

Einleitung: Schöne neue Verbraucherwelt?

Big Data, Scoring und das Internet der Dinge

Christian Bala und Wolfgang Schuldzinski

DOI 10.15501/978-3-86336-912-5_1

Abstract

Mit Big Data wird die Debatte um die Informatisierung des Alltags über die Frage nach dem Datenschutz hinaus geführt. Es geht nicht mehr allein um die Erfassung von Daten. Mit der Fähigkeit große, auch unstrukturierte Datenmengen zu speichern, miteinander zu verknüpfen und zu analysieren, können intelligente System Schlüsse ziehen. Verhaltensweisen werden vorhersagbar und auch manipulierbar, was Unternehmen die Möglichkeit gibt zielgenau zu werben, eine soziale Auslese zu betreiben und ihre Risiken zu minimieren. Verbraucherinnen und Verbraucher werden dabei zu Datenlieferanten, ohne dass ihnen die dahinter liegenden Strukturen und Mechanismen transparent sind.

Dieser Beitrag erscheint unter der Creative-Commons-Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 Deutschland | CC BY-SA 3.0 DE
Kurzform | <http://creativecommons.org/licenses/by-sa/3.0/de/>
Lizenztext | <http://creativecommons.org/licenses/by-sa/3.0/de/legalcode>

1 Von Big Brother zu Big Barbie?

Durchdringend, mit kalten Augen, starrt der große Bruder von den Standbildern und Plakaten in den Verfilmungen der Orwellschen Dystopie „1984“. Ein Diktator, den das Volk lieben soll, und den es zugleich fürchtet, da jeder Einzelne weiß, dass er in dem totalitären Staat unter Beobachtung steht. Das ist die alte Fratze des Überwachungsstaates, vor der jeder zurückschreckt. So hässlich ist das neue Gesicht der Überwachung nicht mehr: Freundlich, mit großen Augen, lächelt die „Hello Barbie“ aus den Regalen und Online-Shops. Ein Spielzeug, das die Kinder lieben, aber nicht fürchten werden, denn schließlich sollen sie nicht nur mit der Puppe reden, sondern sich ihr auch anvertrauen: „Just like a real friend, Hello Barbie™ doll listens and remembers the user’s likes and dislikes, giving everyone their own unique experience“, heißt es in der Produktbeschreibung auf der Webseite des Herstellers (Mattel, Inc. 2015). Dafür gab es 2015 den „Big Brother Award“ des Vereins Digitalcourage, denn die Puppe, die in Europa wegen Datenschutzbedenken (noch) nicht zu haben ist, überträgt die Gespräche an eine Serverfarm der Firma Toytalk, wo sie nicht nur für Marketingzwecke und zur Verbesserung des Produkts ausgewertet, sondern auch in Protokollen für die Eltern per E-Mail aufbereitet werden (siehe Neumann 2015). Käuferinnen und Käufer zahlen also rund 75 US-Dollar dafür, dass ihre Kinder zu Datenquellen für Unternehmen werden, kostenlos deren Produkte verbessern und über die kleinen Geheimnisse ihres Nachwuchses Bescheid wissen. Wobei das Produkt, kaum auf dem Markt, bereits durch den Kryptologen Matt Jakobowski gehackt war. Er konnte auf „Account-IDs, Audio-dateien, das Mikrofon und Netzwerknamen“ zugreifen, „mit etwas mehr Aufwand“ ließ sich die Puppe „auch mit einem anderen Server verbinden – und damit dann auch steuern, was die Barbie sagt.“ (Schirmmacher 2015)

