abida
ASSESSING BIG DATA

# BIG DATA IM BEREICH HEIM UND FREIZEIT

## SMART LIVING: STATUS QUO UND ENTWICKLUNGSTENDENZEN

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

ConPolicy – Institut für Verbraucherpolitik

Dr. Sara Elisa Kettner
Prof. Dr. Christian Thorun

gemeinsam mit:

Stiftung Neue Verantwortung

Jan-Peter Kleinhans

# ABIDA - ASSESSING BIG DATA

## PROJEKTLAUFZEIT 01.03.2015-28.02.2019

Westfälische Wilhelms-Universität Münster,
Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung

Karlsruher Institut für Technologie,
Institut für Technikfolgenabschätzung und Systemanalyse (ITAS)

Leibniz Universität Hannover
Institut für Rechtsinformatik
(IRI)

Technische Universität Dortmund,
Wirtschafts- und Sozialwissenschaftliche Fakultät (WiSo) Techniksoziologie

Ludwig-Maximilians-Universität München,
Forschungsstelle für Information, Organisation und Management (IOM)

Wissenschaftszentrum
Berlin für Sozialforschung

## ABIDA - Assessing Big Data
## Über das Gutachten

Das Gutachten wurde im Rahmen des ABIDA-Projekts mit Mitteln des Bundesministeriums für Bildung und Forschung erstellt. Der Inhalt des Gutachtens gibt ausschließlich die Auffassungen der Autoren wieder. Diese decken sich nicht automatisch mit denen des Ministeriums und/oder der einzelnen Projektpartner.

ABIDA lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung.

www.abida.de
© 2018 – Alle Rechte vorbehalten

# ZUSAMMENFASSUNG

Unser Alltag und Privatleben werden immer mehr durch die Digitalisierung geprägt und so ist es kaum verwunderlich, dass auch das Haus und die Freizeit von Verbraucherinnen und Verbrauchern immer stärker vernetzt und digital gestaltet werden. Zwar ist die Verbreitung von Smart Living-Anwendungen bisher relativ gering, es gibt jedoch ein immenses Potential für diese auf dem Massenmarkt. Big Data spielt dabei bereits eine große Rolle und wird auch in Zukunft immer intensiver genutzt werden, um Smart Living-Dienste zu optimieren.

Bisher existiert jedoch keine systematische Untersuchung des Einsatzes von Big Data im Bereich Smart Living. Diese Lücke soll das zugrundeliegende Gutachten schließen und zielt deshalb darauf ab, einen Überblick über datengetriebene Smart Living-Anwendungen zu geben. Darüber hinaus sollen notwendige Handlungsbedarfe hinsichtlich informationeller Selbstbestimmung, User-Profiling und IT-Sicherheit im Bereich Smart Living und Big Data identifiziert und Handlungsempfehlungen entwickelt werden. Das Gutachten wurden zwischen September 2017 und Februar 2018 erstellt und basiert methodisch auf den Ergebnissen einer Literaturanalyse, Experteninterviews und Expertenworkshops.

Aus der Perspektive der Verbraucherinnen und Verbraucher existiert derzeit noch eine Reihe von Hürden für die Nutzung von Smart Living-Anwendungen: Neben dem Preis, der mangelnden Nutzbarkeit und inkompatiblen Protokollen werden Sicherheits- und Privatsphärebedenken genannt. Um diese Hürden zu überwinden, sind auf dem Markt Bestrebungen zu beobachteten, um den Wünschen der Verbraucherinnen und Verbraucher besser zu begegnen. So werden Anwendungen in Zukunft besser zusammenspielen und Funktionen in das Haus integrieren, die bisher außerhalb des Hauses lagen. Zusätzlich und einhergehend mit technischen Entwicklungen wird außerdem prognostiziert, dass die Sprachsteuerung an Bedeutung gewinnen wird und die Gestensteuerung ein Potential für den Smart Living Markt birgt.

Auch aus Anbieterperspektive ist der Smart Living-Markt in Bewegung. So befinden sich auf dem Markt unterschiedliche Akteure, die neue Produkte und Anwendungen durch Partnerschaften anbieten wollen. Überdies werden durch den Einsatz von Big Data alte Geschäftsmodelle gestärkt oder neue Geschäftsmodelle geschaffen. Eine besondere Bedeutung auf dem Smart Living-Markt wird den Plattformen beigemessen, die die Interoperabilität der Anwendungen gewährleisten. Insgesamt ist außerdem zu beobachten, dass im Bereich des Smart Homes Branchengrenzen verschwimmen und Anbieter neue Bereiche entlang der Wertschöpfungskette erschließen.

Neben diesem vielversprechenden Ausblick zur Entwicklung neuer, hilfreicher Smart Living-Anwendungen und den Erfolgschancen relevanter Marktakteure, existieren aus Verbrauchersicht jedoch auch Bedenken. Gerade in den Bereichen Datenschutz, Datenweitergabe an Dritte und IT-Sicherheit stehen Verbraucherinnen und Verbraucher, Anbieter und Gesetzgeber Herausforderungen gegenüber:

i) Informationelle Selbstbestimmung: Die in der Studie durchgeführte Analyse ausgewählter Datenschutztexte im Bereich smarter Beleuchtung, Videokameras und Sprachassistenten zeigt, dass diese oftmals hinter den gesetzlichen Vorgaben zurückbleiben. So haben einige Produkte keine Datenschutzerklärung oder bieten diese lediglich in englischer Sprache an. Außerdem sind die Texte insgesamt sehr lang, komplex und nur selten werden gestalterische Elemente eingesetzt, die das Lesen der Verbraucherinnen und Verbraucher unterstützen. Bei App-gesteuerten Produkten fällt außer-

dem auf, dass technische Zugriffe auf das Smartphone gewährt werden, bei den Zweifel bestehen, wie plausibel diese Zugriffe tatsächlich sind. Auch wenn die Ergebnisse nicht repräsentativ sind, werfen sie einige Fragen für den Datenumgang von Smart Home-Anwendungen auf. Über die empirische Auswertung hinaus, werden außerdem eine Reihe psychologischer Hürden dargestellt und deren Bedeutung für das Verhalten von Verbraucherinnen und Verbrauchern beleuchtet. Hierzu zählen beispielsweise eine mangelnde Kontrollüberzeugung, soziale Normen, Habituation, Heuristiken, Selbstregulationsdefizite und Vertrauen.

ii) Umgang mit Nutzerdaten: Die Ergebnisse zeigen, dass User-Profiling in Smart Home-Anwendungen bislang nicht so umfassend und allgegenwärtig geschieht, wie dies bei heutigen Online-Diensten und Apps der Fall ist. Bisher hängt es sehr stark von der jeweiligen Smart Home-Anwendung und dem Hersteller ab, ob und inwieweit eine Datenerfassung und -analyse zu Zwecken des Profilings stattfindet. Nichtsdestotrotz lässt sich schon heute in bestimmten Anwendungsbereichen (Sprachassistenten und Smart-TVs) absehen, dass durch User-Profiling potenziell tiefgreifende Rückschlüsse auf die Lebensgewohnheiten der Nutzerinnen und Nutzer möglich sind. Dies stellt Gesetzgeber und Gesellschaft u.a. hinsichtlich Drittbetroffenheit und Schutz der Privatsphäre vor signifikante Herausforderungen.

iii) Sicherheitsrisiken: Die Ergebnisse zeigen, dass der Markt derzeit versagt, verhältnismäßig vertrauenswürdige Smart Home-Anwendungen zu produzieren. Viele Smart Home-Anwendungen sind einfach, voll-automatisiert und massenhaft durch Kriminelle zu kompromittieren und stellen als Teil von Botnetzen eine direkte Gefahr für Dritte dar. Hier besteht dringender Handlungsbedarf durch den Gesetzgeber hinsichtlich verbindlicher Mindeststandards, einer gerechteren Verteilung von Verantwortlichkeiten zwischen Herstellern, Betreibern und Nutzerinnen und Nutzern sowie dem Abbau von Intransparenz am Markt.

