Recht auf ›Privaten Raum‹ (nicht nur das Recht auf Privatheit, sondern auf Freiheit im Privaten) unter dem Eindruck von Covid-19 stehen. Die demokratische Zumutung rechtfertigt sich im Angesicht der tödlichen Bedrohung, die ein für das Auge unsichtbares Virus wie Sars-Cov-2 darstellt. Es gilt, zwischen so vielen Daten und ›demokratischen Zumutungen‹ wie nötig, um Covid-19 einzudämmen und so vielen Freiheiten und Rechten wie möglich, die Balance zu wahren.

> »Diese Pandemie ist eine demokratische Zumutung; denn sie schränkt genau das ein, was unsere existenziellen Rechte

49 Ebd.

50 Rössler 2016.

> und Bedürfnisse sind – die der Erwachsenen genauso wie die der Kinder. Eine solche Situation ist nur akzeptabel und erträglich, wenn die Gründe für die Einschränkungen transparent und nachvollziehbar sind, wenn Kritik und Widerspruch nicht nur erlaubt, sondern eingefordert und angehört werden – wechselseitig.«[51]

In diesem Zusammenhang lohnt es sich, einen Blick auf die Corona-App zu werfen. Diese App soll helfen, Infektionsketten zu erkennen und zu durchbrechen. Zu diesem Zweck werden sehr sensible Informationen über Corona-Infektionen weitergegeben. Daher wurde bei der Entwicklung der App großen Wert auf ausreichenden Datenschutz und Sicherheit gelegt.

Bei der installierten App erhält man eine anonymisierte Nachricht, wenn sich eine infizierte Person für mindestens 15 Minuten und in einem Umkreis von 2 m oder weniger in der Nähe des jeweiligen Appnutzers aufgehalten hat. Dazu muss die infizierte Person allerdings ebenfalls die App installiert haben. Nur wenn die Menschen verstanden haben, warum diese App so wichtig ist und wenn sie überzeugt sind, dass sie dieser App vertrauen können, werden sie sie auch einsetzen.[52]

Um dieses Vertrauen zu rechtfertigen, haben in Österreich drei Organisationen den Quellcode der österreichischen App analysiert. Das Ergebnis ist ein langer Bericht, der Mängel aufzeigt und Verbesserungsvorschläge macht. Diese wurden von den Entwicklern der App bereitwillig aufgegriffen. Teilweise wurden sie sofort umgesetzt, zum Teil wurde ihre Umsetzung für einen späteren Zeitpunkt anvisiert.

---

51 Regierungserklärung von Bundeskanzlerin Dr. Angela Merkel, 2020.

52 Die App wurde 22,8 Millionen Mal heruntergeladen. Stand 19.11 2020. Vgl. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_20112020.pdf?__blob=publicationFile. [Letzter Zugriff 19.11.2020].

Eine solche Zusammenarbeit ist nicht unbedingt selbstverständlich. Das zeigt das Beispiel Deutschlands. Dort haben mehrere Organisationen einen offenen Brief an die Regierung geschickt, indem sie u.a. darum baten, den Argumenten und ›Vorbehalten‹ von ›Experten‹ mehr Gehör zu schenken. Hauptkritikpunkt war dabei der zentrale Ansatz, den die deutsche Bundesregierung ursprünglich verfolgte. Dieser Brief wurde von rund 300 internationalen Wissenschaftlerinnen und Wissenschaftlern unterzeichnet.[53] Erfreulicherweise hat auch Deutschland sich inzwischen für eine dezentrale Speicherung der Daten entschieden.

> »Die Corona-App ist zwar Open Source – der Programmcode ist für alle einsehbar und die Software gratis – nicht aber die Schnittstelle zum Betriebssystem.«[54]

Dahinter beginnt das Firmengeheimnis von Google und Apple. Grassegger, ein Schweizer Journalist, hat dies einmal so beschrieben: »Es ist, als ob man die Bauanleitung einer Tür veröffentlicht, aber nichts über das Zimmer dahinter.«[55]

Das ist wohl einer der Gründe, warum die Corona-App keine Daten über individuelle Erkrankungen liefert und die Identität der Infizierten verschleiert.[56] Zu groß ist die Angst davor, dass persönliche Daten missbraucht werden könnten.[57]

---

53 Denn eine zentrale Speicherung wäre deshalb so problematisch, weil die Sicherheit dieser hochsensiblen Daten nicht wirklich gewährleistet werden kann. Auch ist das Risiko einer De-Anonymisierung deutlich höher als bei einer dezentralen Lösung. Zudem besteht die Gefahr, dass diese Daten auch für andere Zwecke verwendet werden. Die Privatheit der Nutzer ist so nicht ausreichend sichergestellt.

54 Grassegger 2020

55 Grassegger 2020.

56 Berichtet wird dies explizit über die SwissCovid App, aber das gilt sicherlich auch für die deutsche und die österreichische Corona-App.

57 Vgl. Grassegger 2020.

Neueste Entwicklungen zeigen, wie groß die Datensammelwut des Staates ist. So hat die EU-Kommission einen Gesetzesentwurf vorlegt, der das Teilen wertvoller Datensätze innerhalb der Europäischen Union erleichtern soll und mit dem der Zugang sowohl zu persönlichen Daten von Nutzern als auch zu nicht-persönlichen Daten erleichtert werden soll. Dass hier Datenschützer vor allem wegen der Daten von Nutzenden erhebliche Bedenken haben, liegt auf der Hand, denn diese sind durch Gesetze wie die Datenschutzgrundverordnung geschützt.[58]

Vor diesem Hintergrund ist es nicht verwunderlich, dass es auch kritische Stimmen zum Verhalten des Staates gibt:

> »Der Staat, so das Bild, ist nicht nur Partner in der Abwehr von Risiken und Verletzungen, er ist nicht nur Baumeister und Helfer bei der Konstruktion von Schutzwällen, welche die Sicherheit der Informationsverarbeitung gewährleisten; er ist bei dieser Verarbeitung auch Spion und Lauscher an der Wand, gegen die Interessen derer, für deren Kommunikation er sich interessiert.«[59]

Dieses Zitat ist insofern bemerkenswert, als es von einem Repräsentanten des Staates, einem Verfassungsrichter, kommt, der die Rolle des Staates durchaus zwiespältig sieht. Es entstammt einem Vortrag auf dem 7. Deutschen Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am 14. Mai 2001. Winfrid Hassemer war durchaus bewusst, dass dem Veranstalter des Kongresses, dem BSI, diese Aussage wohl kaum genehm sein würde.

In diesen Zusammenhang passt auch eine Aussage von Obama auf der South By Southwest Interactive, einer wichtigen Technikkonfe-

58 Vgl. Fanta, A./Kamps, L. 2020.

59 Hassemer 2001. Winfried Hassemer, verstorbener deutscher Strafrechtler, einst Vizepräsident des deutschen Bundesverfassungsgerichts.

renz in Austin, Texas. Er plädiert dort für eine gesunde Skepsis gegenüber dem Staat.

> »Wir alle schätzen unsere Privatsphäre, unsere Gesellschaft beruht auf der Verfassung und den Bürgerrechten (Bill of Rights), sowie auf einer gesunden Skepsis gegenüber übergroßer Regierungsmacht.«[60]

60 »All of us value our privacy, and this is a society that is built on a Constitution and a Bill of Rights and a healthy skepticism about overreaching government power.« Remarks by the President at South By Southwest Interactive, 2016.

# Unsere Daten: Pro und Contra

Unsere Daten kann man unter sehr verschiedenen Aspekten betrachten. Sie gehören mittlerweile zu den wertvollsten Rohstoffen unseres Jahrhunderts, durch sie bieten sich ungeahnte Möglichkeiten zum Beispiel der Steuerung und Überwachung von Prozessen. Aber getreu dem Motto ›Wissen ist Macht‹ verleihen sie demjenigen, der sie besitzt, Macht, etwa indem man damit Menschen kontrollieren und beeinflussen kann. Diese Daten sind Segen und Fluch zugleich. Im folgenden Abschnitt sollen einige dieser Aspekte näher betrachtet werden.

## Der Wert der Daten

> »Persönliche Daten sind das Erdöl des Internet und die neue Währung der digitalen Welt.«[1]

Dieser bekannte Satz zeigt sehr deutlich, welchen Stellenwert persönliche Daten heute besitzen. Ablesen lässt sich das auch an wirtschaftlichen Aussagen und Prognosen. So schätzt die EU-Kommission, dass der EU-Datenmarkt (auf dem digitale Daten als aus Rohdaten gewon-

1 »Personal data is the new oil of the Internet and the new currency of the digital world.« Kuneva 2009.

nene Produkte oder Dienste gehandelt werden) bis 2020 auf 84 Milliarden Euro anwachsen wird.[2]

> »Unentgeltliche Datenlieferungen aller führen zu nicht gekannten Gewinnen sehr weniger Digitalunternehmer und verstärken so das Ungleichgewicht zwischen ihnen und uns.«[3]

Das im obigen Zitat angesprochene Ungleichgewicht ergibt sich u.a. dadurch, dass die ungeheuren Mengen an Daten zwar den sammelnden Konzernen bekannt sind, die Betroffenen aber in der Regel keine Ahnung haben, welche Daten über sie gesammelt, geschweige denn, welche Schlüsse daraus gezogen wurden.

Bedauerlicherweise hat die Europäische Union in der Richtlinie 2019/770 festgelegt, dass der Verbraucher die Bereitstellung digitaler Dienstleistungen statt mit Geld auch mit der Bereitstellung personenbezogener Daten bezahlen kann.[4]

Noch nie waren Daten so wertvoll wie heute, lässt sich doch mit ihnen vortrefflich Geld verdienen. Diese Gewinne spiegeln sich in den Börsenwerten der IT-Unternehmen wider, deren wichtigste Handelsware Daten sind. Beispielhaft seien hier die Börsenwerte für die GAFAM-Konzerne aufgeführt.[5]

- Alphabet, der Mutterkonzern von Google, hat mit Stichtag 08.07.2020 einen Börsenwert von 966 Milliarden US-Dollar.[6]

---

2 Vgl. Europäische Datenwirtschaft: EU-Kommission stellt Konzept für Daten-Binnenmarkt vor 2017.

3 Runde 2016.

4 Vgl. RICHTLINIE (EU) 2019/770 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, 2019.

5 GAFAM steht für Google, Apple, Facebook, Amazon, Microsoft.

6 Bloomberg 2020.

- Apple hat mit Stichtag 08.07.2020 einen Börsenwert von 1581 Milliarden US-Dollar.[7]
- Facebook hat mit Stichtag 08.07.2020 einen Börsenwert von 647 Milliarden US-Dollar.[8]
- Amazon hat mit Stichtag 08.07.2020 einen Börsenwert von 1376 Milliarden US-Dollar.[9]
- Microsoft hat mit Stichtag 08.07.2020 einen Börsenwert von 1543 Milliarden US-Dollar.[10]

## Die Profiteure der Datensammlungen und ihre Argumente

Die großen Konzerne verdienen Milliarden mit den Daten ihrer Kunden. Durch den Zugriff auf diese Daten ist jedoch die Privatsphäre dieser Kunden massiv bedroht. Insofern steht für die Konzerne das Konzept einer geschützten Privatsphäre diametral zu ihrem Geschäftsmodell. Diejenigen, die von diesen Datensammlungen profitieren, deren Geschäftsgrundlage diese Daten sind, setzen alles daran, jegliche Bedenken gegen das Datensammeln zu zerstreuen. Hier einige der bekanntesten Zitate dazu:

> »Sie haben keine Privatsphäre mehr. Finden Sie sich damit ab.«[11]

7 Ebd. Am Mittwoch, den 19.08.2020 stieg die Aktie auf über 2 Billionen US-Dollar, sank dann aber bis zum Ende dieses Handelstages auf 1,9789 Billionen US-Dollar. Vgl. Rekord für Apple: Börsenwert erreicht zwei Billionen Dollar, 2020.

8 Bloomberg 2020.

9 Ebd.

10 Ebd.

11 »You have zero privacy anyway – Get over it.« Sprenger 1999; Wefing 2010.

Scott McNealy, einer der Gründer von Sun Microsystems, machte 1999 diesen Ausspruch. Sein Kommentar zur nicht mehr zeitgemäßen Privatheit fand große Beachtung.

> »Diese Privatsphäre, über die Sie so besorgt sind, ist eine Illusion. Alles, was Sie aufgeben müssen, ist ihre Illusion, nicht ihre Privatsphäre.
>
> Im Internet können Sie heute alles über ihren Nachbar finden, seine Kreditlimits, wo er arbeitet, wie er seine Raten zahlt und Vieles mehr.«[12]

Diese Äußerungen machte Oracle Chef Larry Ellison bei einem Fernsehinterview in San Francisco (2001).

> »Privatsphäre ist nicht mehr zeitgemäß.«[13]

Mit diesem Zitat reiht sich Marc Zuckerberg in den Reigen der großen Profiteure ein.

Von diesen Konzernen zu verlangen, sie sollten den Schutz der Privatsphäre achten, würde bedeuten, dass sie ihr Geschäftsmodell in Frage stellen, denn mit diesen Daten verdienen sie Milliarden. Shoshana Zuboff, emeritierte Professorin für Betriebswirtschaftslehre

12 »The privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy. Right now, you can go onto the Internet and get a credit report about your neighbor and find out where your neighbor works and how much they earn.« Fenwick/Brownstone 2003; Faber 2001.

13 »[…] privacy is no longer a ›social norm‹.« Dies ist ein vielzitierter Ausspruch von Zuckerberg. Facebook's Zuckerberg Says Privacy No Longer A ›Social Norm‹, 2016. Der genaue Wortlaut wird in Medium wie folgt wiedergegeben: »People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people […] that social norm is just something that has evolved over time.« Sneyd 2018; Haupt 2010.

an der Harvard Business School, zieht den folgenden sehr treffenden Vergleich:

> »Von Überwachungskapitalisten zu verlangen, sie sollten die Privatsphäre achten oder der kommerziellen Überwachung im Internet ein Ende setzen, wäre so, als hätte man Henry Ford dazu aufgefordert, jedes T-Modell [ein Auto von Ford, dessen großer Erfolg auf der Massenfertigung beruhte] von Hand zu fertigen. Solche Forderungen sind existentielle Bedrohungen, die das Überleben der betreffenden Entität gefährden, weil sie deren Grundmechanismen in Frage stellen.«[14]

> »Alle wollen, dass ihre Kommunikation sicher ist – außer vor ihnen selber.«[15]

Während die Konzernchefs einerseits aus gutem Grund den Schutz der Privatsphäre als nicht mehr zeitgemäß betrachten, versuchen sie mit einem anderen Argument die Nutzer dazu zu bewegen, doch genau ihnen ihre Daten anzuvertrauen. So stellt das Versprechen von Konzernen, die Daten seien bei ihnen sicher, ein Lockmittel dar, um eben in den Besitz dieser Daten zu kommen. Verschwiegen wird dabei wohlweislich, dass mit der Sicherheitsgarantie gleichzeitig ein Zugriff auf die Daten durch die Institution, die diese Sicherheit garantiert, verbunden ist.

Bruce Schneier, ein renommierter amerikanischer Sicherheitsexperte, beschreibt diesen Run auf die Daten sehr witzig, aber leider sehr zutreffend:

> »Eric Schmidt will, dass Ihre Daten sicher sind. Er möchte, dass Google der sicherste Platz für Ihre Daten ist – solange es Ihnen nichts ausmacht, dass Google Zugriff auf Ihre Daten hat. Face-

14 Zuboff 2016; vgl. auch Zuboff 2018, S. 224.

15 »Everyone Wants You To Have Security, But Not from Them.« Schneier 2015.

> book will das Gleiche: Ihre Daten vor allen außer vor Facebook schützen. Hardware-Unternehmen sind nicht anders. Letzte Woche haben wir gelernt, dass Lenovo-Computer mit einem Stück Adware namens Superfish ausgeliefert wurden, das die Sicherheit der Benutzer brach, um sie für Werbezwecke auszuspionieren. Regierungen sind nicht anders. Das FBI will, dass die Leute eine starke Verschlüsselung haben, aber es wünscht den Backdoor-Zugang, damit es an Ihre Daten kommen kann. Der britische Premierminister David Cameron möchte, dass Sie gute Sicherheit haben, so lange sie nicht so stark ist, dass die britische Regierung ausgeschlossen ist. Und natürlich, die NSA gibt viel Geld aus, um sicherzustellen, dass es keine Sicherheit gibt, die sie nicht brechen kann. Unternehmen wollen Zugang zu Ihren Daten, um damit Gewinn zu machen; Regierungen wollen es aus Sicherheitsgründen, seien sie wohlwollend oder bösartig.«[16]

Angesichts dieser Übermacht fällt es schwer, nicht zu resignieren. Doch auch wenn man sich vor dem Zugriff sowohl des Staates als auch der Konzerne nur bedingt schützen kann, empfiehlt es sich, trotz allem stets darauf bedacht zu sein, so wenig Daten wie irgend möglich preiszugeben. Unterstützung kommt hier von den Bürgerrechtsbewegungen, die immer wieder gegen diese Übermacht der Datensammler protestieren und sich für den Schutz der Daten der Bürger einsetzen.