Überwachung in der Welt des Konsums hat, so der Jurist Daniel J. Solove (2004; 2011), weniger die Disziplinierung zum Ziel, weshalb er die Metapher vom „Big Brother“ für überstrapaziert hält. Vielmehr geht es um die Gewinnung eines Datenpools, um mehr über das Verhalten der Kundinnen und Kunden zu erfahren. „Consumer surveillance can be understood as a form of surveillance that aims at predicting and, in combination with (personalized) advertising, controlling the behavior of consumers.“ (Sandoval 2012, 148) Indem die Unterneh-

men das Verhalten der „Verbrauchenden“ besser kennen und daraus Vorhersagen ableiten, können sie nicht nur ihre Produkte besser an den Mann oder die Frau bringen, sondern zwischen begehrten und ungewollten Kundinnen und Kunden unterscheiden (siehe Bala und Müller 2014, 26; Bendrath 2007, 7). Dieses Ziel wird durch die „Datenfusion“ erreicht, also das Zusammenspiel verschiedener Datenquellen im Zusammenspiel mit Maschinen, die Muster erkennen und daraus Schlüsse ziehen, auf deren Basis Entscheidungen gefällt werden (siehe Hofstetter 2014; Schlieter 2015; Schneier 2015).

Dabei müssen noch nicht einmal die eigenen Daten unmittelbar negative Auswirkungen haben. Vielmehr ermöglicht es bereits die Masse der gesammelten Daten Menschen nach Gruppen zu klassifizieren, denen bestimmte Eigenschaften zugewiesen werden. Daraus wird dann abgeleitet, wie sich ein anderes Individuum, dessen Merkmale mit denen der identifizierten Gruppe übereinstimmen, wahrscheinlich verhalten wird, unabhängig davon, ob diese Voraussage zutrifft oder nicht. Big Data, also die Fähigkeit große, auch unstrukturierte Datenmengen nicht nur zu speichern, sondern auch miteinander zu verknüpfen und zu analysieren, kann dazu führen, dass Verbraucherinnen und Verbraucher, ohne dass sie es wissen und ohne dass ihr reales Verhalten dazu beigetragen hat, einer negativen Auslese durch Unternehmen ausgesetzt sind (siehe Bauman 2009, 11). „Als Schlagwort steht Big Data für die Überlagerung eines statistisch fundierten Kontrollwissens durch eine medientechnologisch fundierte Makroorientierung an der ökonomischen Verwertbarkeit von Daten und Informationen.“ (Reichert 2016, 22)

Die Grundlage dieses Scorings ist meist undurchsichtig und kann deshalb auch recht willkürlich sein. So berichtet Frank Pasquale in seinem Buch „The Black Box Society“, dass eine Kreditkartenfirma sich für die mentale Gesundheit ihrer Kundschaft interessierte. Datenauswertungen hatten ergeben, dass Paare, die eine Paartherapie aufsuchen, sich eher scheiden lassen, als Paare die das nicht tun. Scheidungen können aber zu finanziellen Belastungen und Kreditausfällen führen. Nun durchforstete das Unternehmen die Buchungen der Kundinnen und Kunden, mit der Folge, dass die Kreditwürdigkeit von Personen in Zweifel stand, nur weil sie eine Paarberatung aufsuchten (siehe Pasquale 2015, 37). „Put another way, credit-card companies are becoming much more interested in understanding their customers' lives and psyches, because, the theory goes, knowing what makes cardholders tick will help firms

determine who is a good bet and who should be shown the door as quickly as possible.“ (Duhigg 2009). Obwohl keine Kausalität zwischen einer Eheberatung und verzögerter Kreditrückzahlung besteht, reichte dem Unternehmen die Korrelation zwischen Eheberatung und Scheidung aus, um die Kreditlinie von Kundinnen und Kunden zu kürzen, die versuchten, ihre ehelichen Probleme zu lösen – und den Fehler begingen, den Therapeuten mit ihrer Kreditkarte zu bezahlen (siehe Pasquale 2015, 37).

Die mit einem schlechten Scorewert versehenen Verbraucherinnen und Verbraucher wissen nichts, wie Joseph K. in Franz Kafkas „Der Prozess“ (2005), über die Gründe für die Entscheidung: „The Trial captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one’s life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process.“ (Solove 2004, 38) Das Urteil in dieser schönen neuen Verbraucherwelt wird auf der Basis der verfügbaren Daten getroffen.