Aus den Ergebnissen leiten sich die folgenden 12 Handlungsempfehlungen ab. Die ersten zehn beziehen sich auf die Problemfelder im Bereich der informationellen Selbstbestimmung, des User-Profilings und der IT-Sicherheit. Die letzten beiden Empfehlungen sind übergeordnet und beziehen sich auf weitere relevante Problemfelder:

1. Handlungsempfehlung: Es bedarf einer konsequenten Rechtsdurchsetzung durch Behörden und Verbraucherorganisationen, um gesetzeswidrige Datenschutzpraktiken zu ahnden und auf Missstände hinzuweisen. Die neuen schärferen Sanktionsmöglichkeiten, die aus der Datenschutzgrundverordnung resultieren, sollten konsequent angewendet werden.
2. Handlungsempfehlung: Um die Komplexität zu reduzieren und den Zugang zu Datenschutzerklärungen zu erleichtern, sind Tools für Verbraucherinnen und Verbraucher hilfreich. Hierzu zählen insbesondere Privacy Bots, die den Verbraucherinnen und Verbrauchern mehr Selbstbestimmtheit und Kontrolle ermöglichen können. Die Entwicklung solcher Technologien sollte gefördert werden.
3. Handlungsempfehlung: Intermediäre wie Smart Home-Plattformen oder Steuerungseinheiten sollten beim Datenschutz mehr in den Fokus genommen werden. So könnten diese beispielsweise das Gesamtrechtemanagement aller über die Plattform gesteuerten Smart Home-Anwendungen übernehmen. Auf diese Weise könnten die Privatsphärepräferenzen aller sich im Smart Home befindlichen Anwendungen effektiv gesteuert werden.
4. Handlungsempfehlung: Der selbstbestimmte Umgang von Verbraucherinnen und Verbrauchern mit ihren personenbezogenen Daten sollte gestärkt werden, so dass die Motivation, sich mit Datenschutztexten auseinanderzusetzen und die Informiertheit gestärkt wird. Dies

könnte beispielsweise durch Anzeige von Datenschutztexten by Default, der Ausgestaltung differenzierter Einwilligungssituationen oder Kampagnen für Verbraucherinformation erreicht werden.

5. Handlungsempfehlung: Es braucht klare Regeln durch den Gesetzgeber, inwieweit zum Kaufzeitpunkt vorhandene und zugesicherte Funktionalität im Nachhinein durch den Hersteller an erweitere Datenanalyse oder User-Profiling geknüpft werden darf.
6. Handlungsempfehlung: Unternehmen sollten Auskunft über strategische Partnerschaften und Informationsquellen von Smart Home-Anwendungen geben. Die Informationen könnten beispielsweise über dieselbe Plattform zur Verfügung gestellt werden, über die Verbraucherinnen und Verbraucher auch ihre Accountdaten verwalten.
7. Handlungsempfehlung: Es mangelt nicht an Sicherheits-Guidelines, vielmehr können die vorhandenen als Grundlage für weitere regulatorische Interventionen (Siegel, Mindestanforderungen) genommen werden. Der Fokus sollte darauf liegen, Anreize für Hersteller zu schaffen, die vorhandenen Best Practices zu befolgen.
8. Handlungsempfehlung: Siegel sollten lediglich als *ein* Baustein einer nachhaltigen IT-Sicherheitspolitik betrachtet werden. Damit sie tatsächlich Informationsasymmetrien zwischen Herstellern und Verbraucherinnen und Verbrauchern abbauen, müssen die Rahmenbedingungen richtig gesetzt werden.
9. Handlungsempfehlung: Da Safety (Produktsicherheit) und Security (IT-Sicherheit) voneinander abhängen, sollten europaweite Mindestanforderungen für beide Aspekte definiert werden. Dies könnte als Ko-Regulierungsansatz zusammen mit der Industrie geschehen, indem sektorspezifische Mindestanforderungen definiert werden und dadurch IT-Sicherheit Teil der CE-Konformitätstests wird. Für eine effektive und effiziente Überwachung der Einhaltung durch Marktteilnehmer, benötigt es jedoch eine umfassende Modernisierung des derzeitigen CE-Ökosystems aus Testlaboren, Standardisierung und Marktüberwachung.
10. Handlungsempfehlung: Die Ausweitung der Produkthaftung auf Softwarebestandteile ist eine notwendige aber keine hinreichende Bedingung zur Stärkung der IT-Sicherheit in Smart Home-Anwendungen. Der Fokus sollte auf einer gerechteren Verteilung von Rechten und Pflichten zwischen Hersteller, Betreiber und Nutzerin und Nutzer liegen.
11. Handlungsempfehlung: Trotz der großen Chancen, die sich aus der Vernetzung von Hausgeräten ergeben, sollten Anwendungen nicht um jeden Preis und vollständig vernetzt werden. So müssen Verbraucherinnen und Verbraucher die Möglichkeit behalten, auch nicht-vernetzte Produkte zu nutzen.
12. Handlungsempfehlung: Die Forschung zu den Auswirkungen des Smart Homes auf Verbraucherinnen und Verbraucher sollte ausgeweitet und gefördert werden.

# VORBEMERKUNGEN UND DANKSAGUNGEN

Dieses Gutachten fasst die inhaltlichen Ergebnisse des Forschungsvorhabens „Big Data im Bereich Heim und Freizeit – Smart Living: Status Quo und Entwicklungstendenzen“ zusammen, die im Zeitraum von September 2017 bis Februar 2018 erstellt wurden.

In diesem Zusammenhang möchten wir uns herzlich bei einer Vielzahl von Personen bedanken, die uns bei der Umsetzung dieser Studie mit Ihrer Expertise und Ihren Hinweisen unterstützt haben. Hierzu zählen die Expertinnen und Experten, die wir im Rahmen der Experteninterviews und der beiden Expertenworkshops befragen konnten. Zum anderen möchten wir uns beim Auftraggeber und den Projektbetreuer an der Westfälische Wilhelms-Universität Münster und am Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), insbesondere Herrn Dr. Siemoneit, bedanken.