## Die Farce von den kostenlosen Diensten

> »Google gibt seine Dienste weitgehend kostenlos weiter. Aus der Sicht des Einzelnen ist dies ein Geschäftsmodell, mit dem er oder sie leben kann. Aber darin liegt das Risiko: Die Dienste

16 Schneier 2015.

> sind nicht wirklich kostenlos; sie kommen auf Kosten Ihrer persönlichen Daten.«[17]
>
> »Du bist nicht der Kunde der Internetkonzerne. Du bist ihr Produkt.«[18]
>
> »Kostenlose Inhalte […] sind der ›verfluchte Geburtsfehler des Internet‹. Man übersah, dass es nichts kostenlos gibt.«[19]
>
> »Wer immer einem ein kostenloses Angebot macht, ist verdächtig. Man sollte unbedingt alles ausschlagen, was sich als Schnäppchen, Prämie oder Gratisgeschenk ausgibt. Das ist immer gelogen. Der Betrogene zahlt mit seinem Privatleben, mit seinen Daten und oft genug mit seinem Geld.«[20]
>
> »Die Kostenfreiheit der Dienstleistungen ist somit eine Illusion. Wir bezahlen für den Service mit unseren Daten und, viel teurer, mit unserer Privatsphäre. Das Wohlfahrtsstaatsmodell à la Silicon Valley ist mit einem Verlust persönlicher Freiheiten verbunden.«[21]

Wer benützt sie nicht gerne, die vielen kostenfreien Dienste, wie z.B. die Google Suche, Google Maps, Google Mail, die vielen angebotenen Apps wie z.B. WhatsApp Messenger, Dropbox und viele mehr?

Bequemlichkeit und der teilweise wirklich gute Service der vielen kostenlosen Dienstleistungen führen dazu, dass diese Angebote be-

17 »Google largely gives away its services for free. From the individual's perspective, this is a business model that he or she can live with. But therein lays the risk. The services aren't actually free; they come at the cost of your personal information.« Conti 2008, S. 1.

18 Lanier 2014.

19 Otte 2014.

20 Enzensberger 2014.

21 Lobe 2014.

denkenlos angenommen werden. Privatsphäre und Sicherheit sind dagegen unwichtig.

> »Im Umgang mit modernen Technologien sind vielen Nutzern in den vergangenen Jahren Fragen wie Datenschutz oder selbst das Bankgeheimnis zunehmend egal geworden – solange sie ihm einen Zusatznutzen bieten. Komfort steht da ganz oben auf der Liste.«[22]

22 Kanning 2016.

# Unsere Daten: Was verraten sie über uns?

Dass unsere Daten gesammelt werden, dürfte inzwischen hinlänglich bekannt sein. Aber was danach mit diesen Daten passiert, an wen sie weitergegeben werden und welche Schlussfolgerungen daraus gezogen werden, von all dem haben die meisten Menschen keine Vorstellung. Die nachfolgenden Abschnitte widmen sich diesem Aspekt der Sammlung von Daten.

## Nothing to Hide

> »Ich habe nichts zu verbergen.«
> »Nothing to Hide.«[1]

»Ich habe nichts zu verbergen« ist wohl die am meisten verbreitete Ausrede, warum Privatheit unwichtig sei.

Als Begründung für die Unsinnigkeit dieser Aussage wird gerne eine Aussage von Richelieu zitiert: »Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen.«[2]

Häufig lassen eine gewisse Bequemlichkeit sowie der Komfort der vielen kostenlosen Dienste, die das Leben einfacher und bequemer machen und auf deren Nutzung man nicht verzichten möchte, die Ri-

1 Titel eines Buches von Daniel Solove. Ders. 2001.

2 Schneier 2006a; vgl. die engl. Fassung Schneier 2006b.

siken einer Herausgabe von privaten Daten als marginal erscheinen. Immer wieder findet man Berichte, dass Menschen sehr sensible private Daten bereitwillig gegen marginale Belohnungen herausgeben.

> »Ein Gratis-Mandelgipfel genügt als Köder, und schon reichen zahlreiche Kunden einem unbekannten Bäcker AHV-Nummern [Sozialversicherungsnummern] und Angaben zu Partnerschaften über die Theke.«[3]

Gerne wird auch argumentiert, dass man, wenn man nichts Unrechtes getan habe, man auch nichts zu verbergen brauche, was impliziert, dass Privatheit das Verbergen von Unrecht zum Ziel hat. Das ist ein vielfach angeführtes Argument, um Vertreter des »Nothing to Hide« Standpunktes zu überzeugen.

Doch mag man noch so gute Argumente haben, die Menschen, die den Standpunkt vertreten, sie hätten nichts zu verbergen, sind weitgehend argumentations- und überzeugungsresistent. Alle Versuche, sie zu überzeugen, sind damit von vornherein zum Scheitern verurteilt – egal wie gut die vorgebrachten Argumente sind.

Man kann das sehr schön an der Reaktion auf die Snowden-Enthüllungen sehen. Eine repräsentative Umfrage des Marktforschungsunternehmens GfK im Auftrag der »Welt am Sonntag« zeigt, dass 76,9 Prozent der Befragten ihren Umgang mit persönlichen Daten nicht geändert haben.[4]

Interessant ist, was der Philosoph Michael Sandel in diesem Zusammenhang über seinen Sohn sagt:

> »Der ist erst Ende 20 und ihm ist es egal, ob die NSA erfährt, mit wem er telefoniert hat. Denn für ihn liegt die Grenze ganz woanders: Wenn seine Eltern auf solche Informationen zugreifen könnten, würde er es als Verletzung seiner Rechte sehen.

3 Mäder 2019.

4 Vgl. Heuzeroth 2014.

> Das Beispiel zeigt, dass es bei der Frage nach Privatsphäre eine Rolle spielt, wer solche Daten nutzen möchte und ob es mit einer Zustimmung geschieht.«[5]

Wer weiß schon, welche Daten über ihn gesammelt werden. Wer sich dafür interessiert, wird in Publikationen eine Fülle von Hinweisen finden. Damit kann er zumindest eine Ahnung bekommen, was über ihn gesammelt sein könnte, auch wenn es im Detail nicht feststellbar ist. Dieses Datensammeln ist im Grunde heimtückisch. Man merkt es nicht, es tut nicht weh, und sollte es wirklich wehtun, ist es zu spät. Man spricht hier auch von der mangelnden Spürbarkeit von Überwachung.[6]

Ein weiterer Punkt ist, dass kaum jemand eine Vorstellung hat, was man mit diesen Daten machen kann, welche Informationen sich daraus gewinnen und welche Schlussfolgerungen sich ziehen lassen.

So wird häufig die Ansicht vertreten, dass die sogenannten Verbindungsdaten, also wer, wann mit wem kommuniziert hat, unkritisch seien. Amerikanische Forscher haben jedoch in einer Studie nachgewiesen, dass die Überwachung mittels dieser Verbindungsdaten (auch als Telefonmetadaten bezeichnet) erhebliche Auswirkungen auf die Privatsphäre hat. Telefonmetadaten sind eng miteinander verbunden, leicht wiedererkennbar und ermöglichen auf einfachste Weise Zugang zu Orten, Beziehungen und sensiblen Schlussfolgerungen.[7]

Dem Thema »Privacy« hat der amerikanische Juraprofessor an der George Washington University Law School, Daniel Solove, ein sehr lesenswertes Buch gewidmet. Es hat den Titel »Nothing to Hide«[8]. Ob er damit wirklich eine größere Gruppe überzeugen konnte, darf man bedauerlicherweise bezweifeln.

---

5 Wir brauchen eine neue Privacy-Debatte, 2016.

6 Vgl. Jahr 1 nach Snowden, 2015.

7 Vgl. Mayer/Mutchler/Mitchel 2016.

8 Solove 2001.

Hinzu kommt ein weiterer Aspekt: Es gibt inzwischen ein Phänomen, das mit dem Begriff der »Inverse Privacy« beschrieben wird.

> »Eine persönliche Information, zu der jemand Zugang hat, aber Du selbst nicht, bezeichnet man als inversely (entgegengesetzt) privat.«[9]

Damit wird die Situation beschrieben, dass eine dritte Partei Zugriff auf meine privaten Daten hat, ich selbst diesen Zugriff aber nicht habe.

Besonders brisant ist das, wenn die gespeicherten Daten einer Analyse unterzogen werden. Welche Schlüsse über meine Kreditwürdigkeit, meinen Gesundheitsstatus und über vieles mehr gezogen werden, erfahre ich nicht, habe somit auch keine Möglichkeit, etwaige Fehler zu korrigieren.

Es ist diese Inverse Privacy, die wir immer häufiger antreffen. Ein anschauliches Beispiel dafür bietet Max Schrems, dem Facebook nach langwierigem Verfahren eine CD mit 1200 pdf-Seiten zur Verfügung stellte. Dies war die Antwort auf eine Anfrage von Max Schrems nach allen Daten, die Facebook über ihn gespeichert hat.[10]

> »Wenn wir unsere Daten einfach gratis weggeben, vergeben wir auch ein Teil unserer Stimme in der Demokratie.«[11]

Inzwischen weiß man, dass diese Daten auch dazu benützt werden, Menschen zu beeinflussen. Das bekannteste Beispiel dafür ist Cambridge Analytica. Diese Firma hat mit (nicht rechtmäßig erworbenen) Daten von Facebook-Nutzern versucht, die Wahl von Donald Trump sowie den Brexit zu unterstützen. Ob diejenigen, die so leichtfertig

9 »Call an item of your personal information inversely private if some party has access to it but you do not.« (Gurevich/Hudis/Wing 2016)

10 Vgl. Bähr 2015; Levine 2015.

11 Pagel/Portmann/Vogt 2020.

ihre Daten zur Verfügung stellen, sich darüber im Klaren sind, wozu ihre Daten missbraucht werden können, mag man bezweifeln.

## No Place to Hide

> »Es wird keinen Ort mehr geben, wo man sich verstecken kann.«[12]

> »Siehst du, die Übeltäter [die Terroristen] schlagen gerne zu, und dann versuchen sie, sich zu verstecken. Und langsam, aber sicher, werden wir sicherstellen, dass sie keinen Platz zum Verstecken haben.«[13]

Diese Warnung des amerikanischen Präsidenten George W. Bush, dass es nirgendwo auf der Welt mehr einen Platz geben werde, wo man sich verstecken kann, richtet sich zunächst an Terroristen. Es war eine seiner Reaktionen auf den Anschlag vom September 2001 auf das World Trade Center.

Die Gefahren durch Überwachung wurden in den USA schon sehr früh erkannt. So warnte Senator Frank Church in einer Nachrichtensendung:

> »Diese Fähigkeit [der NSA alles zu überwachen] könnte zu jeder Zeit gegen das amerikanische Volk gerichtet werden, und kein Amerikaner hätte mehr Privatsphäre. […] Es gäbe keinen Platz mehr zum Verstecken.«[14]

---

12 Es gibt eine ganze Reihe von Büchern mit diesem Titel, z.B. Greenwald 2014.

13 »You see, the evildoers [the terrorists] like to hit and then they try to hide. And slowly, but surely, we're going to make sure they have no place to hide.« Bush at FEMA Headquarters, 2001.

14 »That capability [of the NSA] at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to

Bemerkenswert an diesem Zitat ist, dass diese Warnung vor den Möglichkeiten der NSA aus dem Jahr 1975 stammt (siehe Kapitel »Privatheit und Demokratie«). Senator Frank Church war Vorsitzender des Sonderausschusses des US-Senats zur Untersuchung des Regierungshandelns mit Bezug zu Aktivitäten der Nachrichtendienste. Aus diesem Sonderausschuss, auch als *Church Committee* bezeichnet, gingen die ständigen Ausschüsse zur Kontrolle der Nachrichtendienste im US-Senat und im Repräsentantenhaus hervor.[15]

Es gibt zwei wichtige Bücher mit identischem Titel, die sich mit dem Verlust der Privatsphäre durch die massenhaften Datensammlungen befassen.

### 1. »No Place to Hide« von Robert O'Harrow Jr., 2006[16]

O'Harrow zeigt uns, dass es in dieser neuen Welt eines hochtechnologisierten Inlandgeheimdienstes buchstäblich keinen Platz zum Verstecken gibt.[17] Dieses Buch hat an seiner Aktualität kaum etwas eingebüßt.

Die Datenindustrie wird weiter und immer schneller Informationen über uns sammeln. Die Regierung wird diese Daten im Namen des Heimatschutzes und der Strafverfolgung kaufen. Vermarkter werden uns weiterhin beobachten und Profile erstellen, um uns noch profitabler für sie zu machen.[18]

---

monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide.« Bamford 2005.

15 Vgl. Church Committee 2019.

16 O'Harrow Jr. 2006.

17 »O'Harrow shows us that, in this new world of high-tech domestic intelligence, there is literally no place to hide.« No Place to Hide 2006.

18 »The data industry continues to collect information about you at an accelerating pace. The government continues to buy it in the name of homeland security and law enforcement. Marketers continue to watch you and profile you with the aim of making you more profitable to them.« O'Harrow Jr. 2006, S. 303-304.

Daran hat sich bis heute nichts geändert. Die Snowden-Enthüllungen zeigen im Detail das, was O'Harrow bereits 2006 beschrieben hat.

## 2. »No Place to Hide« von Glenn Greenwald, 2014[19, 20]

Tatsächlich trifft die Warnung, dass es nirgendwo auf der Welt mehr einen Platz geben werde, wo man sich verstecken kann, inzwischen auf jeden zu, d.h. in unserer Zeit wird niemand mehr die Möglichkeit haben, sich zu verstecken. Man mag sagen, verstecken müssen sich nur Terroristen und Kriminelle, aber kein ehrenwerter Bürger. Doch sollte man nicht vergessen, dass die Möglichkeit, sich zu verstecken z.B. indem man in den Untergrund ging, vielen während der Herrschaft des Naziregimes das Leben gerettet hat. Damals war das noch möglich. Heute spricht viel dafür, dass ein Verstecken nicht mehr möglich ist.

> »Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun.«[21]

Dieser sehr bekannte Ausspruch von Google CEO Eric Schmidt zeigt in erschreckender Weise, dass hier eine Welt propagiert wird, in der man sich nicht nur nicht mehr verstecken kann, sondern in der es zudem keine Geheimnisse mehr gibt.

19 Greenwald 2014.

20 Greenwald 2015, Titel der deutschen Ausgabe: *Die globale Überwachung: Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen*.

21 Stöcker 2009. »If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.« Esguerra 2009.

## Wir werden überwacht

> »Du wirst beobachtet.«[22]
>
> »Überwachung ist das Geschäftsmodell des Internet.«[23]
>
> »Einen Staat, der mit der Erklärung, er wolle Straftaten verhindern, seine Bürger ständig überwacht, kann man als Polizeistaat bezeichnen.«[24]

Regierungsbehörden und Privatunternehmen wissen sehr viel über uns. Sie wissen, wo wir leben, was wir verdienen, wofür wir unser Geld ausgeben, was uns gefällt, wofür wir uns interessieren, was wir lesen usw. Die Liste lässt sich beliebig fortsetzen. Es gibt kaum etwas, was sie nicht wissen.

Dabei ist nicht entscheidend, ob staatliche Stellen oder Konzerne die Daten sammeln. Denn im Zweifelsfalle kann sich der Staat die Informationen von den Konzernen besorgen. Insbesondere in den USA müssen die großen Konzerne auf Grund des Patriot Acts die gesammelten Daten der Regierung auf Anforderung zur Verfügung stellen.

»Solange Überwachung das Geschäftsmodell des Internets ist, gibt es keinen großen Unterschied zwischen den Regierungen und den Konzernen«, sagt Bruce Schneier, »›sie alle wollen dich ausspionieren‹.«[25]

---

22 »You are being watched.« O'Harrow Jr. 2006.

23 »Surveillance is the business model of the Internet.« Schneier 2015.

24 Ernst Benda, ehemaliger Präsident des Bundesverfassungsgerichts, im Interview mit tagesschau.de, 5. Juni 2007, Stegers 2007.

25 »Solange Überwachung das Geschäftsmodell des Internets ist, gibt es keinen großen Unterschied zwischen den Regierungen und den Konzernen, … sie alle wollen dich ausspionieren.« (nach Schneier) Drösser 2016.

> »Wer sieht, kann kontrollieren; wer gesehen wird, kann kontrolliert werden.«[26]

Seit Snowden wissen wir, wie die Internetüberwachung der Geheimdienste, insbesondere der NSA funktioniert. Es sind die Hauptknotenpunkte der Kabel- und Servicewerke sowie die IXPs [Internet-Knoten], an denen so gut wie alle Kommunikation abgefangen werden kann. Zudem verschafft die NSA sich Zugriff auf die Server der großen Internetkonzerne, die die vertraulichen Daten ihrer Kunden dort speichern. So gelingt es ihr ein zentralisiertes Schattennetzwerk zu erschaffen, mit dem sie das gesamte globale Netzwerk übersieht und letztendlich auch kontrolliert. Dies alles geschieht unter Ausschaltung jeglicher demokratischen Kontrolle und unbemerkt für die Nutzer des Netzes.