2 Wer hat schon was gegen ein gesünderes Leben?

Basierte die Praxis der Kreditkartenfirma noch auf konkreten Zahlungen ihrer Kundinnen und Kunden, sind die Daten die das Internet der Dinge generiert vielfältig, die Datenmengen sind riesig und der Datenstrom ist kaum zu kontrollieren. Zudem ist nicht ersichtlich, wer Zugriff auf diese Daten hat und wie sie verwertet werden. Einer Diskussion über diese Intransparenz und Unschärfe versuchen Anbieter zu entgehen, indem sie den Nutzen ihrer Technologien anpreisen und die Steigerung der Lebensqualität in den Vordergrund stellen. Das Internet der Dinge und Big Data sollen als Hilfe, ja als Lösung von Problemen erscheinen. Die Haltung Probleme durch Technik lösen zu wollen, ist Bestandteil einer Weltsicht, die Evgeny Morozov als Solutionismus bezeichnet

hat. Damit beschreibt er aber nicht nur einen technikzentrierten Blick auf soziale oder wirtschaftliche Herausforderungen, sondern die Tendenz Umstände als Problem zu identifizieren, die eigentlich keine sind (siehe Morozov 2013, 26). Wearables, also Smartwatches oder Fitnessarmbänder, sind Beispiele für eine „solution in search of a problem“ (Piwek et al. 2016).

Wearables und Apps die eine Zulassung als Medizinprodukte haben, können sicherlich dazu beitragen, die Werte von Risikopatienten oder chronisch Erkrankten zu überwachen und so ihr Wohlbefinden und ihre Sicherheit zu steigern. Braucht man aber tatsächlich eine elektronische Zahnbürste mit Bluetooth, welche das Putzverhalten in einer App protokolliert? Ist es sinnvoll, ständig die Vitalzeichen eines gesunden Neugeborenen über einen Schnuller auf das elterliche Smartphone übertragen zu lassen (siehe Blue Maestro Limited 2016), um dann bei jedem Temperaturanstieg den Kinderarzt aufzusuchen?

Die Versicherer betonen den Nutzen einer Verknüpfung von Wearables und Big Data und übernehmen dabei die Argumentationen der Anbieter von Trackern und entsprechender Software. So verkündete der Vertreter eines großen Versicherungskonzerns auf einer Tagung über Big Data, dass die Nutzerinnen und Nutzer durch Selbstvermessung und die Auswertung von Vergleichsdaten auf mögliche schwere Erkrankung hingewiesen werden könnten. Wer könne denn schon etwas dagegen haben, wenn man durch Wearables und Health Apps ein gesünderes Leben führe? Und so auch der Vorstandsvorsitzende der Techniker Krankenkasse Jochen Baas in einem Interview mit der „Süddeutschen Zeitung“: „Wir können über das Risiko einer Erkrankung informieren, wenn wir die Krankheiten, den Puls, das Ausmaß der Bewegung und so weiter zusammen analysieren.“ (Jochen Baas im Interview mit Bohsem und Schäfer 2016).

Abgesehen davon, dass man mit dieser Argumentation auch zu standardmäßigen DNA-Analysen und regelmäßige MRTs raten könnte, denn schließlich werden so Dispositionen für Krankheiten erkennbar, verschleiert sie nur mühsam die dahinter stehenden Interessen, nämlich die Risiken für das eigene Unternehmen zu minimieren. Mit seiner Argumentation schien der Versicherungsvertreter nicht allein die Datenschutzbedenken vom Tisch wischen zu wollen, sondern vor allem den Stachel gegen jene Stimmen zu löcken, welche vor den gesellschaftlichen Auswirkungen der Informatisierung warnen.

Fanden Wearables zunächst begeisterte Aufnahme in der Szene von Selbstvermessern und -optimierern (siehe Selke 2014), werden sie seit 2015 von privaten und gesetzlichen Krankenversicherern entdeckt. Vorreiter sind hier die USA: Arbeitgeber und betriebliche Krankenversicherer erhoffen sich, durch diese Geräte den Krankenstand der Belegschaft zu senken. Noch ist die Teilnahme an solchen Programmen weitgehend freiwillig, doch die christlich-evangelikale Oral Roberts University in Oklahoma hat für neue Studierende das Fitbit-Armband zur Pflicht gemacht. Diese erhobenen Daten werden an die Hochschule übermittelt und zur Grundlage der Bewertung in einigen Kursen. (Siehe Frankel 2016; Thielman 2016)