Inhaltsverzeichnis


1 Einleitung ... 9
1.1 Zielsetzung und Fragestellung ... 10
1.2 Methodische Vorüberlegungen und Methodisches Vorgehen ... 12
1.2.1 Methodische Vorüberlegungen ... 12
1.2.2 Methodisches Vorgehen ... 15
1.3 Aufbau des Gutachtens ... 15
2 Anwendungen und Verbraucherperspektive ... 17
2.1 Einleitung und Abgrenzung ... 17
2.1.1 Definition ... 17
2.1.2 Vernetzung und Automatisierung ... 18
2.1.3 Anwendungsbereiche ... 18
2.2 Rolle von Big Data in Anwendungen ... 21
2.3 Verbraucherperspektive ... 22
2.3.1 Kenntnis der Anwendungen und Informiertheit ... 22
2.3.2 Aktuelle Verbreitung der Anwendungen ... 23
2.3.3 Interesse an den Anwendungen ... 24
2.3.4 Verbraucherhürden ... 25
2.4 Entwicklungstendenzen ... 27
2.5 Zusammenfassung ... 28
3 Markt- und Anbieterlandschaft ... 30
3.1 Relevante Marktakteure und deren Rollen ... 30
3.1.1 Veränderungen in der Akteurslandschaft ... 31
3.1.2 Erfolgsfaktoren und Gründe für Veränderungen in der Akteurslandschaft ... 32
3.2 Aktuelle und künftige Geschäftsmodelle ... 33
3.3 Die Rolle von Big Data für Anbieter ... 33
3.4 Partnerschaften ... 34
3.5 Zusammenfassung ... 35
4 Informationelle Selbstbestimmung und Transparenz ... 36
4.1 Methodik und Stichprobe ... 36
4.2 Festlegung der Bewertungskriterien ... 38
4.2.1 Notwendige Bedingungen - Datenschutzerkärung vorhanden und in deutscher Sprache ... 38
4.2.2 Kontaktmöglichkeiten für datenschutzrechtliche Anliegen ... 39
4.2.3 Verbraucherrealität und situationale Faktoren ... 39
4.2.4 Inhalte der Datenschutztexte ... 40
4.2.5 Technische Zugriffe und Berechtigungseinstellungen zur Datenerhebung (App-Spezifisch) ... 41
4.3 Ergebnisse ... 42

4.3.1 Notwendige Bedingungen – Datenschutzerklärung vorhanden und in deutscher Sprache ... 42
4.3.2 Kontaktmöglichkeiten für datenschutzrechtliche Anliegen ... 43
4.3.3 Verbraucherrealität und situationale Faktoren ... 44
4.3.4 Inhalte der Datenschutztexte ... 46
4.3.5 Technische Zugriffe und Berechtigungseinstellungen zur Datenerhebung (App-Spezifisch) ... 47
4.4 Weitere Faktoren / Personale Faktoren ... 48
4.5 Zusammenfassung ... 49
5 Umgang mit Nutzerdaten: User-Profiling und Datenweitergabe ... 51
5.1 Bedeutung und Zwecke des User-Profilings aus Anbieterperspektive ... 51
5.2 Datenhandel und -weitergabe an Dritte ... 52
5.2.1 Punktueller Datenhandel durch einzelne Hersteller ... 52
5.2.2 Machtkonzentration bei Sprachassistenten ... 53
5.2.3 Marktplätze ... 53
5.3 Konsequenzen des User-Profilings für Verbraucherinnen und Verbraucher ... 53
5.3.1 Intransparenz und Manipulation ... 54
5.3.2 Staatliche Zugriffsmöglichkeiten ... 55
5.3.3 Komplexität des Smart Homes ... 55
5.4 Zusammenfassung ... 56
6 Sicherheitsrisiken ... 57
6.1 Relevante Sicherheitsrisiken und Beispiele ... 57
6.2 Ursachen für Sicherheitsrisiken ... 59
6.3 Zusammenfassung ... 60
7 Problemsynthese, Lösungsansätze und Handlungsempfehlungen ... 62
7.1 Informationelle Selbstbestimmung ... 62
7.1.1 Rechtliche Vorgaben konsequent durchsetzen ... 62
7.1.2 Verbesserung der Informiertheit durch Überwindung DSE-inhärenter Hürden ... 63
7.1.3 Zugang zur Datenschutzerklärung verbessern ... 67
7.1.4 Datenmanagement durch Plattformen ermöglichen ... 68
7.1.5 Verbrauchermotivation und Verbraucherbildung stärken ... 68
7.2 Umgang mit Nutzerdaten ... 70
7.2.1 Zugesicherte Funktionalität ... 71
7.2.2 Transparenz über Partnerschaften schaffen ... 72
7.3 Sicherheitsrisiken ... 73
7.3.1 Capacity Building und Best Practices ... 73
7.3.2 Informationsasymmetrien zwischen Herstellern und Verbraucherinnen und Verbrauchern abbauen ... 74
7.3.3 Unverhältnismäßig unsichere Geräte vom Markt ausschließen ... 76
7.3.4 Hersteller stärker zur Verantwortung ziehen ... 77
7.4 Weitere Problemfelder ... 77
7.4.1 Datensparsame Anwendungen fördern und Recht auf „analoge Welt“ stärken ... 78

7.4.2 Forschungsbedarfe identifizieren und angehen ..... 78
8 Literatur ..... 80
9 Appendix ..... 89
9.1 Experteninterviews ..... 89
9.2 Informationelle Selbstbestimmung – Ausgewählte Anwendungen ..... 90

Tabellenverzeichnis

Tabelle 1: Anwendungsbereiche und Produktbeispiele für Smart Living-Anwendungen ..... 20
Tabelle 2: Unterscheidung von Smart Home-Systemen und -Plattformen ..... 31
Tabelle 3: Bewertungskriterium und Indikatoren zu notwendigen Bedingungen ..... 39
Tabelle 4: Bewertungskriterium und Indikator zu Kontaktmöglichkeiten für datenschutzrechtliche Anliegen ..... 39
Tabelle 5: Bewertungskriterien und Indikatoren zu situationalen Faktoren ..... 40
Tabelle 6: Bewertungskriterium und Indikatoren zu ungenauen Formulierungen ..... 41
Tabelle 7: Bewertungskriterien und Indikatoren zu technischen Zugriffen ..... 42
Tabelle 8: Ergebnisse zu notwendigen Bedingungen ..... 43
Tabelle 9: Ergebnisse zu Kontaktmöglichkeiten für datenschutzrechtliche Anliegen ..... 44
Tabelle 10: Ergebnisse zu situationalen Faktoren ..... 44
Tabelle 11: Ergebnisse zu technischen Zugriffen ..... 48
Tabelle 12: Ausgewählte Anwendungen, die bei der Analyse der Datenschutzerklärungen berücksichtigt wurden ..... 90