> »Zumindest in der Theorie kann die NSA so nun Informationen über jede normale Internetteilnehmerin abrufen, die Kommunikation jeder mit jeder heimlich mitlesen oder sogar Kommunikationsströme einfach abbrechen oder unbemerkt manipulieren.«[27]

Wer auch immer Daten sammelt, der wird diese Daten nicht nur sammeln, sondern eben auch analysieren. Und das läuft völlig intransparent für den Nutzer ab, d.h. er hat keine Ahnung, welche Schlüsse aus seinen Daten gezogen werden. Die Daten werden bewertet und klassifiziert. Dabei geht es nicht nur darum, auf welche Werbung jemand besonders anspricht, sondern es kann durchaus sein, dass damit der Preis bestimmt wird, den jemand angeboten bekommt, aber auch die Sonderangebote, die gemacht werden. Ob jemand einen Handyvertrag oder einen Kredit bekommt, wie teuer eine Versicherung sein wird,

26 Nosthoff/Maschewski 2017.

27 Fichtner 2016.

die er abschließen möchte und dergleichen mehr, all dies ergibt sich u.a. aus der Analyse seiner Daten.

Wer weiß schon, dass man aus ca. 170 Likes auf Facebook auf sehr sensible Daten schließen kann wie ethnische Zugehörigkeit, Geschlecht, sexuelle Orientierung, politische Präferenzen, religiöse Einstellung, Raucher bzw. Nichtraucher, Trinker, Einnahme von Drogen, Alleinstehend oder in einer Partnerschaft lebend?[28]

> »Bei der Überwachung geht es nicht darum, Ihre Geheimnisse zu kennen, sondern um die Verwaltung von Bevölkerungsgruppen, die Verwaltung von Menschen.«[29]

> »Menschen ändern automatisch ihr Verhalten, wenn sie überwacht werden.«[30]

Das ist der Fall, wenn ein Versicherungsunternehmen, wie z.B. Generali, Kunden mit einer ermäßigten Krankenversicherung lockt, wenn sie per App belegen, dass sie Sport treiben. De facto ist dies eine Zustimmung zur Überwachung mit dem Ziel einer Verhaltensänderung im Lebensstil. Der Betroffene gibt damit ein Stück seiner Freiheit auf, indem er versucht, sich so zu verhalten wie der Konzern es wünscht. Was man dabei nicht übersehen sollte, ist, dass es hier keineswegs um das Wohl des Einzelnen geht, sondern einzig und allein um die ökonomischen Interessen von mächtigen Konzernen. Wenn der Betroffene alt oder krank wird, kann man davon ausgehen, dass sich das Belohnungssystem gegen ihn wenden wird.[31]

---

28 Vgl. Christl/Spiekermann 2016, S. 15.

29 »Surveillance is not about knowing your secrets, […] but about managing populations, managing people.« Grossman 2016.

30 Janker 2014.

31 Vgl. ebd.

> »Das größte Sicherheitsrisiko ist aber immer noch der sorglose Umgang der Bürger mit ihren persönlichen Daten.«[32]

Es ist dieser Aspekt, der der Überwachung Tür und Tor öffnet. Selbst wenn Bürger sagen, dass ihnen ihre Privatsphäre wichtig ist, richten sie sich nicht danach. Man spricht hier vom sogenannten Privacy Paradox.

> »Das Privacy Paradox beschreibt die – auf den ersten Blick – widersprüchliche Tatsache, dass sich Internetnutzer einerseits Sorgen um ihre Privatsphäre im Netz machen, andererseits aber ganz und gar nicht besorgt handeln: Trotz großer Bedenken stellen sie sensible Daten wie Handynummern, Aufenthaltsorte oder private Fotos offen ins Netz. Das Privacy Paradox umfasst dieses Auseinanderdriften von Einstellungen und konkretem Handeln in der digitalen Welt.«[33]

## Das Internet der Dinge (IoT)

> »Dinge aus unserem Alltag sammeln Daten über uns, verschicken diese und werten sie aus.«[34]

Das Internet der Dinge (Internet of Things) besteht aus minimalen Sensoren und Minicomputern, die untereinander im Informationsaustausch stehen. Sie sind so klein, dass sie überall eingesetzt werden können, in Geräten, in Bekleidung und sogar im menschlichen Körper. Sie sind mit dem Internet verbunden und können so kommunizieren. Sie sammeln Unmengen an Daten, analysieren sie und geben sie weiter. Dieses Internet der Dinge ist ein riesiges globales Netzwerk,

32 Thiel 2016.

33 Lutz/Strathoff 2014.

34 Dr. Datenschutz 2015.

dessen Struktur ›jederzeit und überall verfügbar, für jedes und jeden‹ ist. Es verbindet Geräte, Systeme, Daten und Personen. Man spricht auch davon, dass dieses Netzwerk ubiquitous – allgegenwärtig – ist. Dadurch eröffnen sich bisher ungeahnte Möglichkeiten z.B. zur technischen Steuerung von Geräten, die den Alltag der Menschen gravierend verbessern. Man denke nur daran, wie bequem es ist, wenn man mit dem Handy auf dem Nachhauseweg die Heizung hochstellen kann, oder wenn der Staubsauger eine Info an das Handy sendet, dass neue Staubsaugerbeutel bestellt werden müssen. Weitere Beispiele sind – die Waschmaschine, die an das Handy eine Nachricht schickt, wenn sie durchgelaufen ist – oder das Fitnessarmband, das die sportlichen Aktivitäten seines Trägers misst und diese auf sein Handy schickt, vielleicht aber auch an seine Krankenkasse – oder das mit vielen Sensoren und Prozessoren ausgestattete Auto, das die Strecke erfasst, die gefahren wurde, und das mitteilt, wenn getankt werden muss, und vieles mehr – oder der Fernseher, der nicht nur den Aufruf von TV-Sendungen erlaubt, sondern mit dem man Zugriff auf Online-Videotheken hat, mit dem man im Internet surfen und auch per Skype kommunizieren kann – oder der Kühlschrank, der erkennt, wann welche Waren verbraucht sind und diese selbstständig nachbestellt. Ein gutes Beispiel ist auch die französische Bahn, die Züge und Gleise mit Sensoren ausrüstet, die Daten für die Wartung senden. Das ermöglicht den Ingenieuren in den Reparaturwerkstätten, frühzeitig Probleme zu erkennen und Ersatzteile zu bestellen, noch bevor ein Defekt auftritt.[35] Die Liste ließe sich beliebig fortsetzen.

Dass, wie bei allem Neuen, mit dieser Technologie auch Gefahren verbunden sind, gerät dabei oft in Vergessenheit.

35 Vgl. Hill 2018.

> »Daten, die aus dem Internet der Dinge gesammelt werden, decken sensible Verhaltensmuster auf, die Verbraucher lieber geheim halten würden.«[36]

Auf diese Risiken für die Privatsphäre weist das Electronic Privacy Information Center in den USA hin. Bei der Vielzahl der Daten und Kommunikationsbeziehungen gestaltet sich deren Schutz immer schwieriger. So mag der intelligente Stromzähler (Smart Meter), der den Stromverbrauch misst und gegebenenfalls an den Versorger sendet, beim Stromsparen helfen. Mit ihm lässt sich aber auch feststellen, wie viele Menschen gerade in der Wohnung sind und was sie tun.[37] Jemanden in einer Wohnung zu verstecken, ist damit kaum noch möglich. Man denke hier nur an Anne Franks Familie. Sie wäre bei Vorhandensein eines Smart Meters wohl sehr viel früher entdeckt worden.

Die Privatsphäre ist durch das Internet der Dinge auch dadurch bedroht, dass die riesige Menge der Daten ein sehr detailliertes Abbild der Realität erlaubt. Man kann mit Hilfe dieser vielen Sensoren das alltägliche Leben einer großen Zahl von Menschen in Echtzeit erfassen. Wer kann sich schon vorstellen, dass sich aus diesen Daten auch Rückschlüsse auf persönliche Vorlieben, Gewohnheiten, Krankheiten oder Stimmungen ziehen lassen.[38]

Ein typisches Beispiel für die Manipulation des Nutzers sind Telematik-Tarife von Kfz-Versicherungen. Bei diesen Tarifen entscheidet das Fahrverhalten über die Höhe der Versicherungsprämie. Der Versicherer kontrolliert damit nicht nur den Fahrstil des Versicherten, sondern er versucht außerdem, diesen dahingehend zu beeinflussen,

---

36 »Data Collected from the Internet of Things May Reveal Sensitive Behavior Patterns That Consumers Wish to Keep Private.« The On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things 2016.

37 Vgl. Biermann 2013.

38 Vgl Internet der Dinge Was ist das, was bringt das, wie riskant ist das? 2016. (test ist eine Zeitschrift der Stiftung Warentest)

dass weniger Unfälle verursacht werden, wodurch sich der niedrigere Versicherungstarif für die Versicherung letztlich auszahlt.

> »Immerhin behauptet die Allianz: Autofahrer, die diese App einsetzten, führen nach einiger Zeit deutlich vorsichtiger, es gebe einen signifikanten Einfluss des Systems auf den Fahrstil.«[39]

Wer hätte sich zudem vorstellen können, dass ein Herzschrittmacher oder ein Fitnessarmband zu Belastungszeugen bei schweren Verbrechen werden können.[40] Wer weiß schon, dass man den Fahrer eines Wagens durch die Analyse des Fahrstils eindeutig identifizieren kann. Damit lässt sich z.B. feststellen, ob der Sohn und nicht der Vater der Fahrer des Wagens war, oder ob der Fahrer unter Alkohol oder Drogen stand. Somit kann also auch das Auto zum Belastungszeugen gegen den Fahrer des Wagens werden.[41]

Dabei bleibt es aber nicht bei einer Analyse, sondern der nächste Schritt ist dann diese Realität zu kontrollieren.

> »Das Problem [das oft in Zusammenhang mit Ubiquitous Computing gesehen wird] ist die Beeinträchtigung der Privatsphäre. In Wirklichkeit sind es aber die Kontrollmöglichkeiten, die diese Technologie so problematisch machen.«[42]

Die Gefahr der Kontrolle durch solche allgegenwärtigen Systeme hat bereits der US-Informatiker Mark Weiser (1952 bis 1999) erkannt.[43]

---

39 Siedenbiedel 2017.

40 Vgl. Heller 2017.

41 Vgl. Greenberg 2016.

42 »The problem [associated with ubiquitous computing] while often couched in terms of privacy is really one of control.« Christl/Spiekermann 2016, S. 118.

43 »According to Mark Weiser: The problem, while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, whe-

Beispiele dafür in der heutigen Zeit z.B. sind das Fitnessarmband, das die körperlichen Aktivitäten seines Trägers überwacht, der Fernseher, der Auskunft geben kann über empfangene Sendungen, aber auch über die Anzahl der Personen im Raum. Ist die Spracherkennung aktiv, können sogar Gespräche aufgenommen werden.[44] Die elektrische Zahnbürste, deren App das Putzverhalten analysiert und Tipps gibt. Vernetzte Haushaltsgeräte und Sensoren, die zum Beispiel dabei helfen können, dass alte Menschen länger in ihren Wohnungen bleiben können, indem sie überwachen, ob sich ein Mensch normal in seiner Umgebung bewegt, und bei Problemen den Pflegedienst oder einen Verwandten alarmieren.[45]

Shoshana Zuboff warnt daher zu Recht vor diesen Gefahren des Internet der Dinge und kämpft gegen die Übermacht von Google:

> »Das Internet der Dinge bietet gewaltige Möglichkeiten zum Reality-Mining und zur Beeinflussung der Realität. […] Google und andere werden ihr Geld damit verdienen, dass sie diese Realität kennen, manipulieren, kontrollieren und in kleinste Stücke schneiden.«[46]

Bemerkenswert ist, dass bei einem ersten Projekt für ein Smart Home, der intelligenten Steuerung einer Wohnung oder eines Wohnhauses, dieses so konzipiert war, dass Daten aus diesem Projekt ausschließlich den Hausbewohnern zustanden, so dass der Schutz der Privatsphäre gewahrt blieb.[47]

Kaum jemand weiß, dass das auch heute noch möglich ist. Man kann nämlich ein Smart Home auch ohne Internet betreiben. »Wer

---

re information is flowing, how it is being used … and what are the consequences of any given action.« Chow 2017.

44 Vgl. Lobe 2017.

45 Vgl. Schipper 2015.

46 Zuboff 2014.

47 Vgl. Zuboff 2018, S. 20.

sein Smart Home offline lässt, ist sehr viel sicherer – muss aber auf einige Funktionen verzichten.«[48]

> »Es geht nicht mehr nur um Ihre Privatsphäre, sondern auch um Ihr Leben.«[49]

Auf möglicherweise tödliche Gefahren durch das Internet der Dinge weist Ross Anderson hin, ein renommierter Sicherheitsexperte und Professor an der University of Cambridge. So kann der Hackerangriff auf den Bordcomputer eines Autos einen tödlichen Unfall zur Folge haben. Ein gehackter Fernseher ist zwar nicht lebensgefährlich, aber den geplanten Fernsehabend dürfte man wohl erst einmal vergessen. Und was passiert, wenn ein Herzschrittmacher gehackt wird, mag man sich lieber nicht ausmalen.

Es gilt daher, bei den Nutzern ein Bewusstsein für das Vorhandensein dieser Datensammlungen und deren Risiken zu schaffen. Zudem stellt sich die Frage, ob wirklich alles mit jedem vernetzt sein muss. Auch wird das Thema Sicherheit dieser Systeme in Zukunft immer wichtiger werden.

Trotz aller Gefahren, sei es durch die Bedrohung der Privatsphäre als auch durch Möglichkeiten zur Kontrolle und zur Manipulation sowie gravierender Sicherheitsmängel, wird kaum jemand in unserer Gesellschaft mehr auf die bisher ungeahnten Möglichkeiten, die ein solches riesiges Netzwerk bietet, verzichten wollen.

48 Ohland 2019.

49 »It's not just your privacy that's on the line anymore, it's your life.« Anderson 2017.

# Schutz der Privatsphäre durch Verschlüsselung und Anonymisierung

## Wichtige Schutzmaßnahmen

> »Verschlüsselung ist die wichtigste Technologie zum Schutz der Privatsphäre. (Bruce Schneier)«[1]

> »Verschlüsselung und Anonymität, getrennt oder zusammen, schaffen eine Zone der Privatheit zum Schutz von Meinung und Überzeugung.«[2]

Verschlüsselung und Anonymisierung sind die wichtigsten Hilfsmittel, die wir haben, um unsere Kommunikation und unsere Daten vor unberechtigten Zugriffen zu schützen. Auch wenn es keinen hundertprozentigen Schutz gibt, so kann man damit den unbefugten Zugriff zumindest erheblich erschweren.

Je mehr unser Leben im digitalen Raum stattfindet, desto wichtiger werden Werkzeuge für die Kommunikationssicherheit wie Verschlüsselung und Anonymisierung, für den Schutz der Menschenrechte – insbesondere für das Recht auf Privatheit und für das Recht auf freie Meinungsäußerung. Werkzeuge für die Kommunikationssi-

1 »Encryption is the most important privacy-preserving technology we have. (Bruce Schneier)«. Crowe, A./Lee, S. and Verstraete, M. 17. Juni 2015.

2 »Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief.« Encryption and Anonymity create »a zone of privacy online«, says UN Special Rapporteur 2015.

cherheit geben Menschen Zugang zu sicheren und privaten Räumen für ihre persönliche Entfaltung, wo sie ohne unbefugte Einmischung kommunizieren können.[3]

Leider lassen neueste Untersuchungen den Schluss zu, dass Anonymisierung mithilfe Künstlicher Intelligenz und maschinellen Lernens ausgehebelt werden kann. Die derzeit verwendeten Verfahren zur Anonymisierung bieten nicht den versprochenen Schutz der Daten.[4]

> »Verschlüsselung und andere Schutzmaßnahmen (z.B. Zeitverzögerungen bei der Eingabe falscher PINs) sichern unsere Systeme und sollten niemals untergraben werden.«[5]

> »Der Kampf um die Verschlüsselung […] dreht sich im Kern um Freiheit und Unabhängigkeit.«[6]

Doch so wichtig heute Verschlüsselung ist, wird sie doch im Privatbereich nur von vergleichsweise wenigen eingesetzt. Zwar kann in den meisten westlichen Ländern jeder Verschlüsselung einsetzen, doch vielen fehlt das technische Know-how und das Wissen um die Bedeutung von Verschlüsselung. Zudem gilt, dass wir von Verschlüsselung

3 »As more of our lives are lived in the digital realm, communication security tools, such as encryption and anonymity tools and services, are increasingly important to the protection of human rights – particularly the right to privacy and the right to freedom of expression. Communication security tools give individuals access to safe and private spaces for personal development where they can communicate without unwarranted interference.« Anna Crowe, Sarah Lee and Mark Verstraete. (17th June 2015). Securing Safe Spaces Online. Abgerufen am 15. November 2020 von https://privacyinternational.org/sites/default/files/2018-02/Securing %20 Safe %20Spaces %20Online_2_0.pdf.