In Deutschland bot Anfang 2015 die Generali als einer der ersten Anbieter Kranken- und Berufsunfähigkeitsversicherungen an, die günstigere Tarife für diejenigen Kundinnen und Kunden versprochen, die regelmäßig Sport treiben und dies über einen Tracker und ihr Smartphone nachweisen. Die gesetzlichen Krankenkassen zogen nach, und belohnen Fitnessaktivitäten mit Wearables nun im Rahmen ihrer Bonusprogramme, die es seit 2004 erlauben eine gesunde Lebensführung mit Geld zu belohnen. Gemessen wird momentan nur aufgrund der geltenden Datenschutzgesetze, ob die Bedingungen für die Bonusprogramme erfüllt sind, beispielsweise eine bestimmte Anzahl an Schritten. (M. M. Becker 2016, 36)

Diese Haltung erscheint schon auf der Ebene der Grundannahmen problematisch und zeugt von solutionistischem Denken. Fast erinnert diese Strategie an das alte Bonmot, dass ein Gesunder nicht gesund, sondern nur schlecht untersucht ist. Da es nun die Möglichkeit gibt, den Puls, Atemfrequenz, Schweißproduktion, etc. direkt zu messen, sollte sie auch ausgeschöpft werden, auch wenn Ärzte mit den Tracking-Daten wenig anfangen können: „Für Franz Bartmann, Vorstandsmitglied der Bundesärztekammer, sind Tracking-Daten in Patientenakten „Datenmüll“. Die vorwiegenden Nutzer seien leistungsbereite junge Menschen, die meist kein Fall für den Arzt seien. Sinnvolle Daten, die vom Patienten erfasst werden und in die Behandlung einfließen, müssten darüber hinaus die strengen Kriterien des Medizinproduktegesetzes erfüllen.“ (K. B. Becker 2016)

Diese Sichtweise wird durch eine Studie über Consumer Health Wearables bestätigt, die betont, dass Personen, die einen gesunden Lebensstil pflegen,

ihre eigenen Fortschritte quantifizieren wollen (siehe Piwek et al. 2016). Darüber hinaus wird die tatsächliche medizinische Brauchbarkeit dieser Produkte infrage gestellt und ihre Reliabilität und Validität angezweifelt: „Devices are marketed under the premise that they will help improve general health and fitness, but the majority of manufactures provide no empirical evidence to support the effectiveness of their products.“ (Piwek et al. 2016). Die Gefahr von Fehlalarmen und Selbstdiagnosen, die zur Verunsicherung der Nutzerinnen und Nutzer beitragen, sind ebenfalls Risiken, vor denen gewarnt wird (siehe Piwek et al. 2016).

Neben Zweifeln an der Brauchbarkeit der verfügbaren Geräte für das Ziel der Gesundheitsüberwachung und Bedenken in puncto Datenschutz und Datensicherheit weist Health Tracking noch eine gesellschaftliche und politische Dimension auf: Bonusprogramme ziehen vor allem gesunde Versicherte an, die für sich einen Nutzen sehen, ihre Daten gegen Geld zu tauschen (siehe M. M. Becker 2016, 36). Dieses Verhalten ist in der wissenschaftlichen Literatur als Unraveling bekannt (siehe u. a. Benndorf, Kübler und Normann 2015; Jentzsch 2016; Peppet 2015). „Für jene Versicherte, die aufgrund ihrer Lebensumstände den größten gesundheitlichen Risiken ausgesetzt sind – kurz gesagt Alleinerziehende, Arme, Erwerbslose und Menschen ohne soziale Bezüge – sind die Anreize zu gering und die Hürden zu hoch, um ihr Verhalten zu ändern.“ (M. M. Becker 2016, 37) Dies kann aber zu diskriminierenden Effekten führen, die schon aus dem Scoring bekannt sind, denn nicht verfügbare Daten könnten als „schlechtes Risiko“ interpretiert werden; als jene die nichts für ihre Gesundheit tun, keinen Präventionswillen oder Eigenverantwortung zeigen (siehe M. M. Becker 2014). Letztlich würde die Bereitschaft zur Einschränkung der Privatsphäre der einen, zu einer Schlechterstellung derjenigen führen, die nichts preisgeben wollen oder können. (Siehe auch Jentzsch 2016)¹