Abbildungsverzeichnis

Abbildung 1: Verbraucherhürden im Smart Home ..... 27
Abbildung 2: Beispiel - Datenschutzerklärung mit Navigationsleiste ..... 45
Abbildung 3: Beispiel - Datenschutzerklärung mit Drill-Down-Menü ..... 46
Abbildung 4: Psychologische Faktoren, die die informationelle Selbstbestimmung beeinflussen .. 49
Abbildung 5: Beispiel - Datenschutzsiegel ..... 64
Abbildung 6: Beispiel - One-Pager ..... 65
Abbildung 7: Beispiel - Interaktive Datenschutzerklärung ..... 66

## Abkürzungsverzeichnis

| | |
|---|---|
| AAL | Ambient Assisted Living |
| API | Application Programming Interface |
| BDSG | Bundesdatenschutzgesetz |
| Bitkom | Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. |
| BMJV | Bundesministerium der Justiz und für Verbraucherschutz |
| BMWi | Bundesministerium für Wirtschaft und Energie |
| BMZ | Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| DCTI | Deutsches CleanTech Institut |
| DIVSI | Deutsches Institut für Sicherheit und Vertrauen im Internet |
| DSE | Datenschutzerklärung |
| DSGVO | Datenschutzgrunverordnung |
| DsiN | Deutschland sicher im Netz |
| GftD | Gesellschaft für transparenten Datenschutz mbH |
| IoT | Internet of Things |
| ML | Maschine Learning |
| PwC | PricewaterhouseCoopers GmbH |
| SDK | Software Development Kit |
| SVRV | Sachverständigenrat für Verbraucherfragen |

# 1 EINLEITUNG

Unser Alltag und Privatleben werden immer mehr durch die Digitalisierung geprägt. Das GfK-Handelspanel belegt, dass sogenannte Smart Home-Anwendungen auch in deutschen Haushalten immer beliebter werden (GfK, 2016a). Demnach besitzen beispielsweise über 40% der Haushalte bereits einen Smart TV und 60% der Anfang 2016 auf dem deutschen Markt verkaufen Fernsehgeräte hatten eine Smart-Funktion (GfK, 2016b). Laut einer Statista-Umfrage (2016a) fand die Mehrheit der Befragten unter 50 Jahren das Thema Smart Home interessant oder sogar sehr interessant, bei den 18-29-Jährigen lag der Anteil sogar über 80%.

Während sich smarte Unterhaltungselektronik am häufigsten verkauft, steigt auch die Beliebtheit von vernetzten Haushaltsgroßgeräten, wie etwa smarten Waschmaschinen sowie smarte Sicherheitstechnologie und Heimautomatisierung, wie etwa vernetzbare Rauchmelder, smarte Überwachungskameras oder selbststeuernde Rollläden (GfK, 2016a). Weitere Bereiche, in denen smarte Anwendungen Einzug halten, sind das Energiemanagement (etwa über Smart Meter und selbstregulierende Heizungsthermostate) und Sprachassistenzsysteme bis hin zur häuslichen Pflege („Ambient Assisted Living"-Anwendungen wie etwa Vitalfunktionsmessungs- und Sturzerkennungs-Systeme).

Betrachtet man darüber Smart Living-Anwendungen im weiteren Sinne, können der Liste noch „Connected Cars" und smart Watches, sonstige Wearables bzw. smarte Kleidung sowie Smartphones und Tablets hinzugefügt werden, deren räumliche Nutzung über den privaten häuslichen Bereich hinausgeht.

Als Gründe für die Nutzung von Smart Home-Anwendungen nennen Verbraucherinnen und Verbraucher in der Studie von Deloitte und der TU München (2015) etwa eine Steigerung des persönlichen Komforts, eine Erhöhung der Wohnsicherheit, eine Reduktion der Energiekosten sowie Entertainment und Spaß bei der Nutzung. Jedoch nicht alle Deutschen sehen Smart Home-Anwendungen durchweg positiv. In einer Umfrage von Splendid Research (2017) empfanden 65% der Befragten die steigende Automatisierung ihres Zuhauses als unheimlich, fast 60% befürchteten, Opfer von Hackerangriffen zu werden und 54% sorgten sich um ihre Privatsphäre.

Tatsächlich sammeln die smarten Anwendungen quasi kontinuierlich große Mengen an Daten über ihre Nutzerinnen und Nutzer sowie deren Umfeld. Durch die stetige Aufzeichnung der Daten lassen sich teilweise detaillierte Nutzungs- und Verhaltensprofile erstellen, etwa über Abwesenheitszeiten von Haushaltsmitgliedern oder Präferenzen bzw. Gewohnheiten dieser. Insbesondere im Gesundheitsbereich, etwa bei Fitness-Armbändern oder bei Ambient Assisted Living-Anwendungen, handelt es sich bei den gesammelten Daten teilweise um besonders sensible, persönliche Informationen. Sprachassistenzsysteme oder Devices mit Mikrofon können überdies auch persönliche Informationen aus Gesprächen aufzeichnen, etwa von Haushaltsmitgliedern untereinander – jedoch auch von Besucherinnen und Besuchern, die im Haushalt zu Gast sind. Durch die Vernetzung der Anwendungen untereinander können die gesammelten Daten zudem in Echtzeit zusammengeführt werden, wodurch noch detailliere und umfassendere Profile über die Nutzerinnen und Nutzer und ihr Umfeld ermöglich werden.

Die generierten Datenmassen sind teilweise mit konventionellen Methoden der Datenverarbeitung nicht mehr auswertbar und werden häufig mit dem Begriff „Big Data" bezeichnet. Big Data zeichnet sich insbesondere durch drei Charakteristika aus: die enorme Datenmenge (Volume), die hohe Geschwindigkeit des Datenverkehrs (Velocity) und die unterschiedliche Beschaffenheit und Komplexi-

tät der Daten (Variety), die verschiedene Datenquellen und Strukturen zusammenführt (vgl. z.B. Wissenschaftliche Dienste des Deutschen Bundestages, 2013). Darüber hinaus sind aus unternehmerischer Sicht zwei weitere Vs relevant, nämlich Veracity (Richtigkeit der Daten) und Value (Wert) (Marr, 2015). Laut einer Analyse des Branchenverbands Bitkom (2012) zielt die Auswertung der Datenmassen (Big Data-Analytics) meist auf das Erkennen von Zusammenhängen, Bedeutungen und Mustern in den Daten ab, um u.a. Vorhersagen über die Zukunft treffen zu können oder Anomalien zu erkennen. Unternehmen erkennen zunehmend die wirtschaftliche Bedeutung von Big Data und versuchen, Big Data-Analytics gewinnbringend einzusetzen. Eine neue Qualität der Daten kann im Big Data-Bereich etwa dadurch erreichet werden, dass Daten kombiniert werden, die vorher keinen Bezug zueinander hatten, unter anderem da sie technisch vorher nicht ausgewertet werden konnten. Die neuen Möglichkeiten der Datenanalyse über Big Data-Methoden werden jedoch nicht nur positiv beurteilt. Insbesondere bei der Nutzung personenbezogener Daten für Big Data-Anwendungen sehen Kritiker das Recht auf informationelle Selbstbestimmung, den Schutz persönlicher Daten und die Zweckbindung von erhobenen Daten nicht gewährleistet, insbesondere da die Zusammenführung verschiedener Datenquellen häufig eine De-Anonymisierung ermöglicht (vgl. Wissenschaftliche Dienste des Deutschen Bundestages, 2013).