4 Vgl. Michaels 2019; Hern 2019.

5 »Encryption and other protections (such as time delays as incorrect PINs are entered) secure our systems, and should never be undermined.« Landau 2016.

6 »The fight about encryption, Landau said, ›is, at its core, about freedom and liberty‹.« Landau 2017.

per Mausklick meilenweit entfernt sind. Und es ist nicht sicher, ob wir dies jemals erreichen werden. Dazu sind viel zu viele an unverschlüsselten Informationen interessiert.

## Der Staat will bei Verschlüsselung mitlesen können

> »[Der ehemalige englische] Premierminister David Cameron will gar keine verschlüsselte Kommunikation zulassen: ›Wollen wir in unserem Land Kommunikationsmöglichkeiten erlauben, die wir nicht lesen können? Ich sage nein, wollen wir nicht, und wir müssen dementsprechende Gesetze erlassen‹.«[7]

> »Auch [der ehemalige deutsche] Innenminister Thomas de Maizière will, dass der Staat entschlüsseln kann: ›Unsere Sicherheitsbehörden sollen, natürlich unter rechtsstaatlichen Voraussetzungen, befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln, wenn dies für ihre Arbeit und zum Schutz der Bevölkerung notwendig ist‹.«[8]

> »Michael Rogers [ehemaliger NSA-Chef] will keine Hinter-, sondern eine Vordertür in Krypto-Algorithmen: ›Ich würde das nicht Hintertür nennen. Wenn ich den Ausdruck Hintertür, höre, denke ich, das klingt irgendwie dubios. Warum würden wir die Hintertür nehmen? Wir würden das ganz öffentlich machen‹.«[9]

Diese drei Aussagen mögen stellvertretend sein für die Forderung nach dem Zugriff auf verschlüsselte Informationen, wie sie immer wieder von Politikern erhoben wird.

7 Rieger 2015.

8 Ebd.

9 Ebd.

Die Botschaft ist klar: Der Staat will bei verschlüsselter Kommunikation mitlesen können. Begründet wird dies damit, dass nur so eine Verfolgung von Terroristen und Kriminellen möglich sei, die natürlich ebenfalls verschlüsselt kommunizieren.

Diese Forderung ist nachvollziehbar. Wenn eine richterliche Genehmigung vorliegt, ist gegen ein Mitlesen der verschlüsselten Informationen nichts einzuwenden. Das Problem ist nur, dass man dazu z.B. einen Zweitschlüssel oder eine Hintertür benötigt. Und wenn der Staat über einen solchen außerordentlichen Zugang verfügt, ist leider zu befürchten, dass über kurz oder lang auch Kriminelle, Terroristen sowie feindliche Staaten darüber verfügen werden. Das kann die Sicherheit der gesamten Internetinfrastruktur gefährden. Der Schaden, der dadurch entsteht, ist nach Ansicht von Experten bei weitem schlimmer als die fehlende Entschlüsselungsmöglichkeit der Informationen von Kriminellen und Terroristen.[10]

Dieses Dilemma ist schwer zu lösen. Interessanterweise legen die Enthüllungen u.a. von Snowden nahe, dass die Überwachung sich nicht nur gegen Terroristen und Kriminelle richtete, sondern u.a. auch dem Ziel der Wirtschaftsspionage diente.[11]

Zwei ganz wichtige Stellungnahmen zu diesem Thema – eine pro und eine contra Verschlüsselung durch die USA – werden daher hier aufgeführt.

Nachstehender Aufruf wurde am 28. Juli 2015 in der Washington Post veröffentlicht.

> »Warum die Angst vor der allgegenwärtigen Datenverschlüsselung übertrieben ist. […] Heutzutage bietet die allgegenwärtige Verschlüsselung wesentliche Sicherheit, da fast jeder ein vernetztes Gerät besitzt. Wenn Strafverfolgungs- und

10 Vgl. Abelson et al. 2015.

11 Vgl. Meister 2015.

> Geheimdienstorganisationen eine Zukunft ohne gesicherten Zugang zu verschlüsselter Kommunikation vor sich haben, werden sie Technologien und Techniken entwickeln, um ihre legitimen Missionsziele zu erreichen.«[12]

Die Autoren dieses Aufrufes sind Mike McConnell, ehemaliger Direktor der NSA und Direktor der Nationalen Nachrichtendienste, Michael Chertoff, ehemaliger US-amerikanischer Minister für Innere Sicherheit und Vorstandsvorsitzender der Chertoff Group, einer Beratungsfirma für Sicherheit und Risikomanagement und William Lynn, ehemaliger stellvertretender Verteidigungsminister und Geschäftsführer von Finmeccanica North America und DRS Technologies, einem Luft- und Raumfahrt- so wie Rüstungs-Unternehmen.

Sie unterstreichen in ihrem Aufruf, wie wichtig eine Ende-zu-Ende-Verschlüsselung in der heutigen Zeit ist. Das ist eine Verschlüsselung, bei der nur der Sender und der Empfänger Zugriff auf die verschlüsselte Nachricht haben. Ihrer Ansicht nach bedeutet jeder Eingriff des Staates in Verschlüsselungsmechanismen eine Schwächung des Schutzes von Informationen vor unbefugtem Zugriff. Für die Unterzeichner stellt die Sicherheit einer Kommunikationsinfrastruktur durch eine Ende-zu-Ende-Verschlüsselung ein höheres Gut als der Einbau staatlicher Überwachungsmöglichkeiten dar. Denn durch eine solche Ende-zu-Ende-Verschlüsselung ist eine Massenüberwachung aller Bürger nicht mehr möglich.

Gleichzeitig machen die Unterzeichner klar, dass ihrer Meinung nach der Staat Mittel und Wege finden wird, seine Ziele auch unter diesen Gegebenheiten zu erreichen.

---

12 »Why the fear over ubiquitous data encryption is overblown. […] Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.« McConnell/Chertoff/Lynn 2015.

Das Aufregende an diesem Aufruf ist, dass er nicht von irgendwelchen Bürgerrechtsbewegungen kommt, von denen man solche Statements kennt, sondern von ehemaligen hohen Regierungsvertretern. Er kommt somit aus genau den Kreisen, die derzeit massiv eine Einschränkung der Verschlüsselung fordern, damit der Staat darauf zugreifen kann.

Nachstehender Aufruf erschien am 11. August 2015 in der New York Times. Es ist sozusagen die Gegenposition zu dem vorherigen Aufruf.

> »Wenn die mobile Verschlüsselung die Gerechtigkeit aussperrt. […] Die neuen Verschlüsselungsrichtlinien von Apple und Google haben es schwieriger gemacht, Menschen vor Kriminalität zu schützen. Wir unterstützen die Datenschutzrechte von Einzelpersonen. In Ermangelung einer Zusammenarbeit von Apple und Google müssen Regulierungsbehörden und Gesetzgeber in unseren Ländern nun ein angemessenes Gleichgewicht zwischen den geringfügigen Vorteilen der Vollplattenverschlüsselung und der Notwendigkeit lokaler Strafverfolgungsbehörden zur Aufklärung und Verfolgung von Straftaten finden. Die Sicherheit unserer Gesellschaft hängt davon ab.«[13]

Bei den Unterzeichnern handelt es sich um Cyrus Vance, Staatsanwalt des Regierungsbezirks Manhattan, François Molins, leitender Pariser Staatsanwalt, Adrian Leppard, Londoner Polizeichef, und Javier Zaragoza, leitender Staatsanwalt des Obersten Gerichtshofs in Spanien.

13 »When Phone Encryption Blocks Justice. […] The new encryption policies of Apple and Google have made it harder to protect people from crime. We support the privacy rights of individuals. But in the absence of cooperation from Apple and Google, regulators and lawmakers in our nations must now find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes. The safety of our communities depends on it.« Vance Jr./Molins/Leppard/Zaragoza 2015.

Sie wenden sich gegen die Verschlüsselung der gesamten Festplatte, die Google und Apple inzwischen anbieten. Ein Zugriff der Justiz ist hier nicht mehr möglich, da Apple und Google nicht im Besitz der Schlüssel sind. Die Unterzeichner führen einen Fall an, wo der Mörder nicht gefasst werden konnte, da kein Zugriff auf die verschlüsselten Inhalte von Smartphones möglich war. Sie weisen darauf hin, dass dies kein Einzelfall war, sondern immer öfter vorkommt. Im Gegenzug dazu zitieren sie den Angriff auf Charlie Hebdo, bei dem die Daten der Smartphones entscheidend für die rasche Untersuchung dieser Terroranschläge waren. Sie fordern legale Wege, um die Verschlüsselung auf modernen Smartphones umgehen zu können.

Erwähnenswert ist in diesem Zusammenhang der Vorstoß von Susan Landau, Professorin für Politik der Cybersicherheit (*cybersecurity policy*) am Worcester Polytechnic Institute (Massachusetts). Sie plädiert dafür, dass der Staat Kapazitäten ausbauen sollte, um verschlüsselte Informationen gesetzeskonform entschlüsseln zu können. Dass eine solche Vorgehensweise durchaus erfolgversprechend sein kann, zeigt das Beispiel des Attentäters von San Bernardino. Nachdem Apple sich geweigert hatte, das FBI bei der Entschlüsselung des iPhones des Attentäters zu unterstützen, beauftragte das FBI einen professionellen Hacker, dem Vernehmen nach handelt es sich um die israelische Firma Cellebrite.[14] Diese entdeckte, so wird berichtet, einen Software-Fehler im iPhone, der letztendlich das Knacken des Handy-Zugangscodes ermöglichte, ohne dabei Daten zu verlieren. Das FBI soll dafür 1,3 Millionen Dollar bezahlt haben.[15]

Wie die New York Times vor kurzem berichtete, haben mindestens 2000 Strafverfolgungsbehörden in den USA Werkzeuge, mit denen sie sich Zugriff auf verschlüsselte Smartphones verschaffen können. Eine

14 Vgl. Israelische Firma hilft FBI angeblich beim iPhone-Hack, 2016.

15 Vgl. Eisner 2016.

solche Vorgehensweise entspricht genau dem, was Susan Landau vorgeschlagen hat.[16]

Solange es Verschlüsselung geben wird, solange werden auch die Versuche, diese auszuhebeln nicht aufhören. Derzeit besonders unter Beschuss steht die Ende-zu-Ende-Verschlüsselung, bei der nur Sender und Empfänger die Nachricht lesen können. Der Anbieter kennt die Schlüssel nicht, kann somit die Nachrichten auch nicht entschlüsseln. Ginge es nach dem Willen der Strafverfolgungsbehörden, sollten Firmen wie Apple, Facebook u.a. gezwungen werden, Verschlüsselung nur dann anzubieten, wenn sie für all diese Kommunikationen auch Nachschlüssel anfertigen, die sie den Strafverfolgern bei Bedarf aushändigen können. Entsprechende Vorschläge gibt es in den USA und auch von Seiten der Europäischen Kommission.[17] Die Umsetzung dieser Vorschläge käme einer Abschaffung der Ende-zu-Ende-Verschlüsselung gleich.

Die Forderung nach Zugang zu verschlüsselten Informationen ist eine unendliche Geschichte. Gerade erst haben Regierungsvertreter aus Amerika, Kanada, Großbritannien, Australien und Neuseeland ein Kommuniqué herausgegeben, in dem sie fordern, dass die Industrie ihnen für die Strafverfolgung den Zugriff auf verschlüsselte Inhalte ermöglicht. Indien und Japan haben sich dem Aufruf angeschlossen.[18]

Ein interessantes Beispiel, was passiert, wenn der Staat selber Verschlüsselungsdienste anbietet, ist die sogenannte deutsche De-Mail.

> »Keine Regierung ist so blöd, ihren Bürgern ein abhörsicheres Kommunikationsmedium zu geben.« (Linus Neumann)[19]

16 Vgl. Nicas 2020.

17 Vgl. Moechel 2020.

18 Vgl. »Five Eyes« fordern Zugang zu verschlüsselten Apps, 2020; International Statement: End-To-End Encryption and Public Safety, 2020.

19 Totschkas_blog 2.0, 2013.

Dies ist der sehr drastische Kommentar von Linus Neumann, Sprecher des Chaos Computer Clubs Deutschland, zur so hochgepriesenen deutschen De-Mail. Über diesen Dienst können Nutzer Nachrichten und Dokumente sicher, vertraulich und nachweisbar über das Internet austauschen.

Tatsächlich ist die De-Mail ein gutes Beispiel, wie der Staat sich Zugriff auf verschlüsselte Kommunikation verschafft.

Die De-Mail wird vom Dienstanbieter, nicht vom Kunden verschlüsselt. Sie wird zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten vom akkreditierten Dienstanbieter kurzzeitig automatisiert entschlüsselt. Über diesen Dienstanbieter kann der Staat im Bedarfsfall auf die De-Mail zugreifen. Wirklich sicher wäre eine Ende-zu-Ende-Verschlüsselung gewesen, bei der die Nachrichten auf dem Rechner des Absenders so verschlüsselt werden, dass sie erst wieder vom Empfänger auf dessen Rechner entschlüsselt werden können. Damit haben weder Provider noch Nachrichtendienste Zugriff auf den Inhalt dieser Mails. Dies war bei der De-Mail bisher nicht vorgesehen. Nach massiver Kritik an dem Konzept der De-Mail, insbesondere vom Chaos Computer Club, wird eine derartige Option tatsächlich angeboten.[20] Es ist jedoch zu befürchten, dass ein großer Teil der Nutzer der De-Mail diese zusätzliche Option nicht nutzen wird, da sie mit einem zusätzlichen Aufwand verbunden ist.

20 Vgl. Bleich 2015.

# Die gesellschaftliche Dimension von Privatheit

## Der soziale Wert von Privatheit

> »Märkte diskriminieren und sind unfair.«[1]

> »Konzerne erzeugen Kundenprofile. […] Auf Grund dieser Profile erhalten Kunden zum Beispiel sehr unterschiedliche und unterschiedlich attraktive Angebote, ohne sich dessen bewusst zu sein, dass die Angebote auf ihre gesamte finanzielle, soziale und private Situation personalisiert sind.«[2]

Um den Schutz vor solchen Diskriminierungen geht es u.a. in diesem Abschnitt. Beate Rössler, Professorin für praktische Philosophie an der Universität von Amsterdam, spricht hier von der Vermarktung der Privatsphäre und plädiert für moralische Grenzen.

Je mehr man über eine Person weiß, desto genauer kann man einschätzen, welche besonderen Vorlieben sie hat, worauf sie vermutlich reagieren wird, was ihr wichtig ist, was sie ablehnt usw. Die Vielzahl der verfügbaren Daten ermöglicht eine gezielte, individualisierte Ansprache einzelner Personen. Das wird bereits mit Erfolg bei der Werbung eingesetzt.

1 »Markets discriminate and are unfair.« Rössler 2015, S. 150.

2 »Companies generate customer's profiles. […] Because of these profiles, customers receive, for instance, very different und differently attractive offers from companies without their being aware that the offers are personalized to their overall financial, social, private situation.« Ebd., S. 151.

Nun kostet Werbung Geld, und sie soll natürlich erfolgreich sein, was bedeutet, dass sie Gewinn bringen soll. Das führt dann fast automatisch zu einer Kategorisierung der Benutzer. Diejenigen Kunden, die als gewinnversprechend eingestuft werden, werden entsprechend bevorzugt behandelt, während diejenigen, die mehr kosten, als sie bringen, in die Kategorie »waste« einsortiert werden, was so viel bedeutet wie »nicht profitabel«, »Abfall«. Diese Kunden werden wohl kaum lukrative Angebote, Rabatte oder dergleichen mehr bekommen.

Ein bekanntes Beispiel hierfür ist das US-Reiseunternehmen Orbitz, das Nutzern von Apple-Computern teurere Hotelzimmer anbot mit der Begründung, dass diese gern etwas mehr zahlen als Windows-User.[3]

Eine Untersuchung der George Washington University in Washington hat herausgefunden, dass Dienste wie z.B. Uber und Lyft, mit denen Benutzer bequem von ihrem Telefon aus Fahrten zu einem bestimmten Ort bestellen können, einen höheren Preis pro Meile für eine Reise berechnen, wenn der Abholpunkt oder das Ziel ein Viertel mit einem höheren Anteil an Bewohnern ethnischer Minderheiten ist als diejenigen mit überwiegend weißen Bewohnern.[4]

Ein weiteres Beispiel ist der Versuch von Airlines, Flugpreise erst nach der Anmeldung des Kunden individuell zu berechnen.