1 Dieser Effekt kann auch im digitalen Wohnungsmarkt beobachtet werden. Bei Immobilienscout24 können Wohnungssuchende Einkommensnachweise, Bonitäts- und Selbstauskünfte hochladen, die dann von den potenziellen Vermietern eingesehen werden können. Ein auskunftsfreudiges Profil wird als „Top-Bewerber“ angezeigt. Wer allerdings über ein geringeres Einkommen verfügt und deshalb keine Nachweise hochlädt, könnte bei der Vorauswahl bereits durchs Raster fallen. (Siehe Müller 2016)

Der Prozess der Offenlegung, warnt Nicola Jentzsch (2016) vom Deutschen Institut für Wirtschaftsforschung (DIW, Berlin), könnte aufgrund seiner inneren Logik zur sozialen Norm werden. Schon die Zukunftsvisionen der privaten und gesetzlichen Versicherer zeigen ambitioniertere Ziele: TK-Chef Baas träumt bereits jetzt davon, dass jedermann „so ein Gerät haben“ wird (Jochen Baas im Interview mit Bohsem und Schäfer 2016). Wird aber die Selbstvermessung zur Norm, wird auch der damit verbundenen Ideologie der Selbstoptimierung, im Sinne einer fehlerfreien Funktion, zur Akzeptanz verholfen, was im Gegensatz zum Solidarprinzip steht: „Leistungsträger werden von Leistungsverweigerern getrennt, Kostenverursacher von Kosteneinsparern, ‚Health-On‘-Menschen (Gesunde) von ‚Health-Off‘-Menschen (Kranke)“ (Selke 2015, 83).

3 Big Data – mehr als Datenschutz oder Datensicherheit

Big Data führt die Debatte über die Informatisierung über die engere Frage nach dem Datenschutz hinaus, denn die „Ordnung des Wissens ist immer auch eine politische Ordnung“ (Grassmuck 2012, 15). Das Internet der Dinge hebt die Frage nach der Datensicherheit auf ein neues Niveau, wenn die Gebrauchsgegenstände angreifbar werden, siehe das Beispiel „Hello Barbie“ (siehe Schirmmacher 2015). Mit Big Data und dem Internet der Dinge sind erhebliche gesellschaftliche, politische und soziale Fragen verbunden. Technik ist kein neutrales Werkzeug, sondern prägt das Denken und Verhalten (siehe Latour 1996; Mainzer 2014; Weizenbaum 1978). Und bei allen Beteuerungen der Anbieter mit ihren Produkten die Welt zu verbessern, haben sie ein wirtschaftliches Eigeninteresse, so stehen die Anbieter von Fitnessstrackern unter hohem Druck der Investoren (siehe Windeck 2016). Durch die Fähigkeit große, auch unstrukturierte Datenmengen zu speichern, miteinander zu verknüpfen und zu analysieren, können intelligente Systeme Schlüsse ziehen. Verhaltensweisen werden vorhersagbar und auch manipulierbar, was Unternehmen die Möglichkeit gibt, zielgenau zu werben, eine soziale Auslese zu betreiben und ihre Risiken zu minimieren. Verbraucherinnen und Verbraucher werden dabei

zu Datenlieferanten, ohne dass ihnen die dahinter liegenden Strukturen und Mechanismen transparent sind.

In diesem Spannungsfeld aus Recht, Informatik und Sozialwissenschaft bewegte sich der 7. Workshop Verbraucherforschung, der am 15. Juni 2015 in Düsseldorf in Kooperation mit dem Düsseldorfer Instituts für Wettbewerbsökonomie (DICE) der Heinrich-Heine-Universität stattfand und dessen Vorträge diesem Band zugrunde liegen:

- Der Physiker und Soziologe *Dirk Helbing*, der unlängst mit Yvonne Hofstetter, Gerd Gigerenzer und anderen ein „Digital-Manifest“ für eine digitale Demokratie veröffentlicht hat (Helbing et al. 2016), hegt in seinem Artikel grundlegende Skepsis an den Hoffnungen, die mit Big Data als einer „Super-Intelligenz“ verknüpft werden. Vielmehr sieht er die Drohung einer automatisierten Gesellschaft, die auf der Basis von Big-Data-Analysen Entscheidungen trifft. Im Gegensatz dazu entwirft er die Idee einer kollektiven Intelligenz, welche eine partizipative Form der Nutzung des Netzes darstellt.
- Der Beitrag von *Barbara Kolany-Raiser*, die an der Westfälischen Wilhelms-Universität Münster das interdisziplinäre Projekt ABIDA (Assessing Big Data) koordiniert, zeigt die rechtlichen Probleme, die mit smarten Alltagsgegenständen und insbesondere Wearables im Gesundheitsbereich verbunden sind. Sie zeigt die fehlende Transparenz der Anbieterseite auf und öffnet den Blick dafür, dass gegenwärtig vor allem die Verbraucherinnen und Verbraucher die Risiken tragen, welche sich durch Nutzung dieser Güter ergeben.
- Die Integration intelligenter Systeme und die Aussicht auf autonomes Fahren sollen die Sicherheit im Straßenverkehr erhöhen. Doch was ist, wenn das Auto *aufgrund* der smarten Technologie zu einem Sicherheitsrisiko wird? *Kerstin Lemke-Rust* gibt in ihrem Artikel einen Überblick, welche Bereiche besonders sensibel sind. Ihre daraus abgeleiteten Handlungsempfehlungen zeigen, dass noch viele Herausforderungen angegangen werden müssen.
- Die Debatte um die Implementierung eines smarten Stromnetzes greift *Ulrich Greveler* auf und stellt Interessenkonflikte zwischen dem Anspruch

eine moderne, effiziente und nachhaltige Infrastruktur zu schaffen und dem Recht auf Privatsphäre fest. Doch diese Interessen müssen nicht unvereinbar sein, wenn der Datenschutz bei der gesetzlichen Ausgestaltung ernst genommen und dessen Einhaltung auch konsequent umgesetzt wird. Auch müsse ein Opt-Out-Recht der Verbraucherinnen und Verbraucher in Erwägung gezogen werden.

- Smarte Autos und Netze, auf diese Datenquellen haben Verbraucherinnen und Verbraucher keinen Zugriff, da die Software eng mit der Hardware verbunden ist und keine Eingriffe Dritter erlaubt. Über ihre mobilen Endgeräte meinen die Nutzerinnen und Nutzer jedoch die Kontrolle zu haben, eine Illusion wie *Michael Schleusener* und *Sarah Hosell* in ihrem Beitrag zeigen, der die Ergebnisse eines im Rahmen des KVF NRW geförderten Forschungsprojektes zusammenfasst, das auch im Bericht zum Online-Handel des Sachverständigenrates für Verbraucherfragen (SVRV) beim Bundesministerium der Justiz und für Verbraucherschutz (BMJV) Erwähnung fand (siehe Reisch et al. 2016). Die Verbraucherinnen und Verbraucher sind, so belegen sie, durch die unkontrollierte Auswertung von Daten manipulierbar geworden.

Danksagung

Der Dank der Herausgeber gilt allen, die dabei geholfen haben, den fünften Band der „Beiträge zur Verbraucherforschung“ zu ermöglichen. An erster Stelle sind natürlich die Autorinnen und Autoren zu nennen. Besonderer Dank gebührt Prof. Dr. Justus Haucap vom DICE, der mit uns gemeinsam den 7. Workshop Verbraucherforschung ausrichtete. Wir danken unseren Kooperationspartnern, dem Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MKULNV) und dem Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen, für die Unterstützung bei der Produktion und der Verankerung der „Beiträge zur Verbraucherforschung“ als fester Bestandteil des KVF NRW. Kathrin Velewald und Corinna Koch haben die Artikel redaktionell betreut. Unsere Lektorin Heike Plank hat mit ihrer gründlichen Hand die kleinen und großen Schnitzer entdeckt. Aranka Schindler von der Gruppe Publikationen der Verbraucherzentrale Nordrhein-Westfalen hat den Band von der Verlagsseite her betreut.