Die Vernetzung der Smart Home-Anwendungen untereinander hat zudem nicht nur Implikationen bezüglich der gesammelten Daten und deren Konsequenzen auf die informationelle Selbstbestimmung, sondern auch im Hinblick auf die technische Sicherheit von Anwendungen. Schlecht gesicherte Smart Home-Anwendungen, die mit anderen vernetzt sind, können von Hackern als Angriffspunkte genutzt werden, um sich unbefugt Zugriff zum Gesamtsystem zu verschaffen. Wissenschaftler haben am Beispiel von smarten Glühbirnen gezeigt, dass sich z.B. ein Computerwurm leicht einschleusen lässt und vernetzte andere Geräte darüber infizieren lassen (Markoff, 2016; Ronen et al., 2017). So können vermeintlich unkritische Anwendungen wie Glühbirnen zum Sicherheitsrisiko für deutlich kritischere Anwendungen wie smarte Türschlösser werden.

Viele Nutzerinnen und Nutzer von Smart Home-Anwendungen setzen sich mit solchen Datenschutz- und Sicherheitsaspekten im Alltag eher wenig auseinander. In einer Statista-Umfrage (2016b) geben über 60% der Befragten an, über das Thema Smart Home entweder nicht gut oder sogar gar nicht gut informiert zu sein. Zudem kommt hinzu, dass die Praktiken der Anbieter, die Verbraucherinnen und Verbraucher über die Nutzungsbedingungen, den Umgang mit ihren Daten und eventuelle Sicherheitsrisiken oder die Verantwortung für Sicherheitsupdates zu informieren bzw. ihre Einwilligung dazu einzuholen, häufig an den Nutzerbedürfnissen vorbeigehen (vgl. Bitkom, 2015a; DIVSI, 2015).

Durch die rasante Entwicklung der Smart Home-Anwendungen in den letzten Jahren besteht teilweise noch großer Forschungsbedarf zur derzeitigen Situation sowie bezüglich praktikabler und angemessener Lösungsansätze.

## 1.1 ZIELSETZUNG UND FRAGESTELLUNG

Ziel dieses Vorhabens ist es, einen Überblick über datengetriebene Smart Living-Anwendungen zu geben, eventuell notwendige Handlungsbedarfe hinsichtlich informationeller Selbstbestimmung, User-Profiling und IT-Sicherheit zu identifizieren und Handlungsempfehlungen zu entwickeln.

Hierfür wird zunächst eine Analyse des Ist-Zustandes für die verschiedenen Smart Living-Anwendungen durchgeführt. Als Grundlage hierfür wird ein strukturierter Überblick über die verschiedenen Anwendungen im Smart Living-Bereich erstellt und die Rolle von Big Data sowie deren

Anwendungsziele untersucht. Danach werden die Akteure im Markt, deren Bedeutung und Rollen sowie beobachtbare Veränderungen analysiert. Auch hier wird die Bedeutung von Big Data in Geschäftsmodellen genauer beleuchtet und strategische Partnerschaften der Marktakteure analysiert.

Des Weiteren untersucht das Gutachten den Umgang der Anbieter mit Daten aus der Nutzung von Smart Living-Anwendungen. Hierbei werden insbesondere Praktiken von Smart Home-Anbietern bei der Nutzer-Information und bezüglich Transparenzpflichten behandelt. Folgend werden Aspekte des Nutzer-Profilings und der Datenweitergabe beleuchtet. Zudem werden Aspekte der technischen Sicherheit der Smart Living-Anwendungen erforscht.

Die gewonnenen Erkenntnisse zu den Praktiken bei der Nutzer-Information, zum Umgang mit Nutzerdaten und zur technischen Sicherheit der Anwendungen werden jeweils Überlegungen zu idealtypischen Bedingungen gegenübergestellt.

Die verschiedenen Erkenntnisse zu den wünschenswerten Zuständen und den identifizierten Defiziten werden anschließend zusammengeführt und Lösungsansätze themenübergreifend ausgearbeitet. Hierbei werden verschiedene Governance-Instrumente identifiziert und diskutiert.

Final werden die Erkenntnisse synthetisiert und hieraus Handlungsempfehlungen abgeleitet.

Zur Erreichung dieser Zielsetzung werden die folgenden Themenkomplexe mit zugehörigen Leitfragen adressiert:

1. Anwendungen und Verbraucherperspektive: Welche Smart Living-Anwendungen existieren bereits? Wie lassen sich die Smart Living-Anwendungen typisieren? Welche Anwendungen haben einen Bezug zu Big Data und welchen? Welche Informationen liegen zum Verbreitungsgrad und der Motivation der Verbraucherinnen und Verbraucher, diese zu nutzen, vor? Welche Verbraucherhürden existieren? Welche zukünftigen Entwicklungen zeichnen sich ab?
2. Markt- und Anbieterlandschaft: Welche Marktakteure gibt es? Welche Bedeutung und welche Rolle haben sie jeweils? Wie verändert sich die Rolle und Bedeutung der Akteure sowie die Struktur des Marktes? Welche Gründe lassen sich für Veränderungen, insbesondere im Hinblick auf Bedeutungsgewinn oder -verlust von Akteuren, finden? Welche Rolle spielt Big Data in den Geschäftsmodellen? Welche strategischen Partnerschaften sind zu beobachten? Inwiefern führen die Marktakteure Leistungen selbst aus oder kaufen Leistungen von anderen Akteuren ein?
3. Informelle Selbstbestimmung und Transparenz: Welche Praktiken der Anbieter von Smart Living-Anwendungen zur Information der Nutzerinnen und Nutzer sind gängig? Inwiefern erfüllen die beobachteten Praktiken Erwartungen des Gesetzgebers und der Verbraucher- und Datenschutzorganisationen? Lassen sich bestimmte Praktiken als besonders positiv oder negativ hervorheben? Welche weiteren Faktoren spielen eine Rolle für die Informiertheit der Verbraucherinnen und Verbraucher?
4. Umgang mit Nutzerdaten – User-Profiling und Datenweitergabe: Welche Bedeutung hat das User-Profiling im Bereich Smart Living? Welcher Zweck wird damit verfolgt? Inwiefern spielt der Datenhandel und die (entgeltliche oder auch unentgeltliche) Datenweitergabe an Dritte eine Rolle? Welche Bedeutung und Rolle haben diesbezüglich Handelsplattformen? Wie sind die Zugriffs- und Nutzungsmöglichkeiten auf die Daten verteilt und bestehen diesbezüglich Hinweise auf Machtkonzentrationen bei bestimmten Akteuren? Welche Aussagen können über eine aus Verbrauchersicht wünschenswerte Verteilung und Ausgestal-

tung der Datenzugriffs- und Nutzungskompetenzen durch die Smart Living-Anbieter oder Dritte getroffen werden?