> »Wenn Sie also immer am Montag berufsbedingt von A nach B fliegen müssen, zahlen Sie eben etwas mehr, während der Student neben Ihnen das gleiche Ticket für den halben Preis bekommt.«[5]

Ein anderes Beispiel sei hier noch erwähnt:

3 Vgl. Apple-Nutzer zahlen mehr für Hotelzimmer, 2012.

4 Vgl. Lu 2020.

5 Schrems 2014, S. 28.

> »[Zwei Wirtschaftsauskunfteien] haben offenbar Konzepte für Datenpools entwickelt, in denen Energieversorger Informationen über Kund:innen sammeln könnten. Die Anbieter könnten die Daten nutzen, um Verbraucher:innen systematisch am Vertragswechsel zu hindern.«[6]

Durch solche Datensammlungen besteht die Gefahr einer Diskriminierung, sei es auf Grund des Kaufverhaltens, des Geschlechtes, des Alters, des Einkommens oder anderer Komponenten. Die Auswirkung einer solchen Diskriminierung mag in Bezug auf Werbung noch vergleichsweise harmlos erscheinen. Anders sieht es aus, wenn solche Daten z.B. in den Besitz von Versicherungen gelangen. Da kann es durchaus zu gravierenden Diskriminierungen und Benachteiligungen kommen, sei es, dass höhere Beiträge erhoben werden, oder sei es, dass im Extremfall sogar das Versicherungsverhältnis gekündigt wird. Ähnlich verheerend können solche Daten sein, wenn Kreditauskunfteien darauf Zugriff erhalten.

> »Die Geschichte hat uns immer wieder gezeigt, dass riesige Datenregister autokratisches Denken verstärken.« (Kate Crawford)[7]

Kate Crawford, leitende Wissenschaftlerin bei Microsoft Research, weist so auf die Risiken hin, die diese riesigen Datenregister mit sich bringen. Sie bringt Beispiele aus der Geschichte, die zeigen, welch verheerende Wirkung solche Datenregister haben können. So ermöglichte etwa IBM während der Nazizeit durch seine Hollerith-Maschinen die Verfolgung von Juden, Romas und anderen ethnischen Gruppen.[8]

6 Pekel 2020.

7 Blumencron von 2017.

8 Vgl. Solon 2017.

Wenn Donald Trump ein Register für Muslime einrichten möchte, so hält ihm Crawford entgegen, dass Facebook bereits so etwas wie ein Muslim-Register der Welt geworden ist.[9]

Crawford erwähnt Untersuchungen der Universität Cambridge, die zeigen, dass es möglich ist, die religiösen Überzeugungen der Menschen auf der Grundlage dessen, was sie im sozialen Netzwerk »liken«, vorherzusagen. Christen und Muslime wurden in 82 % der Fälle korrekt klassifiziert, und ähnliche Ergebnisse wurden für Demokraten und Republikaner erzielt (85 %).[10] Obiger Studie kann man ebenfalls entnehmen, dass man allein durch eine Analyse von Facebook Likes auch sehr genaue Aussagen machen kann über ethnische Zugehörigkeit, sexuelle Orientierung und vieles mehr.[11] Die Möglichkeit zur Diskriminierung ist hier offensichtlich.

Ein Beispiel für eine solche Diskriminierung findet man bei Facebook und Instagram. Lange Zeit konnten dort Werbetreibende ihre Anzeigen auf bestimmte Nationalitäten oder kulturelle Hintergründe zuschneiden. Das führte dazu, dass in den USA Afroamerikaner und Hispanics von Anzeigen für Jobs und Wohnungen ausgeschlossen wurden. Nach Protesten, Gerichtsverfahren und etlichen Besserungsversprechen musste die Funktion entfernt werden.[12]

Diese Datenprofile können jedoch nicht nur eine Diskriminierung zur Folge haben. Sie ermöglichen auch Manipulationen. Die Technik,

9 Vgl. Brühl/Kolb 2017.

10 »Crawford said, mentioning research from that showed it is possible to predict people's religious beliefs based on what they ›like‹ on the social network. Christians and Muslims were correctly classified in 82 % of cases, and similar results were achieved for Democrats and Republicans (85 %).« Solon 2017.

11 »We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender.« Kosinski/Stilwell/Graepel 2013.

12 Vgl. Targeted Advertising 2020.

die hier eingesetzt wird, ist das Microtargeting. Damit werden Benutzerprofile genauer erforscht und gezielte Einflussnahmen organisiert.

Beate Rössler, Professorin für praktische Philosophie an der Universität von Amsterdam, warnt eindringlich vor den Möglichkeiten einer Manipulation aufgrund der detaillierten Datenprofile.

> »Je genauer die Profile sind, die auf Millionen von personenbezogenen Daten basieren, um so vorhersehbarer und anfälliger sind die betreffenden Personen für eine Manipulation.«[13]

Eine Manipulation der Entscheidung zum Brexit oder der Wahl von Donald Trump durch Cambridge Analytica mag zurzeit in den Bereich der Spekulation fallen. Doch könnte es durch die Verwendung von tausenden von Datenpunkten in einigen Jahren tatsächlich möglich sein, die Ansichten von Menschen zu manipulieren. Dies ist für Crawford durchaus realistisch.[14]

> »Privatsphäre hat auch einen sozialen Wert. Wenn sie das Individuum schützt, tut sie dies um der Gesellschaft willen.«[15]

Folgen wir der Argumentation von Daniel Solove, Professor an der juristischen Fakultät der George Washington Universität und vehemen-

13 »Then it is probable that the more precise the profiles, based on millions of personal data, the more predictable and susceptible to manipulation the subject becomes.« Rössler 2015, S. 141.

14 »Crawford was skeptical about giving Cambridge Analytica credit for Brexit and the election of Donald Trump, but thinks what the firm promises – using thousands of data points on people to work out how to manipulate their views – will be possible ›in the next few years‹.« Solon 2017.

15 »Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. […] We protect individual privacy as a society because we recognize that a good society protects against excessive intrusion and nosiness into people's lives. […] Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society.« Solove 2015, S. 79-80.

ter Kämpfer für den Erhalt der Privatsphäre, so sollte eine Gesellschaft nicht nur vor Diskriminierung und Manipulation schützen, sondern auch vor übermäßiger Zudringlichkeit und der Neugierde anderer.

Seiner Ansicht nach ist Privatsphäre zu haben ein Stück Lebensqualität, die eine Gesellschaft ermöglichen sollte. Indem eine Gesellschaft individuelle Rechte schützt, entscheidet sie sich dazu, sich als Gesellschaft zurückzunehmen, um so einen Freiraum zu schaffen, in dem der Einzelne gedeihen kann. Eine Gesellschaft ohne Privatsphäre wäre erdrückend. Sie wäre wohl kaum der Ort, an dem man leben wollte.

## Privatheit und Demokratie

> »Privatheit ist eine wichtige Bedingung für Demokratie, Rechtsstaatlichkeit und informationelle Selbstbestimmung.«[16]

Obigen Satz findet man auf der Homepage des Forums Privatheit. Das Forum wirbt dort für ein selbstbestimmtes Leben in einer digitalen Welt.

Den Hinweis, dass der Schutz der Privatsphäre von entscheidender Bedeutung für das Bestehen einer Demokratie ist, findet man immer wieder, und das nicht nur in der heutigen Zeit.

> »Die Wahrung der Privatsphäre ist entscheidend für einen demokratischen politischen Prozess.«[17]

Dieser Satz stammt aus dem Buch »Privacy On The Line«. Er ist sehr ernst zu nehmen, denn die Autoren Whitfield Diffie, dem Mitbegründer des sogenannten Diffie-Hellman-Schlüsselaustausch, einer

16 Forum Privatheit 2020.

17 »Preservation of privacy is critical to a democratic political process.« Whitfield/Landau 2007, S. 170.

bahnbrechenden Erfindung in der Kryptographie, die den sicheren Austausch kryptographischer Schlüssel über eine unsichere Verbindung ermöglicht, und Susan Landau, die nicht nur – wie bereits erwähnt – Professorin für Politik der Computer- und Netzsicherheit am Worcester Polytechnic Institute (Massachusetts), sondern auch Visiting Professor of Computer Science am University College London ist, sind Experten auf diesem Gebiet.

Sie begründen ihre Aussage damit, dass Änderungen oft zaghaft beginnen, und eine politische Diskussion häufig im privaten Bereich startet. Für Journalisten gilt, dass sie im privaten Bereich aktiv sein müssen, wenn sie Quellen schützen wollen. Und Anwälte können ihre Klienten nicht wirklich verteidigen, wenn ihre Kommunikation nicht geschützt ist.[18]

> »Die Privatsphäre wird geschützt, weil sie für die Freiheit und das Streben nach Glück unerlässlich ist. Unsere Verfassung prüft die Macht der Regierung zum Schutz der Rechte von Einzelpersonen, damit alle unsere Bürger in einer freien und gerechten Gesellschaft leben können. Im Gegensatz zu totalitären Staaten glauben wir nicht, dass eine Regierung ein Monopol auf die Wahrheit hat.«[19]

18 »Change often begins most tentatively, and a political discussion often starts in private. Journalists need to operate in private when cultivating sources. Attorneys cannot properly defend their clients if their communications are not privileged.« Whitfield/Landau 2007, S. 170.

19 »Personal privacy is protected because it is essential to liberty and the pursuit of happiness. Our Constitution checks the power of Government for the purpose of protecting the rights of individuals, in order that all our citizens may live in a free and decent society. Unlike totalitarian states, we do not believe that any government has a monopoly on truth.« Final Report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1976, S. 290.

Es ist beeindruckend, wie aktuell obige Aussage ist, obwohl sie bereits 1976 gemacht wurde. Diese Zeilen stammen aus dem Abschlussbericht des Church Committee. Das Church Committee war ein Sonderausschuss des US-Senats zur Untersuchung des Regierungshandelns mit Bezug zu Aktivitäten der Nachrichtendienste (u.a. geheime Operationen zur Ermordung ausländischer Staatschefs und Putsche). Den Vorsitz dieses Ausschusses hatte Senator Frank Church.[20]

Dieses Church Committee hat bereits 1976 darauf hingewiesen, wie wichtig der Schutz der Privatsphäre für eine freie demokratische Gesellschaft ist.

Dieses Committee untersuchte auch, inwieweit die Rechte amerikanischer Bürger durch die Techniken der Geheimdienste verletzt wurden. Sein Bericht liest sich wie ein Lehrstück in Bürgerrechte und Demokratie.

> »Wir haben gesehen, dass Teile unserer Regierung in ihren Einstellungen und Handlungen Taktiken anwenden, die einer Demokratie nicht würdig sind und gelegentlich an die Taktiken totalitärer Regime erinnern.«[21]

Während des Kalten Krieges verwendeten die Geheimdienste verdeckte Techniken, die in die Privatsphäre eindrangen, um ihr vages, unkontrolliertes und zu weit gefasstes Mandat zum Sammeln von Informationen auszuführen.[22]

Das Wesen der Demokratie ist der Glaube, dass das Volk frei sein muss, um Entscheidungen über Fragen der öffentlichen Ordnung zu

---

20 Vgl. Church Committee 2019. (Siehe hierzu auch das Kapitel »No Place to Hide«.)

21 »We have seen segments of our Government, in their attitudes and action, adopt tactics unworthy of a democracy, and occasionally reminiscent of the tactics of totalitarian regimes.« Final Report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1976 S. 3.

22 »Throughout the cold war period, the intelligence agencies used covert techniques which invaded personal privacy to execute their vague, uncontrolled, and overly broad mandate to collect intelligence.« Ebd., S. 58.

treffen. Die Maßnahmen des FBI störten den demokratischen Prozess, da die Einstellungen des Präsidiums zum sozialen Wandel zu der Überzeugung führten, dass ein solches Eingreifen Teil seiner Verpflichtung zum Schutz der Gesellschaft war. Wenn eine Regierungsbehörde heimlich versucht, dem amerikanischen Volk ihre Ansichten darüber aufzuzwingen, was richtig ist, wird der demokratische Prozess untergraben.[23]

In einem Fernsehinterview äußert sich Church noch sehr viel drastischer zu diesem Thema:

> »Sollte dieser Staat jemals zu einer Tyrannei werden, […] dann könnten ihn die von den Geheimdiensten entwickelten technischen Möglichkeiten in die Lage versetzen, eine totale Schreckensherrschaft zu errichten, und man könnte nichts dagegen unternehmen, weil auch selbst der umsichtigste Versuch, sich zum Widerstand zu vereinen […] dem Staat zur Kenntnis kommen würde. So groß ist die Macht dieser Techniken.«[24]

Die Bedrohung, die von den Geheimdiensten ausgeht, hat Senator Frank Church bereits 1975 erkannt.[25] Die Bedeutung seiner Worte hat damals wohl niemand begriffen.

---

23 »The essence of democracy is the belief that the people must be free to make decisions about matters of public policy. The FBI's actions interfered with the democratic process, because attitudes within the Bureau toward social change led to the belief that such intervention formed a part of its obligation to protect society. When a governmental agency clandestinely tries to impose its views of what is right upon the American people, then the democratic process is undermined.« Ebd., S. 226.

24 Greenwald 2015, S. 292. »He [Senator Frank Church] added that if a dictator ever took over, the N.S.A. ›could enable it to impose total tyranny, and there would be no way to fight back‹.« Senator Frank Church in einem Interview des Fernsehmagazins »Meet the Press«, Bamford 2005.

25 Siehe dazu auch vorhergehende Abschnitte dieses Kapitels.

Eine Warnung, die in die gleiche Richtung geht, findet man in der Abschiedsrede von Dwight Eisenhower, Präsident der USA 1953-1961, aus dem Jahr 1961.

> »Wir müssen auf der Hut sein vor unberechtigten Einflüssen des militärisch-industriellen Komplexes, ob diese gewollt oder ungewollt sind. Die Gefahr für ein katastrophales Anwachsen unbefugter Macht besteht und wird weiter bestehen. Wir dürfen niemals zulassen, dass das Gewicht dieser Kombination unsere Freiheiten oder unseren demokratischen Prozess bedroht. […] Nur eine aufmerksame und kenntnisreiche Bürgerschaft kann eine angemessene Verbindung der riesigen industriellen und militärischen Maschinerie der Verteidigung mit unseren friedlichen Zielen und Methoden sicherstellen, so dass Sicherheit und Freiheit zusammen gedeihen können.«[26]

Bemerkenswert an dieser Rede aus dem Jahre 1961 ist die Warnung vor dem militärisch-industriellen Komplex, der sich heute z.B. in der engen Verbindung zwischen US-Nachrichtendiensten, der US-Armee und den IT-Unternehmen des Silicon Valley manifestiert.[27]

Auch in neuerer Zeit fehlt es nicht an Warnungen vor Angriffen auf die Demokratie. So beschreiben bei der Laudatio zum BigBrother-Award 2013 in der Kategorie Globales Datensammeln, der an Google ging, Rena Tangens & padeluun die Gefahr, die u.a. von Google für die Demokratie ausgeht:

> »Wer sich ständig beobachtet fühlt und annimmt, dass die gespeicherten Informationen ihm oder ihr irgendwann schaden könnten, wird zögern, Grundrechte wie freie Meinungsäuße-

26 Gerste 2011. Deutsche Übersetzung der Abschiedsrede von Präsident Eisenhower. Ploppa 2016. Die Abschiedsrede von Präsident Eisenhower im Original: Eisenhower's Farewell Address to the Nation, 1961.

27 Vgl. Leisegang 2015.

> rung oder Versammlungsfreiheit wahrzunehmen. Wenn das passiert, ist das keine Privatsache mehr, sondern das schadet der Allgemeinheit und einer lebendigen Demokratie.«[28]

Die hier angeführten Argumente dafür, dass die globale Überwachung die Demokratie gefährdet, gehören zu den ganz fundamentalen Aussagen, mit denen immer wieder für mehr Privatheit und weniger Überwachung aufgerufen wird.

Ein weiterer ganz wesentlicher Bestandteil für Demokratie sind u.a. freie und faire Wahlen.[29] Jede Beeinflussung von Wählern ist damit eine Gefahr für die Demokratie. Heute wissen wir, dass die Chance, Personen zu kontrollieren und zu beeinflussen umso größer ist, je mehr private Details man von diesen Personen besitzt. Genau diese Form von Beeinflussung erleben wir heute in ganz großem Stil, und das nicht nur bei den amerikanischen Präsidentschaftswahlen 2016 und bei der Abstimmung zum Brexit. Bei Letzterem basierte die Arbeit von Cambridge Analytica auf den privaten Daten von ca. 87 Millionen Facebook-Nutzern, die illegal beschafft wurden. Für die Möglichkeit, Kunden zu beeinflussen – und das können natürlich auch Wähler sein – warb Cambridge Analytica auf seiner Homepage:

> »Wir sammeln Daten aus öffentlichen Quellen und seriösen Datenanbietern und kombinieren sie mit Ihren eigenen Daten, um tiefere und umfassendere Erkenntnisse zu gewinnen. Diese Datenbestände werden dann zentralisiert, damit

28 Der BigBrotherAward in der Kategorie Globales Datensammeln geht an Larry Page, Sergey Brin und Eric Schmidt, die Gründer und Verwaltungsrat der Google Inc. 2013.

29 Vgl. Demokratie: die erfolgreichste Staatsform, 2020.

> Sie Ihre Kunden schnell und effizient finden und überzeugen können.«[30]

Der Verhaltensforscher Robert Epstein vom American Institute for Behavioral Research and Technology in Kalifornien hat in einer Studie den Einfluss von Suchmaschinen auf Wahlverhalten untersucht und kommt dabei zu dem Schluss:

> »Unsere Untersuchung legt nahe, dass, selbst wenn Google nicht absichtlich Wahlen manipuliert, die Suchalgorithmen des Konzerns seit Jahren die Gewinner von Wahlen auf der ganzen Welt bestimmen, mit wachsendem Einfluss jedes Jahr.« (Robert Epstein)[31]

Die Einflussmöglichkeiten großer Internetkonzerne und vor allem der Sozialen Netzwerke nicht nur auf Wahlergebnisse ist erschreckend.