Literatur

- Bala, Christian und Klaus Müller. 2014. Der gläserne Verbraucher: Konsum und Überwachung. Sozialwissenschaftliche Vorbemerkungen. In: *Der gläserne Verbraucher: Wird Datenschutz zum Verbraucherschutz?*, hg. von Christian Bala und Klaus Müller, 11–40. Bd.1. Beiträge zur Verbraucherforschung. Düsseldorf: Verbraucherzentrale NRW. <http://www.verbraucherzentrale.nrw/bzv1>.
- Bauman, Zygmunt. 2009. *Leben als Konsum*. Hamburg: Hamburger Edition.
- Becker, Kim Björn. 2016. Kassen wollen Daten von Fitness-Armbändern nutzen. *Süddeutsche.de* (8. Februar). <http://www.sueddeutsche.de/wirtschaft/gesundheits-kassen-wollen-daten-von-fitness-armbaendern-nutzen-1.2855193> (Zugriff: 9. März 2016).
- Becker, Matthias Martin. 2014. *Mythos Vorbeugung: Warum Gesundheit sich nicht verordnen lässt und Ungleichheit krank macht*. Wien: Promedia.
- . 2016. Tracken, Checken, Sharen. *Gen-ethischer Informationsdienst*, Nr. 234 (Februar): 35–37.
- Bendrath, Ralf. 2007. Der gläserne Bürger und der vorsorgliche Staat: Zum Verhältnis von Überwachung und Sicherheit in der Informationsgesellschaft. *kommunikation@gesellschaft 8* (Beitrag 7). http://www.soz.uni-frankfurt.de/K.G/B7_2007_Bendrath.pdf.
- Benndorf, Volker, Dorothea Kübler und Hans-Theo Normann. 2015. Privacy concerns, voluntary disclosure of information, and unraveling: An experiment. *European Economic Review 75* (April): 43–59. doi:10.1016/j.euroecorev.2015.01.005.
- Blue Maestro Limited. 2016. Pacif-i: the smart thermometer Pacifier for iOS and Android. <https://www.pacif-i.io/> (Zugriff: 8. März 2016).
- Bohsem, Guido und Ulrich Schäfer. 2016. „Jeder von uns wird so ein Gerät haben“. *Süddeutsche Zeitung* (7. Februar). <http://www.sueddeutsche.de/wirtschaft/montagsinterview-jeder-von-uns-wird-so-ein-geraet-haben-1.2852584?reduced=true> (Zugriff: 9. März 2016).
- Duhigg, Charles. 2009. What does your credit-card company know about you? *The New York Times Magazine* (12. Mai). <http://nyti.ms/1Lwmum3> (Zugriff: 4. März 2016).
- Frankel, Todd C. 2016. Fitbits now mandatory for students at this Oklahoma university. *The Washington Post* (2. Februar). <https://www.washington->

- post.com/news/the-switch/wp/2016/02/02/fitbits-now-mandatory-for-students-at-this-oklahoma-university/ (Zugriff: 3. März 2016).
- Grassmuck, Volker. 2012. Exkursion in die Coy-Galaxis. In: *Per Anhalter durch die Turing-Galaxis*, hg. von Andrea Knaut, Christian Kühne, Rainer Rehak, Stefan Ullrich, Constanze Kurz, und Jörg Pohle, 9–15. Münster: Verl.-Haus Monsenstein und Vannerdat.
- Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari und Andrej Zwitter. 2016. Digitale Demokratie statt Datendiktatur: Das Digital-Mainfest. *Spektrum der Wissenschaft*, Nr. 1: 50–61. <http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933> (Zugriff: 11. März 2016).
- Hofstetter, Yvonne. 2014. *Sie wissen alles: Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen*. München: C. Bertelsmann.
- Jentsch, Nicola. 2016. Auflösung der Privatsphäre – Ende der Solidarität. *DIW Wochenbericht* (8): 168.
- Kafka, Franz. 2005. *Der Prozess: Roman*. Frankfurt am Main: Suhrkamp.
- Latour, Bruno. 1996. *Der Berliner Schlüssel: Erkundungen eines Liebhabers der Wissenschaften*. Berlin: Akademie Verlag.
- Mainzer, Klaus. 2014. *Die Berechnung der Welt: Von der Weltformel zu Big Data*. München: C. H. Beck.
- Mattel, Inc. 2015. Hello Barbie™ Doll – Blonde Hair. *Mattel Shop*. <http://shop.mattel.com/product/index.jsp?productId=65561726> (Zugriff: 2. März 2016).
- Müller, Benedikt. 2016. Digitale Wohnungssuche: Wer sich auszieht, gewinnt. *Süddeutsche Zeitung* (23. März): 15.
- Neumann, Linus. 2015. Technik: „Hello Barbie“. *Big Brother Awards*. <https://bigbrotherawards.de/2015/technik-hello-barbie> (Zugriff: 2. März 2016).
- Pasquale, Frank. 2015. *The black box society: The secret algorithms that control money and information*. Cambridge, Mass.: Harvard University Press.
- Peppet, Scott R. 2015. Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Northwestern University Law Review* 105 (3): 1153-1204. <http://scholarlycommons.law.northwestern.edu/nulr/vol105/iss3/4>.