5. Sicherheitsrisiken: Welche Sicherheitsrisiken sind bereits bekannt oder absehbar? Welche Ursachen gibt es für die identifizierten Sicherheitsrisiken? Welche Rolle spielen Hersteller und Nutzerinnen und Nutzer beim Umgang mit Sicherheitslücken?
6. Problemsynthese, Lösungsansätze und Handlungsempfehlungen: Welche Rahmenbedingungen wären aus Verbraucher-, Datenschutz- und Datensicherheitssicht wünschenswert? In welchen Bereichen besteht Regulierungsbedarf und auf welcher politischen Ebene (national, EU, international)? Welche Governance-Instrumente zur Lösung der identifizierten Probleme kann man bereits beobachten und wie sind diese zu bewerten? Welche weiteren wären denkbar und sinnvoll? Welche Implikationen für die Verbraucherpolitik und andere Politikbereiche ergeben sich aus den Ergebnissen? Welche konkreten Handlungsempfehlungen im Umgang mit Smart Living und speziell Big Data und Smart Living resultieren? Welchen unerwünschten Entwicklungen sollte die Politik entgegenwirken und wie sollte sie dies tun? Welche positiven Entwicklungen sollte die Politik fördern und wie sollte sie dies tun? Welche Anknüpfungspunkte gibt es bereits?

## 1.2 METHODISCHE VORÜBERLEGUNGEN UND METHODISCHES VORGEHEN

### 1.2.1 METHODISCHE VORÜBERLEGUNGEN

Ist- und Soll-Analyse: Zum einen wird die Studie in eine strukturierte Analyse des Ist-Zustandes bezüglich der verschiedenen zu untersuchenden Aspekte gegliedert. Zum anderen werden Aussagen über einen idealtypischen Sollzustand herausgearbeitet. Ist- und Soll-Zustand werden im Schlussteil gegenübergestellt.

Aus Sicht des Verbraucher- und Datenschutzes und der Datensicherheit wünschenswerte Bedingungen: Um vorhandene Defizite bezüglich des Ist-Zustands aufzeigen zu können, müssen Annahmen über aus Sicht des Verbraucher- und Datenschutzes und der Datensicherheit idealtypische Bedingungen getroffen werden. Um den Bedürfnissen der Verbraucherinnen und Verbraucher gerecht zu werden, sollten Smart Home-Anwendungen insbesondere folgende grundlegende Anforderungen erfüllen. Sie sollten:

- technisch vertrauenswürdig sein.
- die informationelle Selbstbestimmung der Nutzerinnen und Nutzer und ihres Umfeldes nicht kompromittieren und ermöglichen.
- Nutzerinnen und Nutzer ausreichend und verständlich über die Nutzungsbedingungen und die damit einhergehenden Implikationen informieren.
- einen ausreichenden Schutz personenbezogener Daten sicherstellen.

Im Rahmen der einzelnen Kapitel ergeben sich jedoch auch weitere themenspezifische Anforderungen an Smart Living-Anwendungen. Hierbei gilt es zu beachten, dass bei der Analyse der Transparenzpflichten keine vollständige juristische Prüfung vorgenommen wird, sondern vor allem Ergebnisse aus der verhaltenswissenschaftlichen und verbraucherpolitischen Literatur berücksichtigt werden.

Auswahl der Anwendungs-Hot-Spots: Aufgrund der Breite an möglichen Smart Home-Anwendungen und dem Umfang der Studie war eine Eingrenzung des Fokus auf bestimmte Anwen-

dungen notwendig. Viele Erkenntnisse, gerade mit Blick auf die Handlungsempfehlungen, lassen sich auf andere Smart Home-Anwendungen übertragen, gleichzeitig unterscheiden sich Smart Home-Anwendungen in bestimmten Bereichen, die eine eigene Würdigung erfordern. Im Folgenden werden daher die zentralen Anforderungen beschrieben, die bei der Auswahl der zu untersuchenden Smart Home-Anwendungen ausschlaggebend waren.

- Marktdurchdringung: Jede der ausgewählten Smart Home-Anwendungen muss eine hohe Marktdurchdringung, derzeitig oder zukünftig absehbar, besitzen. Hintergrund ist, dass die analysierten Smart Home-Anwendungen eine möglichst hohe Relevanz für bzw. Nachfrage durch Verbraucherinnen und Verbraucher haben sollten.
- Unterschiedliche Anwendungsbereiche: Jede der ausgewählten Smart Home-Anwendungen muss einem anderen Anwendungsbereich (Unterhaltungselektronik, Haushaltsgeräte und Heimtechnik, Energiemanagement, Sicherheits- und Kontrollsysteme, etc.) zuzuordnen sein. Durch die Betrachtung unterschiedlicher Anwendungsbereiche werden potenziell mehr unterschiedliche Auswirkungen auf die Nutzerinnen und Nutzer festgestellt.
- Kaufentscheidung der Nutzerinnen und Nutzer: Als grundsätzliches Kriterium wurde festgelegt, dass die Smart Home-Anwendung in der Regel auf einer freiwilligen Kaufentscheidung der Nutzerinnen und Nutzer basieren sollte. Dadurch wurden beispielsweise Smart Meter ausgeschlossen, da Nutzerinnen und Nutzer keinerlei Einfluss darauf haben, ob ein Smart Meter zum Einsatz kommt oder nicht.
- Zentralistisches vs. dezentrales Ökosystem: Je eine der Smart Home-Anwendungen muss auf einem zentralistischen bzw. dezentralen Ökosystem beruhen. Zentralistisches Ökosysteme bedeuten, dass Hersteller und Betreiber dasselbe Unternehmen sind – Beispiel Sprachassistenten von Amazon, Apple oder Google. Bei dezentralen Ökosystemen sind Hersteller und Betreiber unterschiedliche Unternehmen – Beispiel Überwachungskamera die durch TVT hergestellt wird aber von über 70 unterschiedlichen Unternehmen unter eigenem Namen vertrieben wird (Kerner, 2016).
- Ambient Intelligence statt Wearables: Als grundsätzliches Kriterium wurde festgelegt, dass die Smart Home-Anwendung sensorisch die Umgebung erfassen können soll, statt lediglich die Nutzerin oder den Nutzer. Dies bedeutet, dass Wearables (wie z.B. Fitness-Armbänder) sich nicht für eine tiefergehende Analyse eignen, denn durch die sensorische Erfassung der gesamten Umgebung ergeben sich breitere Fragen hinsichtlich Schutz der Privatsphäre und Drittbetroffenheit, die über dieses Gutachten hinausgehen.

Basierend auf diesen Kriterien wurden letztlich drei Smart Home-Anwendungen als Fokus der Analyse identifiziert:

- Sprachassistenten: Sprachassistenten werden, unter anderem aufgrund der Möglichkeit diverse andere Smart Home-Anwendungen zu steuern, immer stärker nachgefragt. Zumindest die derzeit populären Geräte von Amazon, Google und Apple basieren auf zentralistischen Ökosystemen. Obwohl sie eine Schnittstelle zu vielen anderen Smart Home-Anwendungen bilden, können sie vorrangig dem Bereich „Unterhaltung“ zugeordnet werden. Aufgrund der konstanten Überwachung des gesamten Raumes (um Befehlsworte, wie z.B. „Alexa“ zu hören), ergeben sich interessante Fragestellungen bzgl. Privatsphäre und Drittbetroffenheit.