> »Algorithmen entscheiden, wer die Macht hat, sie wirken als mächtige Verstärker und können einen Bias, eine Mehrheitsumkehr, herbeiführen. […] ›Es wird immer einen Bias geben‹, […] doch das eigentliche Problem, das noch nie zuvor in diesem Ausmaß existierte, ist, dass der Bias über mächtige Einflussquellen auftritt, die komplett in privater Hand sind, ohne öffentliche Verantwortbarkeit und Transparenz.«[32]

> »Menschen müssen auch verstehen, dass Demokratie kein Zuschauersport ist. Du musst mitmachen und aktiv sein, und das

30 »We collect data from public sources and reputable data providers and combine it with your own data to produce deeper and richer insights. These data assets are then centralized to help you find and persuade your customers quickly and efficiently.« Cambridge Analytica 2018.

31 Lobe 2015.

32 Lobe 2015.

> kontinuierlich, um sicher zu stellen, dass Du deine Rechte und Freiheiten behältst.«[33]

> »Dass etwas von so gewaltigen Dimensionen – die Umwandlung des Internets in ein Reich der Massenüberwachung, die Schaffung des größten je dagewesenen Systems der Überwachung ohne Anfangsverdacht – vollkommen im Dunkeln vollzogen werden konnte, ließ die Demokratie illusorisch erscheinen.«[34]

Das letztgenannte Zitat findet man im Vorwort der Taschenausgabe des Buches »Die globale Überwachung« von Glenn Greenwald. Der Autor berichtet darin über die illegalen Praktiken der amerikanischen Geheimdienste anhand der Unterlagen des Whistleblowers Edward Snowden. Insofern kann man dieses Buch auch als einen Beitrag zur Erhaltung der Demokratie verstehen, da Greenwald schonungslos aufdeckt, was die Demokratie gefährdet.

Die Enthüllungen von Snowden über die Überwachungspraktiken der amerikanischen Geheimdienste hat weltweit für Empörung gesorgt. Es erfolgte ein Aufschrei gegen diese Überwachungsaktivitäten.

Die Snowden-Dokumente sind ein ganz wichtiger Meilenstein im Kampf gegen Überwachung. Dieser Kampf ist damit aber nicht beendet. Er muss fortgesetzt werden.

> »Democracy Dies in Darkness.«[35]

Dieser Slogan, den man derzeit auf der Homepage der Washington Post findet, unterstreicht die Bedeutung des obigen Zitates von Glenn Greenwald.

---

33 William Binney, ehemaliger Technischer Direktor der NSA. Zitat aus dem Dokumentarfilm »Nothing to Hide« (1:17:56).Nothing to Hide – Dokumentarfilm 2017.

34 Greenwald 2015, S. 10-11.

35 Homepage der Washington Post.

# Freiheit versus Sicherheit

> »Wir müssen generell, um uns selbstbestimmt verhalten zu können, daran glauben und davon ausgehen können, dass wir nicht beobachtet werden, belauscht, getäuscht über die Weitergabe und die Erfassung von Daten, über die Anwesenheit von Personen und darüber, was anwesende Personen von uns wissen und ›wer‹ sie deshalb ›für uns‹ sind.«[1]

Das ist die Freiheit, die es zu verteidigen gilt: Sich frei fühlen zu können, indem man sicher sein kann, dass das eigene Verhalten nicht beobachtet und kontrolliert wird, dass man nicht kategorisiert und manipuliert wird. Diese Form von Freiheit basiert ganz wesentlich auf dem Schutz unserer Privatsphäre. Je weniger man über uns weiß, desto weniger Einfluss- und Kontrollmöglichkeiten gibt es. Privatheit wird damit zum Schutz vor Angriffen auf eben diese Freiheit. Hingegen bedeutet jeder Eingriff in die Privatsphäre ein Verlust an Freiheit und schränkt unsere Autonomie ein.

Viele Einschränkungen dieser unserer Freiheit werden mit dem Versprechen erhöhter Sicherheit begründet. Insbesondere Terroranschläge werden gerne als Anlass dafür genommen. Allerdings sollte man bedenken, dass es auch künftig Anschläge geben wird und dass jedes Mal die Grundrechte weiter eingeschränkt werden, ohne dass dadurch ein Gefühl größerer Sicherheit entstünde.[2]

1 Rössler 2001, S. 211.

2 Vgl. Ali 2016.

Zu diesen Einschränkungen zählen eine Intensivierung der Überwachung, Erfassung immer weiterer Daten wie z.B. Reisedaten, die Einsicht ins Bankkonto, Kreditkartendaten etc. sowie weitere zusätzliche Kontrollen. Besonders im Fokus steht hier auch die Kommunikation wie die Handydaten, die Telefonkontakte und der E-Mail-Verkehr, deren Schutz systematisch versucht wird, auszuhöhlen. Der gläserne Bürger ist das Wunschziel nicht nur des Staates, und diesem Ziel kommt er immer näher. Dabei weiß kaum jemand, was genau über ihn gespeichert ist. Ein Anwender hat seinerzeit von der Telekom die Herausgabe der gespeicherten Telekommunikations-Verkehrsdaten verlangt. Was er damals geliefert bekam, war für ihn die Überwachung unseres Alltags.[3]

Privatheit bietet zumindest einen gewissen Schutz vor Überwachung, Kontrolle und Manipulation. Doch der Ruf nach mehr Sicherheit ist einer ihrer größten Gegner. Zwar kann es weder grenzenlose Freiheit, noch kann es absolute Sicherheit geben. Aber der Fokus verschiebt sich derzeit doch eher in Richtung Sicherheit und damit weg von der Privatheit. Insofern ist die Frage »Freiheit oder Sicherheit?« eine der zentralen Fragen unserer heutigen Gesellschaft.

Es sei hier erinnert an den berühmten Spruch von Benjamin Franklin, der heute noch so aktuell ist wie seinerzeit.

> »Wer wesentliche Freiheiten aufgibt, um ein wenig vorübergehende Sicherheit zu gewinnen, hat weder Freiheit noch Sicherheit verdient«. (Benjamin Franklin)[4]

Jeder muss selbst entscheiden, wie viel Einsatz ihm seine Privatsphäre wert ist. Hilfreich mag hier die folgende Empfehlung sein:

---

3 Vgl. Spitz 2015.

4 »Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.« Volokh 2014.

> »Wer Freiräume wahren will, muss Chancen und Gefahren wahrnehmen – und seine Entscheidungen treffen. […] Der Schlüssel zu einer guten Balance aus Privatsphäre und Sicherheit heißt Eigenverantwortung und kritisches, eigenständiges Denken.«[5]

Es gibt den wunderbaren Leitspruch der Erinnerungsstätte für die Freiheitsbewegungen der deutschen Geschichte in Rastatt (Revolution von 1848):

> »Ewige Wachsamkeit ist der Preis der Freiheit.«[6]

Es bleibt zu hoffen, dass diese Wachsamkeit nicht ausstirbt.

5 Lotter 2017, S. 9.

6 Dieser Leitspruch ist zitiert in einem Vortrag von Prof. Dr. Jutta Limbach anlässlich des Festaktes ›150 Jahre Demokratische Revolution‹ am 27. Februar 1998 in Mannheim, dessen Manuskript mir die Autorin freundlicherweise zur Verfügung gestellt hat.Siehe auch: Das Bundesarchiv 2020.

# Literaturverzeichnis

## Monographien und Artikel aus Zeitschriften


Abelson, H./Anderson, R./Bellovin, S./Benalo, J./Blaze, M./Diffie, W./Weitzner, D. (2015): »Keys Under Doormats«. In: Journal of Cybersecurity 1.1, S. 69-7. Abgerufen am 16.09.2020 von https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Ali, A. H. (18.04.2016): »Wie kann der Westen westlich bleiben?«. In: FAZ Nr. 90, S. 11.

Anderson, R. (2017): »The Threat A Conversation With Ross Anderson«. In: Edge. Abgerufen am 15.11.2020 von https://www.edge.org/conversation/ross_anderson-the-threat?source=post_page.

Bähr, J. (23.09.2015): »Schrems' jahrelanger Kampf gegen Facebook«. In: FAZ. Abgerufen am 15.November 2020 von https://www.faz.net/aktuell/feuilleton/medien/max-schrems-jahrelanger-kampf-gegen-facebook-13819522.html.

Ballweber, J. (14.09.2020): »Deutsche Verwaltung nutzt Microsoft-Produkte nicht rechtskonform«. In: Netzpolitik.org. Abgerufen am 15.11.2020 von https://netzpolitik.org/2020/datenschutzkonferenz-deutsche-verwaltung-nutzt-microsoft-produkte-nicht-rechtskonform/#vorschaltbanner.

Bamford, J. (25.12.2005): »The Agency That Could Be Big Brother«. In: The New York Times. Abgerufen am 12.09.2020 von https://www.nytimes.com/2005/12/25/weekinreview/the-agency-that-could-be-big-brother.html?_r=0.

Beiersmann, S. (15.11.2018): »Niederlande: Sammlung von Microsoft-Office-Telemetriedaten verstößt gegen DSGVO«. In: ZDNet. Abgerufen am 26.11.2020 von https://www.zdnet.de/88347263/.

Biermann, K. (19.11.2013): »Stromkunden sollen sich überwachen lassen – und dafür zahlen«. In: DIE ZEIT. Abgerufen am 15.11.2020 von https://www.zeit.de/digital/datenschutz/2013-11/smart-meter-teuer-daten-vermarkten/komplettansicht.

Bleich, H. (22.04.2015): »De-Mail: Ende-zu-Ende-Verschlüsselung mit PGP gestartet«. In: heise online. Abgerufen am 15.11.2020 von https://www.heise.de/security/meldung/De-Mail-Ende-zu-Ende-Verschluesselung-mit-PGP-gestartet-2616388.html.

Bloomberg (08.07.2020): »Die größten Unternehmen der Welt nach Börsenkapitalisierung«. In: FAZ 156, S. 21.

Blumencron von, M. (16.03.2017): »Trumps neues Menschenregister«. In: FAZ. Abgerufen am 15.11.2020 von https://www.faz.net/aktuell/politik/wahl-in-amerika/usa-legen-riesige-datenregister-ueber-ihre-buerger-an-14927850.html?printPagedArticle=true#pageIndex_2.

Boehring, J. (19.11.2018): »Datenschutz-Folgenabschätzung zeigt hohe Risiken bei Microsoft Office ProPlus Enterprise«. In: Privacy Company. Abgerufen am 15.11.2020 von https://www.privacycompany.de/datenschutz-folgenabschatzung-zeigt-risiken-bei-microsoft-office-proplus-enterprise/.

Bohsem, G. (15.11.2016): »Die großen Fragen«. In: Süddeutsche Zeitung. Abgerufen am 15.11.2020 von https://www.sueddeutsche.de/wirtschaft/nahaufnahme-die-grossen-fragen-1.3034720.

Bordel, S. (18.11.2018): »Microsoft Office sammelt mehr Daten als gedacht und verstösst gegen die DSGVO«. In: Computerworld. Abgerufen am 06.09.2020 von https://www.computerworld.ch/business/datenschutz/microsoft-office-sammelt-daten-gedacht-verstoesst-dsgvo-1625749.html.

Brühl, J./Kolb, M. (16.03.2017): »Träumen Faschisten von Algorithmen?« In: Süddeutsche Zeitung. Abgerufen am 16.11.2020 von https://

www.sueddeutsche.de/digital/tech-festival-sxsw-traeumen-faschisten-von-algorithmen-1.3422870.

BVerfG (05.12.1983): »Urteil des Ersten Senats vom 15.12.1983 – 1 BvR 209/83 –, Rn. 1-215«. Abgerufen am 2.09.2020 von https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html.

BVerfG (27.02.2008): »Urteil des Ersten Senats vom 27.02.2008 – 1 BvR 370/07 –, Rn. 1-333«. Abgerufen am 02.09.2020 von www.bverfg.de/e/rs20080227_1bvr037007.html.

BVerfG Pressemitteilung (27.02.2008): »Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung und zur Aufklärung des Internet nichtig«. Abgerufen am 02.09.2020 von https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2008/bvg08-022.html#Start.

BVerwG 1 (25.09.2019): »Beschluss vom 25.09.2019 – BVerwG 6 C 12.18.« Abgerufen am 23.09.2020 von https://www.bverwg.de/250919B6C12.18.0.

BVerwG. Pressemitteilung (25.09.2019): »EuGH soll Vereinbarkeit der deutschen Regelung zur Vorratsdatenspeicherung mit dem Unionsrecht klären«. Abgerufen am 20.10.2020 von https://www.bverwg.de/pm/2019/66.

Chow, R. (2017): »The Last Mile for IoT Privacy«. In: IEEE Security & Privacy 15.6 (November-Dezember), S. 73-76.

Christl, W./Spiekermann, S. (2016): *Networks of Control*. Wien: Facultas.

Conti, G. (2008): *Googling Security*. Boston: Addison Wesley.

Crowe, A./Lee, S./Verstraete, M. (17.06.2015)» Securing Safe Spaces Online«. Abgerufen am 15.11.2020 von https://privacyinternational.org/sites/default/files/2018-02/Securing%20Safe%20Spaces%20Online_2_0.pdf.

Der Europäische Datenschutzbeauftragte (08.04.2019): »EDPS investigates contractual agreements concerning software used by EU institutions.« Abgerufen am 13.09.2020 von https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-contractual-agreements.de.

Drösser, C. (10.03.2016): »Ermittler vor gesperrtem Smartphone«. In: DIE ZEIT 10, o.S.

Dr. Datenschutz (27.07.2015): »Internet der Dinge« im Einklang mit Datenschutz? Abgerufen am 13.09.2020 von https://www.dr-datenschutz.de/internet-der-dinge-im-einklang-mit-datenschutz/.

Eisner, A. (22.04.2016): »1,3 Millionen für nichts: So macht sich das FBI vor Apple lächerlich«. In: Chip. Abgerufen am 16.09.2020 von https://www.chip.de/news/13-Millionen-fuer-nichts-So-macht-sich-das- FBI-vor-Apple-laecherlich_90083607.html.

Enzensberger, H. (28.02.2014): »Enzensbergers Regeln für die digitale Welt. Wehrt Euch!«. In: FAZ. Abgerufen am 17.11.2020 von https://www.faz.net/aktuell/feuilleton/debatten/enzensbergers-regeln-fuer-die-digitale-welt-wehrt-euch-12826195.html.

Esguerra, R. (10.12.2009): »Google CEO Eric Schmidt Dismisses the Importance of Privacy«. In: EFF. Abgerufen am 12.09.2020 von https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.

Faber, H. (30.09.2001): »Was war. Was wird«. In: heise online. Abgerufen am 09.09.2020 von https://www.heise.de/newsticker/meldung/Was-war-Was-wird-50185.html.

Fanta, A./Kamps, L. (2020): »EU möchte europäische Datenräume schaffen«. In: Netzpolitik.org. Abgerufen am 25.11.2020 von https://netzpolitik.org/2020/data-governance-verordnung-eu-moechte-europaeische-datenraeume-schaffen/.

Fenwick, W./Brownstone, R. (2003): »Electronic Filing: What Is It – What Are Its Implications?«. In: Santa Clara High Technology Law Journal, 19.1, S. 181-227. Abgerufen am 10.09.2020 von https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1317&context=chtlj.

Fichtner, L. (2016): »Techno-Politics as Network(ed) Struggles«. In: FifF-Kommunikation 1, S. 50-54. Abgerufen am 17.11.2020 von https://www.fiff.de/publikationen/fiff-kommunikation/fk-2016/fk-2016-1/fk-2016-1-content/fk-2016-1-p50.pdf.

Fowler, G. A. (28.05.2019): »It's the middle of the night. Do you know who your iPhone is talking to?«. In: The Washington Post. Abgerufen am 05.09.2020 von https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/.

Gajda, A. (2008): »What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to The Right to Privacy«. In: Michigan State Law Review 2008.1, S. 1-37. Abgerufen am 18.11.2020 von https://ssrn.com/abstract=1026680.

Gerste, R. (18.01.2011): »Eisenhowers Warnung vor einem Staat im Staat«. In: NZZ. Abgerufen am 25.11.2020 von https://www.nzz.ch/eisenhowers_warnung_vor_einem_staat_im_staat-1.9130929.

Giordano, M. (19.10.2018): »Hier findest du alle Daten, die Apple über dich gesammelt hat«. In: Welt. Abgerufen am 18.11.2020 von https://www.welt.de/kmpkt/article182295764/Hier-findest-du-alle-Daten-die-Apple-ueber-dich-gesammelt-hat.html.

Grassegger, H. (11.06.2020): »(Er)Lösung dank Technik«. In: Das Magazin 28, S. 1-5.