- Piwek, Lukasz, David A. Ellis, Sally Andrews und Adam Joinson. 2016. The rise of consumer health wearables: promises and barriers. *PLOS Medicine* 13, Nr. 2 (2. Februar): e1001953. doi:10.1371/journal.pmed.1001953.
- Procter & Gamble Service GmbH. 2015. Oral-B SmartSeries. <http://www.oralb-blendamed.de/de-DE/smartseries-app> (Zugriff: 8. März 2016).
- Reichert, Ramón. 2016. Das Politische der Großdatenforschung. *Politikum* 2, Nr. 1: 20–31.
- Reisch, Lucia, Daniela Büchel, Gesche Joost und Zander-Hayat, Helga. 2016. *Digitale Welt und Handel: Verbraucher im personalisierten Online-Handel*. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) beim Bundesministerium der Justiz und für Verbraucherschutz (BMJV). <http://www.svr-verbraucherfragen.de/wp-content/uploads/2016/01/Digitale-Welt-und-Handel.pdf>.
- Sandoval, Marisol. 2012. A critical empirical case study if consumer surveillance on Web 2.0. In: *Internet and surveillance: The challenges of Web 2.0 and social media*, hg. von Christian Fuchs, Kees Boersma, Anders Albrechtslund, und Marisol Sandoval, 147–169. New York: Routledge.
- Schlieter, Kai. 2015. *Die Herrschaftsformel: Wie Künstliche Intelligenz uns berechnet, steuert und unser Leben verändert*. Frankfurt am Main: Westend.
- Schneier, Bruce. 2015. *Data and Goliath: The hidden battles to collect your data and control your world*. New York, NY: Norton.
- Schriirmacher, Dennis. 2015. „Hello Barbie“: Interaktive Barbie gehackt. *heise Security*. 27. November. <http://heise.de/-3025550> (Zugriff: 2. März 2016).
- Selke, Stefan. 2014. *Lifelogging: Wie die digitale Selbstvermessung unsere Gesellschaft verändert*. Berlin: Econ.
- . 2015. Lifelogging oder: Der fehlerhafte Mensch. *Blätter für deutsche und internationale Politik* 60 (5): 79-86.
- Solove, Daniel J. 2004. *The digital person: Technology and privacy in the information age*. New York: New York University Press. <http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm>.
- . 2011. *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press.
- Thielman, Sam. 2016. Fitbit used to track students' physical activity at Oral Roberts University. *The Guardian* (29. Januar). <http://www.theguardian.com>.

com/us-news/2016/jan/29/oral-roberts-university-fitibit-students-physical-fitness-freshman-15 (Zugriff: 3. März 2016).

Weizenbaum, Joseph. 1978. *Die Macht der Computer und die Ohnmacht der Vernunft*. Frankfurt am Main: Suhrkamp.

Windeck, Christof. 2016. Wearables: Nach Fitbit auch Jawbone schwächer bewertet. *heise online*. 17. Januar. <http://heise.de/-3072904> (Zugriff: 9. März 2016).