- (Überwachungs-/Video-)Kameras: Für die Studie wurde der Begriff Kamera weit gefasst und es wurden neben klassischen, vernetzten Überwachungskameras auch Baby-Monitore und Webcams miteinbezogen. Bei vielen Geräten handelt es sich um ein dezentrales Ökosystem, bei dem Hersteller und Betreiber regelmäßig unterschiedliche Unternehmen sind, was zu Herausforderungen hinsichtlich der IT-Sicherheit führt. Ebenso werden kompromittierte Kameras immer wieder für verschiedene Arten von Verbrechen genutzt. Überwachungskameras und Baby-Monitore sind dem Bereich „Sicherheits- und Kontrollsysteme" zuzuordnen. Durch die visuelle Erfassung der Umgebung ergeben sich ebenso interessante Fragestellungen bzgl. Drittbetroffenheit und *Chilling Effects*.
- Beleuchtung: Ähnlich wie bei den Kameras handelt es sich bei vielen smarten Leuchten um ein dezentrales Ökosystem, bei dem Hersteller und Betreiber zumeist unterschiedliche Unternehmen sind. Diese Anwendungen sind dem Bereich „Energiemanagement" zuzuordnen und besitzen unter Smart Home-Anwendungen schon heute eine mittlere bis hohe Marktdurchdringung. Obwohl smarte Leuchten hinsichtlich der sensorischen Erfassung der Wohnräume wesentlich weniger komplex sind als andere Smart Home-Anwendungen (Smart TV, Sprachassistent, Saugroboter), lassen sie trotzdem potenziell umfassende Rückschlüsse auf Lebensgewohnheiten zu. Ebenso stellen sie aufgrund des geringen Preises und des dezentralen Ökosystems einige Herausforderungen an die IT-Sicherheit.

Anwendungs-Hot-Spots im Hauptteil des Gutachtens: In den Kapiteln zur informationellen Selbstbestimmung, dem Umgang mit Nutzerdaten und der Datensicherheit werden die ausgewählten Anwendungs-Hot-Spots tiefergehend analysiert. Der Fokus der einzelnen Kapitel ist wie folgt:

- Informationelle Selbstbestimmung: Die Analyse der Praxisbeispiele basiert auf marktrelevanten Smart Living-Anwendungen in den Bereichen Beleuchtung, Videokameras und Sprachassistenten. Diese Eingrenzung wurde vorgenommen, um eine detaillierte Auswertung der Datenschutzpraktiken vornehmen zu können und neben qualitativen Inhalten auch quantitative Inhalte zu untersuchen.
- Umgang mit Nutzerdaten: Die ausgewählten Praxisbeispiele basieren auf relevanten Fällen aus dem Bereich der Sprachassistenten, da diese das volle Spektrum des User-Profilings abdecken. Zusätzlich werden die Beispiele durch weitere Anwendungen aus dem Bereich der bildlichen Überwachung (Videokameras) angereichert.
- Datensicherheit: Auch für die Praxisbeispiele zur Datensicherheit wurden vornehmlich die Anwendungsbereiche Beleuchtung, Videokameras und Sprachassistenten untersucht.

Geografischen Einordnung: Der Fokus des Gutachtens liegt auf Deutschland. Die Analyse berücksichtigt jedoch auch Literatur und Erfahrungen aus dem europäischen oder außereuropäischen Ausland, sofern diese relevant sind. Eine umfassende, systematische und flächendeckende Berücksichtigung des Auslands ist jedoch nicht vorgesehen. Im Gutachten wird klar gekennzeichnet, auf welchen geografischen Raum der jeweilige Aspekt Bezug nimmt.

Arbeitsaufteilung: Die Autoren haben alle Kapitel gemeinschaftlich bearbeitet. Die Federführung der Kapitel 2, 3 und 4 lag bei ConPolicy, die Federführung der Kapitel 5 und 6 bei der Stiftung Neue Verantwortung.

### 1.2.2 METHODISCHES VORGEHEN

In der Bearbeitung der Studie wurden vier unterschiedliche Methoden angewendet:

#### LITERATURANALYSE

Zur Erarbeitung der Ergebnisse aller Kapitel wurden systematische Literatur- und Internetrecherchen, die sowohl wissenschaftliche Studien als auch graue Literatur einschließen, durchgeführt. Hierbei sind drei übergeordnete Studien hervorzuheben, die einen Überblick über den Status Quo von Smart Living-Anwendungen aus Verbrauchersicht geben. Zu ihnen zählen die Publikation der SmartHome Initiative Deutschland (2017), der Smart Home Index 2017 (Connected Living, 2017) und der Smart Home Monitor 2017 (Splendid Research, 2017).

#### EXPERTENINTERVIEWS

Um tiefergehende Informationen zum Smart Living-Markt aus Nachfrage- und Angebotsperspektive zu gewinnen sowie Fragen zu Erfolgsfaktoren der Anwendungen und künftige Entwicklungen besser abzuschätzen, wurden im Januar 2018 Experteninterviews durchgeführt, die die Literaturrecherche komplementieren. Hierzu wurden in sechs 30-minütigen Telefoninterviews Vertreter aus Wirtschaft, Wissenschaft, Zukunftsforschung und Verbänden interviewt. Die Ergebnisse aus den ausgewerteten Gesprächen sind im Text gekennzeichnet, jedoch anonym und aggregiert aufbereitet. Eine Liste der Interviewpartner findet sich im Appendix.

#### EXPERTENWORKSHOPS

In der Recherchephase wurden außerdem zwei Expertenworkshops durchgeführt. Im ersten Workshop im Januar 2018 wurde eine Problemanalyse des User-Profilings vorgenommen. Der Workshop fand unter dem Titel „User-Profiling in Smart Homes“ in englischer Sprache statt und Vertreter aus Wissenschaft, Wirtschaft und Zivilgesellschaft nahmen hieran teil. Der zweite Workshop im Februar 2018 beschäftigte sich mit relevanten Lösungsansätzen für die Bereiche informationellen Selbstbestimmung, User-Profiling und Datensicherheit. Der Titel des Workshops war „Datenschutz und -sicherheit im Smart Home – Governance-Instrumente“ und auch hier nahmen Vertreter aus Wissenschaft, Wirtschaft, Politik und Zivilgesellschaft teil. Wann immer Ergebnisse aus den Workshops zusammengefasst werden, ist dies gekennzeichnet. Da die Workshops unter „Chatham-House Rule“ stattfanden, werden jedoch keine personenbezogenen Zitate präsentiert.

#### ANWENDUNG VON TEXTANALYSE-TOOLS

Im Kapitel 4 zur informationellen Selbstbestimmung wurden spezielle Methoden zur Auswertung der Datenschutztexte verwendet. Diese werden an der entsprechenden Stelle im Gutachten gesondert vorgestellt.