Greenberg, A. (05. 05.2016): »A Car's Computer Can ›Fingerprint‹ You in Minutes Based on How You Drive«. In: Wired. Abgerufen am 17.11.2020 von https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/.

Greenwald, G. (2014): *No Place to Hide*. New York: Picador.

Greenwald, G. (2015): *Die globale Überwachung*. München: Knaur, deutschsprachige erweiterte Taschenbuchausgabe.

Greif, B. (21.07.2016): »Französische Datenschutzbehörde CNIL mahnt Microsoft wegen Windows 10 ab«. In: ZDNet. Abgerufen am 18.11.2020 von www.zdnet.de/88275135/franzoesische-datenschutzbehoerde-cnil-mahnt-microsoft-wegen-windows-10-ab.

Grossman, W. (09.06.2016): »Democracy, film review: How the EU's data protection law was made«. In: ZDNet. Abgerufen am 13.09.2020 von https://www.zdnet.com/article/democracy-film-review-how-the-eus-data-protection-law-was-made/.

Gurevich, Y., Hudis, E./Wing, J. (07.07.2016): »Inverse Privacy«. In: Communications of the ACM 5, S. 38-42.

Hassemer, W. (14.05.2001): »Informationssicherheit als Staatsaufgabe«. Abgerufen am 08.09.2020 von http://2014.kes.info/archiv/material/bsikongress2001/hassemer.htm.

Haupt, F. (2010): »Privatsphäre, sagt Zuckerberg, ist nicht mehr zeitgemäß«. In: FAZ. Abgerufen am 25.11.2020 von https://www.faz.net/aktuell/feuilleton/buecher/rezensionen/sachbuch/ben-mezrich-the-accidental-billionaires-privatsphaere-sagt-zuckerberg-ist-nicht-mehr-zeitgemaess-1985365-p2.html.

Heller, P. (07.05.2017): »Alexa, War Es Mord?«. In: Frankfurter Allgemeine Sonntagszeitung, S. 59.

Hern, A. (23.07.2019): »›Anonymised‹ data can never be totally anonymous, says study«. In: The Guardian. Abgerufen am 18.11.2020 von https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.

Heuzeroth, T. (13.04.2014): »Deutsche unterschätzen den Wert persönlicher Daten«. In: Die Welt. Abgerufen am 11.09.2020 von https://www.welt.de/wirtschaft/article126882276/Deutsche-unterschaetzen-den-Wert-persoenlicher-Daten.html.

Hill, J. (22.11.2018): »SNCF auf dem Weg zum digitalen Mobility-Service-Provider.« In: Computerwoche. Abgerufen am 18.11.2020 von https://www.computerwoche.de/a/sncf-auf-dem-weg-zum-digitalen-mobility-service-provider-von-morgen,3546146,2.

Janker, K. (26.11.2014): »Wir werden manipulierbar und unfrei«. In: Süddeutsche Zeitung. Abgerufen am 13.09.2020 von https://www.sueddeutsche.de/kultur/juli-zeh-ueber-das-generali-modell-wir-werden-manipulierbar-und-unfrei-1.2232147.

Jasen, G. (06.01.2016): »Cybersecurity Experts Debate Proper Response to Terrorism«. Abgerufen am 06.09.2020 von https://news.columbia.edu/news/cybersecurity-experts-debate-proper-response-terrorism.

Kanning, T. (26.08.2016): »Mit dem Herzschlag ins Bankkonto«. In: FAZ 199, S. 25.

Kaeser, E. (06.11.2018): »Die Religion der Herde – Facebook, mit Nietzsche betrachtet«. In: NZZ. Abgerufen am 18.11.2020 von https://www.nzz.ch/meinung/facebook-mit-nietzsche-betrachtet-die-religion-der-herde-ld.1429269.

Kosinski, M./Stilwell, D./Graepel, T. (09.04.2013): »Private traits and attributes are predictable from digital records of human behavior«. Abgerufen am 18.11.2020 von https://www.pnas.org/content/110/15/5802.

Küchemann, F. (10.05.2014): »Facebook verkauft seine Nutzer«. In: FAZ 108, S. 17.

Kuneva, M. (31.03.2009): »Roundtable on Online Data Collection, Targeting and Profiling«. Abgerufen am 08.09.2020 von https://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

Kurz, C. (28.06.2016): »SIM-Karten werden bald lückenlos überwacht«. In: FAZ. Abgerufen am 18.11.2020 von https://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/anti-terror-reform-uebergrosse-koalition-14309752.html.

Kurz, C. (29.10.2018): »Der Spion, der mit dem Smartphone kam«. In: FAZ. Abgerufen am 18.11.2020 von https://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/wer-bekommt-die-daten-die-die-apps-sammeln-15860984.html.

Landau, S. (01.03.2016): »Testimony for House Judiciary Committee Hearing on »The Encryption Tightrope: Balancing Americans' Security and Privacy««. Abgerufen am 15.11.2020 von https://docs.house.gov/meetings/JU/JU00/20160301/104573/HHRG-114-JU00-Wstate-LandauS-20160301.pdf.

Landau, S. (13.01.2017): »WPI's Susan Landau On What the FBI Needs to Learn About Security«. Abgerufen am 15.11.2020 von https://www.wpi.edu/news/wpi-s-susan-landau-what-fbi-needs-learn-about-security.

Langer, M.-A. (22.07.2019): »Ausspioniert vom eigenen Internet-Browser«. In: NZZ. Abgerufen am 18.11.2020 von https://www.nzz.ch/panorama/ausspioniert-vom-eigenen-internet-browser-ld.1497200?mktcid=nled&mktcval=101&kid=nl101_2019-7-22.

Lanier, J. (2014): *Wem gehört die Zukunft?*. Hamburg: Hoffmann und Campe.

Leisegang, D. (2015): »Der cyber- militärische Komplex«. In: Wissenschaft & Frieden 2015.2: Technikkonflikte, S. 27-30. Abgerufen am 19.09.2020 von https://www.wissenschaft-und-frieden.de/seite.php?artikelID=2042.

Lepore, J. (24.06.2013): »Privacy in an age of publicity«. In: Annals of Surveillance. In: The New Yorker. Abgerufen am 18.11.2020 von https://www.newyorker.com/magazine/2013/06/24/the-prism.

Levine, R. (09.10.2015): »Behind the European Privacy Ruling That's Confounding Silicon Valley«. In: The New York Times. Abgerufen am 18.11.2020 von https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html.

Lobe, A. (2014): »Online-Konzerne als Entwicklungshelfer«. In: FAZ. Abgerufen am 18.11.2020 von https://www.faz.net/aktuell/feuilleton/medien/gratis-internet-google-als-entwicklungshelfer-13745099/die-welt-dreht-sich-mal-wieder-13745188.html.

Lobe, A. (06.08.2015): »Im Netz der Wahlkampfhelfer«. In FAZ. Abgerufen am 18.11.2020 von https://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/algorithmen-beeinflussen-politische-willensbildung-13735791.html?printPagedArticle=true#pageIndex_3.

Lobe, A. (27.07.2017): »Der Spion im Fernseher«. In: Wiener Zeitung. Abgerufen am 18.11.2020 2020 von https://www.wienerzeitung.at/nachrichten/kultur/medien/888347-Der-Spion-im-Fernseher.html.

Lobo, S. (21.01.2015): »Zombie der Netzpolitik«. In: Der Spiegel. Abgerufen am 18.11.2020 von https://www.spiegel.de/netzwelt/web/vorratsdatenspeicherung-vds-ist-nutzlos-sagt-sascha-lobo-a-1014127.html.

Lobo, S. (21.01.2015): »Der immer wiederkehrende Zombie der Netzpolitik«. In: Der Spiegel. Abgerufen am 18.11.2020 von https://www.spiegel.de/netzwelt/web/vorratsdatenspeicherung-vds-ist-nutzlos-sagt-sascha-lobo-a-1014127.html.

Lotter, W. (2017): »Der Balanceakt«. In: Bulletin 2 (Herausgeber: Credit Swiss AG), S. 6-9.

Lu, D. (18.06.2020): »Uber and Lyft pricing algorithms charge more in non-white areas«. In: New Scientist. Abgerufen am 18.11.2020 von https://www.newscientist.com/article/2246202-uber-and-lyft-pricing-algorithms-charge-more-in-non-white-areas/.

Lutz, C./Strathoff, P. (12.06.2014): »Das Paradox der Privatsphäre«. In: Netzwoche 12, S. 27-28.

Mäder, C. (19.10.2019): »Die Privatsphäre schwindet – auch weil wir sie dauernd ausdehnen«. In: NZZ. Abgerufen am 11.09.2020 von https://www.nzz.ch/feuilleton/privatsphaere-das-stadthaus-zuerich-zeigt-ein-thema-der-paradoxe-ld.1513268.

Matthes, M.-C./Dachwitz, I. (29.11.2018): »Politik zur Datenschleuder Windows 10: Aufsichtsbehörden müssen handeln«. Abgerufen am 06.09.2020 von https://netzpolitik.org/2018/politik-zur-datenschleuder-windows-10-aufsichtsbehoerden-muessen-handeln#spendenleiste.

Mayer, J./Mutchler, P./Mitchel, J. (17.05.2016): »Evaluating the privacy properties of telephone metadata«. Abgerufen am 11.09.2020 von https://www.pnas.org/content/113/20/5536.

McConnell, M./Chertoff, M./Lynn, W. (28.07.2015): »Sections Democracy Dies in Darkness«. In: The Washington Post. Abgerufen am 16.09.2020 von https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

Meister, A. (27.05.2015): »Internes Dokument belegt: BND und Bundeskanzleramt wussten von Wirtschaftsspionage der USA gegen Deutschland«. Abgerufen am 16.09.2020 von https://netzpolitik.org/2015/internes-dokument-belegt-bnd-und-bundeskanzleramt-wussten-von-wirtschaftsspionage-der-usa-gegen-deutschland/#vorschaltbanner.

Michaels, J. (25.07.2019): »Datenschutz mit Lücken«. In: FAZ 170, S. 13.

Moechel, E. (17.05.2020): »EU-Ministerrat diskutiert wieder Hintertüren in Verschlüsselung«. In: radioFM4. Abgerufen am 26.09.2020 von https://fm4.orf.at/stories/3002708/.

Nicas, J. (21.10.2020). »The Police Can Probably Break Into Your Phone«. In: The New York Times. Abgerufen am 27.11.2020 von https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html.

Nosthoff, A.-V./Maschewski, F. (24.11.2017): »Jeder Smartphone-Besitzer ist ein Goldesel für Apple und Facebook«. In: NZZ. Abgerufen am 13.09.2020 von https://www.nzz.ch/feuilleton/zuckerberg-der-monopolist-des-lichts-und-herr-des-sehens-ld.1331268.

O'Harrow Jr., R. (2005): *No Place to Hide*. New York: Free Press, paperback.

Ohland, G. (20.06.2019): »Smart Homes ohne Internet, geht das? Ja!«. Abgerufen am 14.09.2020 von https://www.golem.de/news/iot-smart-homes-ohne-internet-geht-das-ja-1906-141709.html.

Otte, M. (19.05.2014): »Je größer die Mythen vom Netz, desto kleiner die Menschen«. In: FAZ 11, S. 13.

Pagel, P./Portmann, E./Vogt, J. (2020): »Editorisches Interview: Demokratie in Zeiten des Internets«. In: Informatik Spektrum 43, S. 1-4. Abgerufen am 19.11.2020 von https://link.springer.com/article/10.1007/s00287-020-01248-5.

Pekel, C. (08.09.2020): »Datenpools könnten Verbraucher:innen den Stromanbieterwechsel erschweren«. In: Netzpolitik.org. Abgerufen am 21.09.2020 von https://netzpolitik.org/2020/plaene-von-auskunfteien-datenpools-koennten-verbraucherinnen-den-stromanbieterwechsel-erschweren/#vorschaltbanner.

Ploppa, H. (26.01.2016): »Präsident Eisenhower warnte vor Militär-Industriellem Komplex«. In: Free21. Abgerufen am 20.09.2020 von www.free21.org/praesident-eisenhower-warnte-vor-militaer-in.

Prosser, W. L. (03.08.1960): »Privacy«. In: California Law Review 58 (3), S. 383-423. Abgerufen am 2.09.2020 von https://berkeleylawir.tind.io/record/1109651?ln=en.

Rebiger, S. (30.04.2016): »Niederlande: Neues Geheimdienstgesetz verschärft Massenüberwachung«. In: Netzpolitik.org. Abgerufen am 06.09.2020 von https://netzpolitik.org/2016/niederlande-neues-geheimdienstgesetz-verschaerft-massenueberwachung/.

Rieger, F. (2015): »Crypto Wars 3.0. Der Staat und die Angst vor der Verschlüsselung«. In: c't 8, S. 78-80.

Rössler, B. (2001): *Der Wert des Privaten*. Frankfurt a.M.: Suhrkamp.

Rössler, B. (2015): »Should personal data be a tradable good? On the moral limits of markets in privacy«. In: B. Roessler/D. Makrosinska, *The Social Value of Privacy*, S. 141-161.

Roessler, B./Makrosinska, D. (2015): *Social Dimensions of Privacy*. Cambridge UK: Cambridge University Press.

Rössler, B. (27.07.2016): »Reisefreiheit für Daten braucht Grenzen«. In: FAZ 50, S. 8.

Roth, P. (28.07.2020): »Facebook Audience Insights: Zielgruppenanalyse und -definition im Detail«. In: AllFacebook.de. Abgerufen am 10.2020 von https://allfacebook.de/zahlen_fakten/audience-insights.

Runde, M. (22.08.2016): »Wir brauchen ein Digitalgesetz«. In: FAZ. Abgerufen am 19.11.2020 von https://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/digitalisierung-wir-brauchen-ein-digitalgesetz-14391040.html?printPagedArticle=true#pageIndex_2.

Sadeghi, A.-R./Dessouki, G. (2016): »Security & Privacy Week Interviews, Part 2.« In: IEEE Security & Privacy 14.6 (November), S. 73.

Schaar, P. (08.08.2016): »Soziale Netzwerke sind keine Hilfsorgane der Sicherheitsbehörden«. In: Europäische Akademie für Informationsfreiheit und Datenschutz e.V. (EAID). Abgerufen am 06.09.2020 von https://www.eaid-berlin.de/soziale-netzwerke-sind-keine-hilfsorgane-der-sicherheitsbehoerden.

Schäfer, J. (01.10.2019): »Vorratsdatenspeicherung: Bundesverwaltungsgericht fragt EuGH«. In: eRecht24. Abgerufen am 07.09.2020 von: https://www.e-recht24.de/news/telekommunikation/11639-

vorratsdatenspeicherung-bundesverwaltungsgericht-fragt-eugh.html.

Schipper, L. (17.03.2015): »Was eigentlich ist das Internet der Dinge?«. In: FAZ. Abgerufen am 19.11.2020 von https://www.faz.net/aktuell/wirtschaft/cebit/cebit-was-eigentlich-ist-das-internet-der-dinge-13483592.html.

Schneier, B. (30.09.2006a): »Der Wert der Privatsphäre«. In: Daten-Speicherung.de – minimum data, maximum privacy. Abgerufen am 11.09.2020 von https://www.daten-speicherung.de/index.php/schneier-der-wert-der-privatsphaere/.

Schneier B. (15.06.2006b): »The Value of Privacy«. In: Schneier on Security. Abgerufen am 12.09.2020 von https://www.schneier.com/crypto-gram/archives/2006/0615.html#1.

Schneier, B. (15.03.2015): »Crypto-Gram«. In: Schneier on Security. Abgerufen am 10.09.2020 von https://www.schneier.com/crypto-gram/archives/2015/0315.html#3.

Schrems, M. (2014): *Kämpf um deine Daten*. Wien: edition a.

Schwesig, M. (09.10.2020): »Antrag des Landes Mecklenburg-Vorpommern«. Abgerufen am 21.09.2020 von https://www.bundesrat.de/SharedDocs/drucksachen/2020/0501-0600/514-20.pdf?__blob=publicationFile&v=1.

Sneyd, A. (01.05.2018): »Is Privacy No Longer a Social Norm for Digital Natives?«. Abgerufen am 10.09.2020 von https://medium.com/@alannahsneyd/is-privacy-no-longer-a-social-norm-for-digital-natives-db62029ce4d9.

Solon, O. (13.03.2017): »Artificial intelligence is ripe for abuse, tech researcher warns: ›a fascist's dream‹«. In: The Guardian. Abgerufen am 17.09.2020 von https://www.theguardian.com/technology/2017/mar/13/artificial-intelligence-ai-abuses-fascism-donald-trump.

Spehr, M. (06.08.2015): Ausgespäht mit Android. In: FAZ. Abgerufen am 19.11.2020 von https://www.faz.net/aktuell/technik-motor/digital/android-apps-geben-heimlich-nutzerdaten-weiter-13731586.html.

Spitz, M. (07.05.2015): »Durchschaut!«. Abgerufen am 19.11.2020 von https://durchschaut1.webnode.com/blog/.

Sprenger, P. (26.01.1999): »Sun on Privacy: ›Get Over It‹«. In: Wired. Abgerufen am 09.09.2020 von https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

Steffens, F. (22.09.2020): »Die Abtreibungsgegner spielen auf Sieg«. In: FAZ. Abgerufen am 19.11.2020 von https://www.faz.net/aktuell/politik/wahl-in-amerika/tod-von-ruth-bader-ginsburg-us-abtreibungsgegner-spielen-auf-sieg-16965149.html.

Stegers, F. (05.06.2007): »Sicherheit zu garantieren wird immer schwieriger. Interview mit Ex-Verfassungsrichter Benda«. Abgerufen am 13.09.2020 von https://www.tagesschau.de/inland/meldung24404.html.

Stöcker, C. (08.10.2009): »Google will die Weltherrschaft«. In: Der Spiegel. Abgerufen am 12.09.2020 von https://www.spiegel.de/netzwelt/netzpolitik/netz-strategie-google-will-die-weltherrschaft-a-665813.html.

Schüler, H. (2020): »Anwenderüberwachung durch Microsofts Office-Software«. In: heise online. Abgerufen am 25.11.2020 von https://www.heise.de/news/Anwenderueberwachung-durch-Microsofts-Office-Software-4968615.html.

Siedenbiedel, C. (28.04.2017): »Nicht jeder will sich im Auto überwachen lassen«. In: FAZ 99, S. 25.

Simitis, S. (2003): *Kommentar zum Bundesdatenschutzgesetz*. Baden-Baden: Nomos Verlagsgesellschaft.

Solove, D. J. (2001): *Nothing to Hide*. New Haven/London: Yale University Press.

Solove, D. (2015): »The meaning and value of privacy«. In: B. Roessler/D. Makrosinska, *The Social Value of Privacy*, S. 71-82.

Thiel, T. (04.05.2016): »Mit der Vernetzung wachsen die Lücken«. In: FAZ 104, S. N4.

Totschkas_blog 2.0. (30.12.2013): »Bullshit made in Germany.« Abgerufen am 16.09.2020 von https://totschka.wordpress.com/2013/12/30/bullshit-made-in-germany/.

Vance Jr., C./Molins, F./Leppard, A./Zaragoza, J. (11.08.2015): »When Phone Encryption Blocks Justice«. In: The New York Times. Abgerufen am 16.09.2020 von https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0.

Volokh, E. (11.12. 2014): »Liberty, Safety, and Benjamin Franklin«. In: The Washington Post. Abgerufen am 21.09.2020 von https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin/.

Warren, S. D./Brandeis, L. D. (15.12.1890): »The Right to Privacy«. In: Harvard Law Review 4.5, S. 193-220. Abgerufen am 19.11.2020 von http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Wefing, H. (19.08.2010): »Die neue Welt ist nackt«. In: DIE ZEIT 34. Abgerufen am 28.11.2020 von https://www.zeit.de/2010/34/Privatsphaere?utm_referrer=https %3A %2F %2Fwww.google.com %2F.

Whitfield, D./Landau, S. (2007): *Privacy On The Line*. Cambridge (Massachusetts)/London: The MIT Press.

Zuboff, S. (30.04.2014): »Schürfrechte am Leben«. In: FAZ. Abgerufen am 19.11.2020 von https://www.faz.net/aktuell/feuilleton/debatten/die-google-gefahr-zuboff-antwortet-doepfner-12916606.html.

Zuboff, S. (05.03.2016): »Wie wir Googles Sklaven wurden«. In: FAZ. Abgerufen am 19.11.2020 von https://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/shoshana-zuboff-googles-ueberwachungskapitalismus-14101816.html?printPagedArticle=true#pageIndex_8.

Zuboff, S. (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt a.M./New York: Campus Verlag.

## Webseiten

Amazon Datenschutzerklärung. (1998-2020): Abgerufen am 15. 11.2020 von https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-

5B1B8CFC3F4A__SECTION_CC8D0F28BF6544B5937531FB0B44AE58.

Apple Daten und Datenschutz. (2020): Abgerufen am 05.09.2020 von https://privacy.apple.com/account.

Apple Datenschutzrichtlinie. (31.12.2019): Abgerufen am 15.11.2020 von https://www.apple.com/at/legal/privacy/de-ww/.

Apple Interessenbezogene Werbung im App Store und in Apple News deaktivieren. (07.04.2020): Abgerufen am 15.11.2020 von https://support.apple.com/de-at/HT202074.

Apple-Nutzer zahlen mehr für Hotelzimmer. (26.06.2012): Abgerufen am 16.09.2020 von https://www.spiegel.de/wirtschaft/service/datenauswertung-bei-orbitz-apple-user-zahlen-mehr-fuer-hotelzimmer-a-840938.html.

Apple Privacy. (2020): Abgerufen am 15.10.2020 von https://www.apple.com/privacy/.

Apple speichert Siri-Daten bis zu zwei Jahre. (19.11.2013): Abgerufen am 14.10.2020 von https://www.focus.de/digital/handy/neuer-datenschutz-skandal-apple-speichert-siri-daten-bis-zu-zwei-jahre_aid_966428.html.

BSI untersucht Sicherheitseigenschaften von Windows 10. (20.11.2018): Abgerufen am 06.09.2020 von https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Studie_Win_10_20112018.html.

Bush at FEMA Headquarters. (01.10.2001): In: The Washington Post. Abgerufen am 12.09.2020 von Transcript seiner Rede im FEMA Headquartier in Washington: https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushtext_100101.html.

Cambridge Analytica. (2018): Abgerufen am 20.11.2020 von https://web.archive.org/web/20180321032231/https://ca-commercial.com/services/.

CDU-Spitze fordert nach Corona-Demo mehr Befugnisse für Polizei. (01.09.2020): In: FAZ. Abgerufen am 15.11.2020 von https://www.faz.net/aktuell/politik/inland/cdu-spitze-fordert-nach-corona-demo-mehr-befugnisse-fuer-polizei-16932769.html.

Church Committee. (05.12.2019): Abgerufen am 17.11.2020 von https://de.wikipedia.org/wiki/Church_Committee.

Das Bundesarchiv. (2020): Ziele und Angebote des Fördervereins Erinnerungsstätte für die Freiheitsbewegungen in der deutschen Geschichte e. V. Abgerufen am 21.09.2020 von https://www.bundesarchiv.de/DE/Content/Artikel/Ueber-uns/Dienstorte/FoeVe_Rastatt/2018-11-14_ziele_angebote_foerderverein.html.

Daten-Speicherung.de – minimum data, maximum privacy. (o.J.): Abgerufen am 5.09.2020 von https://www.daten-speicherung.de/index.php/datenspeicherung/unternehmen/.

Demokratie: die erfolgreichste Staatsform. (20.09.2020): Demokratie: die erfolgreichste Staatsform. Abgerufen am 16.11.2020 von https://www.bmz.de/de/themen/demokratie/hintergrund/index.html.

Der BigBrotherAward 2011 in der Kategorie »Kommunikation« geht an die Apple GmbH. (2011): Abgerufen am 15.11.2020 von https://bigbrotherawards.de/2011/kommunikation-apple.

Der BigBrotherAward 2011 in der Kategorie »Kommunikation« geht an die Facebook Deutschland GmbH. (2011): Abgerufen am 15.11.2020 von https://bigbrotherawards.de/2011/kommunikation-facebook.

Der BigBrotherAward (2013) in der Kategorie »Globales Datensammeln« geht an Larry Page, Sergey Brin und Eric Schmidt, die Gründer und Verwaltungsrat der Google Inc. (2013): Abgerufen am 15.11.2020 von https://bigbrotherawards.de/2013/globales-datensammeln-google.

Eisenhower's Farewell Address to the Nation. (17.01.1961): Abgerufen am 17.11.2020 von http://mcadams.posc.mu.edu/ike.htm.

Encryption and Anonymity create »a zone of privacy online«, says UN Special Rapporteur. (2015): Abgerufen am 26.11.2020 von https://privacyinternational.org/news-analysis/1403/encryption-and-anonymity-create-zone-privacy-online-says-un-special-rapporteur.

EuGH verbietet Vorratsdatenspeicherung erneut. (06.10.2020): Abgerufen am 17.11.2020 von https://posteo.de/news/eugh-verbietet-vorratsdatenspeicherung-erneut.

Europäische Datenwirtschaft. (10.01.2017): »EU-Kommission stellt Konzept für Daten-Binnenmarkt vor«. Abgerufen am 17.11.2020 von https://ec.europa.eu/germany/news/europ%C3%A4ische-datenwirtschaft-eu-kommission-stellt-konzept-f%C3%BCr-daten-binnenmarkt-vor_de.

Facebook's Zuckerberg Says Privacy No Longer A ›Social Norm‹ (VIDEO). (18. 03. 2010): HuffPost. Abgerufen am 10.09.2020 von https://www.huffpost.com/entry/facebooks-zuckerberg-the_n_417969.

Final Report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (26.04.1976): Abgerufen am 17.11.20202 von https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

»Five Eyes« fordern Zugang zu verschlüsselten Apps. (12.10.2020): In: FAZ. Abgerufen am 12.10.2020 von https://www.faz.net/aktuell/politik/ausland/five-eyes-fordert-zugang-zu-verschluesselten-apps-16997581.html.

Forum Privatheit. (2020): Mission Statement. Abgerufen am 19.09.2020 von https://www.forum-privatheit.de/arbeitsschwerpunkte/.

Geschichte der Fotografie. (2017): Abgerufen am 02.09.2020 von https://www.lumas.de/geschichte-fotografie/.

Jahr 1 nach Snowden. (23.12.2015): Abgerufen am 26.11.2020 von https://edoc.hu-berlin.de/handle/18452/14315.2.

Homepage der Washington Post. (o.J.): Abgerufen am 20.09.2020 von https://www.washingtonpost.com/.

International Statement: End-To-End Encryption and Public Safety. (11.10.2020): Abgerufen am 12.10.2020 von https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

Internet der Dinge Was ist das, was bringt das, wie riskant ist das? (23.03. 2016): In: test. Abgerufen am 4.09.2020 von https://www.test.de/Internet-der-Dinge-Was-ist-das-was-bringt-das-wie-riskant-ist-das-4993088-0/.

Israelische Firma hilft FBI angeblich beim iPhone-Hack. (23.05.2016). In: Der Spiegel. Abgerufen am 18.11.2020 von https://www.spiegel.

de/netzwelt/netzpolitik/apple-vs-fbi-cellebrite-koennte-laut-bericht-beim-iphone-hack-helfen-a-1083875.html.

Nardone vs. United States. (1937): Abgerufen am 02.09.2020 von https://caselaw.findlaw.com/us-supreme-court/302/379.html.

No Place to Hide (2006): Abgerufen am 15.11.2020 von https://www.amazon.com/Place-Hide-Robert-OHarrow-Jr/dp/0743287053.

Nothing to Hide – Dokumentarfilm (2017): Abgerufen am 26.11.2020 von https://vimeo.com/195446463.

Olmstead v. United States (2020): Abgerufen am 16.11.2020 von https://en.wikipedia.org/wiki/Olmstead_v._United_States.

Olmstead v. United States (1928): Abgerufen am 19.11.2020 von https://www.oyez.org/cases/1900-1940/277us438.

Olmstead v. United States: (28.06.1928): Abgerufen am 02.09.2020 von https://caselaw.findlaw.com/us-supreme-court/277/438.html.

On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things. (02.06.2016): Abgerufen am 26.11.2020 von https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

Parlament stimmt EU-Richtlinie über Verwendung von Fluggastdaten zu. (14.04.2016): Abgerufen am 8.09.2020 von https://www.europarl.europa.eu/news/de/press-room/20160407IPR21775/parlament-stimmt-eu-richtlinie-uber-verwendung-von-fluggastdaten-zu.

Regierungserklärung von Bundeskanzlerin Dr. Angela Merkel. (23.04.2020): Abgerufen am 08.09.2020 von https://www.bundesregierung.de/breg-de/suche/regierungserklaerung-von-bundeskanzlerin-dr-angela-merkel-1746978.

Rekord für Apple: Börsenwert erreicht zwei Billionen Dollar. (20.08.2020). In: die Zeit. Abgerufen am 18.11.2020 von https://www.zeit.de/news/2020-08/19/rekord-fuer-apple-boersenwert-erreicht-zwei-billionen-dollar.

Remarks by the President at South By Southwest Interactive. (11.03.2016): Abgerufen am 08.09.2020 von https://obamawhite-

house.archives.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive.

Richtlinie (EU) 2019/770 des europäischen Parlaments und des Rates vom 20.05.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. (2019): Abgerufen am 09.09.2020 von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0770&from=D.

Roe v. Wade. (22.01.1973): Abgerufen am 05.09.2020 von https://case-law.findlaw.com/us-supreme-court/410/113.html.

Stoppt die Vorratsdatenspeicherung. (o.J.): Abgerufen am 06.09.2020 von www.vorratsdatenspeicherung.de/content/view/46/42/lang,de/.

Targeted Advertising. (13.09.2020): Abgerufen am 17.09.2020 von https://netzpolitik.org/?na=v&nk=37191-c1411da6c8&id=265.

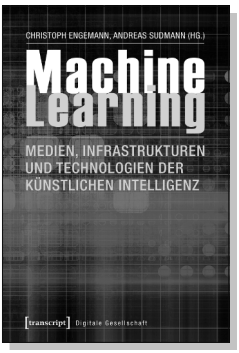
Vorratsdatenspeicherung Alle Menschen unter Generalverdacht. (o.J.): Abgerufen am 13.09.2020 von https://epicenter.works/thema/vorratsdatenspeicherung.

Vorratsdatenspeicherung ist nur in Ausnahmen zulässig. (06.10.2020): In: FAZ. Abgerufen am 08.10.2020 von https://www.faz.net/aktuell/wirtschaft/urteil-des-eugh-pauschale-vorratsdatenspeicherung-ist-nicht-zulaessig-16988320.html.

Wer weiß was über die Nutzer: Die wirkliche Datenkrake heißt Amazon. (25.10.2011): Abgerufen am 06.09.2020 von https://www.foerderland.de/digitale-wirtschaft/netzwertig/news/wer-weis-was-uber-die-nutzer-die-wirkliche-datenkrake-heist-amazon/.

Wir brauchen eine neue Privacy-Debatte. (16.06.2016): Abgerufen am 11.09.2020 von https://www.basecamp.digital/michael-sandel-im-basecamp-wir-brauchen-eine-neue-privacy-debatte/.

# Medienwissenschaft




Christoph Engemann, Andreas Sudmann (Hg.)
**Machine Learning –**
**Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz**
2018, 392 S., kart.
32,99 € (DE), 978-3-8376-3530-0
E-Book:
PDF: 32,99 € (DE), ISBN 978-3-8394-3530-4
EPUB: 32,99 € (DE), ISBN 978-3-7328-3530-0


Tanja Köhler (Hg.)
**Fake News, Framing, Fact-Checking: Nachrichten im digitalen Zeitalter**
**Ein Handbuch**

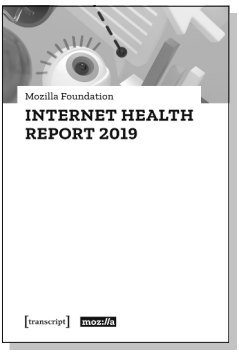
Juni 2020, 568 S., kart., 41 SW-Abbildungen
39,00 € (DE), 978-3-8376-5025-9
E-Book:
PDF: 38,99 € (DE), ISBN 978-3-8394-5025-3


Geert Lovink
**Digitaler Nihilismus**
**Thesen zur dunklen Seite der Plattformen**

2019, 242 S., kart.
24,99 € (DE), 978-3-8376-4975-8
E-Book:
PDF: 21,99 € (DE), ISBN 978-3-8394-4975-2
EPUB: 21,99 € (DE), ISBN 978-3-7328-4975-8

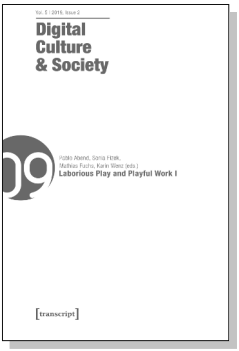
**Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de**

# Medienwissenschaft




Mozilla Foundation
**Internet Health Report 2019**

2019, 118 p., pb., ill.
19,99 € (DE), 978-3-8376-4946-8
E-Book: available as free open access publication
PDF: ISBN 978-3-8394-4946-2




Pablo Abend, Sonia Fizek, Mathias Fuchs, Karin Wenz (eds.)
**Digital Culture & Society (DCS)**
**Vol. 5, Issue 2/2019 – Laborious Play and Playful Work I**

September 2020, 172 p., pb., ill.
29,99 € (DE), 978-3-8376-4479-1
E-Book:
PDF: 29,99 € (DE), ISBN 978-3-8394-4479-5


Gesellschaft für Medienwissenschaft (Hg.)
**Zeitschrift für Medienwissenschaft 23**
**Jg. 12, Heft 2/2020: Zirkulation.**
**Mediale Ordnungen von Kreisläufen**

September 2020, 218 S., kart.
24,99 € (DE), 978-3-8376-4924-6
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-4924-0
ISBN 978-3-7328-4924-6

**Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de**