## 1.3 AUFBAU DES GUTACHTENS

Das Gutachten gliedert sich neben der Einleitung in fünf Kapitel.

Kapitel 2 liefert einen Überblick über existierenden Smart Living- und Smart Home-Anwendungen und nimmt die Verbraucherperspektive ein. Hierzu werden zuerst die relevanten Begriffe definiert

und relevante Anwendungen eingeordnet. Außerdem werden Anwendungsbereiche von Big Data im Bereich Smart Living anskizziert und die Ergebnisse verschiedener Studien und Verbraucherbefragungen zum Kenntnis, Interesse und der Verbreitung von Anwendungen zusammengefasst.

Kapitel 3 legt den Fokus auf die Markt- und Anbieterlandschaft und ordnet relevante Akteure ein. Außerdem werden Änderungen auf dem Smart Living-Markt analysiert und entsprechenden Erfolgsfaktoren zugeordnet. In einem letzten Schritt wird dann die Bedeutung von Big Data für Smart Living-Geschäftsmodelle genauer beleuchtet und relevante Anbieterpartnerschaften vorgestellt.

Kapitel 4 analysiert aktuelle Smart Living-Anwendungen und deren Datenschutzpraktiken empirisch. Hierzu werden zuerst relevante Bewertungskriterien und Indikatoren definiert, die den idealtypischen Zustand von Datenschutzpraktiken beschreiben. Anhand ausgewählter Anwendungen werden die Kriterien dann empirisch überprüft und Handlungsbedarfe identifiziert. Zusätzlich führt das Kapitel in psychologische Faktoren ein, die die informationelle Selbstbestimmung beeinflussen können.

Kapitel 5 legt den Fokus auf den Umgang der Anbieter mit Nutzerdaten. Hierfür wird zuerst der Zweck des User-Profilings aus Anbietersicht dargestellt und Beispiele für Datenhandel- und Weitergabe an Dritte analysiert. Des Weiteren werden die Konsequenzen des Datenumgangs für Verbraucherinnen und Verbraucher vertieft und Aspekte wie Intransparenz oder Manipulation behandelt.

In Kapitel 6 wird der Aspekt der Sicherheitsrisiken von Smart Living-Anwendungen genauer beleuchtet. Anhand ausgewählter Anwendungen werden Sicherheitsvorfälle diskutiert und Auswirkungen und Gefahren sichtbar gemacht. Außerdem werden die Ursachen für Sicherheitsrisiken genauer beleuchtet.

Kapitel 7 fasst die Ergebnisse der vorangehenden Kapitel zusammen und synthesiert die relevanten Herausforderungen für Smart Living-Anwendungen. Außerdem werden für die identifizierten Herausforderungen Lösungsansätze vorgestellt, hinsichtlich ihrer Wirksamkeit bewertet und in Handlungsempfehlungen überführt.

# 2 ANWENDUNGEN UND VERBRAUCHERPERSPEKTIVE

Ziel des zweiten Kapitels ist es, einen Überblick über den Anwendungsraum von Smart Living- und Smart Home-Anwendungen zu geben und ein besseres Verständnis für Verbraucher als Kunden auf dem Smart Living-Markt zu gewinnen. Deshalb wird zuerst der Rahmen des Gutachtens aufgespannt und Smart Living- bzw. Smart Home-Anwendungen definiert. Hiernach werden technische Standards eingeführt und unterschiedliche Installationsformen vorgestellt, die auf dem Smart Living-Markt eine übergeordnete Rolle spielen. Im nächsten Schritte werden die möglichen Anwendungsbereiche und die Rolle von Big Data im Bereich Smart Living aufgezeigt. Im letzten Abschnitt wird die Verbraucherperspektive eingenommen und auf Grundlage unterschiedlicher Verbraucherbefragungen der Kenntnisstand, das Interesse, Verbraucherhürden und perspektivische Entwicklungen diskutiert.

## 2.1 EINLEITUNG UND ABGRENZUNG

### 2.1.1 DEFINITION

Für den Begriff *Smart Living* existiert eine Vielzahl an Synonymen und unterschiedlichen Definitionen. So wird häufig von *Smart Home*, *eHome*, *Connected Home* oder *intelligentem Zuhause / Wohnen* gesprochen. Außerdem werden in diesem Zusammenhang Teilaspekte, wie etwa *Hausautomation* oder *vernetzte Elektronik*, genannt. Auch das *Internet der Dinge* (IoT, OECD, 2017, S.19) findet in diesem Kontext oftmals Verwendung.

Die SmartHome Initiative Deutschland (2017) definiert *Smart Living* als „technische Einrichtungen und Verfahren im Wohnbereich, bei denen Geräte eingesetzt (und) aufgrund einer Datenvernetzung von Sensoren und Aktoren zusätzliche Funktionen der Bereiche Sicherheit, Komfort und Energieeffizienz bieten“ (S. 51). Voraussetzung für Smart Living ist das *Smart Home*, das wie folgt definiert ist: „Ein Smart Home ist ein intelligent vernetztes Gebäude. (…) Entscheidend ist, dass viele Routinevorgänge automatisiert und damit zuverlässig und exakt ablaufen. (…) Eine Wohnung oder ein Wohnhaus ist „smart“, wenn verschiedene Sensoren und Aktoren intelligent miteinander verknüpft werden, um durch automatische Abläufe den darin lebenden bzw. arbeitenden Menschen das Leben zu erleichtern, sicherer zu machen und gleichzeitig den Energieverbrauch des Gebäudes zu reduzieren“ (S. 51).

Eine ähnliche Definition für Smart Home findet sich in Bitkom und DCTI (2015) als „Oberbegriff für technische Verfahren und Systeme in Wohnräumen und -häusern, in deren Mittelpunkt eine Erhöhung von Wohn- und Lebensqualität, Sicherheit und effizienter Energienutzung auf Basis vernetzter und fernsteuerbarer Geräte und Installationen sowie automatisierbarer Abläufe steht“ (S. 9).

Traditionell bzw. in seiner einfachsten Ausführung funktioniert eine Smart Living- bzw. Smart Home-Anwendung wie folgt: Ein Stück Hardware ist mit einer Software ausgestattet, die automatisch eine Funktion ausführt. So könnte ein „smarter“ Thermostat die Zielsetzung haben, die gewünschte Raumtemperatur zu steuern. Seine Funktion wäre, Wärme bereit zu stellen, wenn die tatsächliche Raumtemperatur nicht mit der gewünschten Raumtemperatur übereinstimmt. Sobald weitere solcher Anwendungen miteinander vernetzt werden, ergeben sich zusätzliche Anwendungsszenarien,

die auch in den oben genannten Definitionen formuliert sind. So wäre es beispielsweise in einem vernetzten Wohnhaus möglich, dass der Thermostat seine Zielerfüllung der gewünschten Raumtemperatur mit den Rollläden abstimmt, die eine von außen eintretende Wärme durch die Sonne regulieren (Bourchard et al., 2011, S. 3).

### 2.1.2 VERNETZUNG UND AUTOMATISIERUNG

Aus den vorgestellten Definitionen geht hervor, dass für Smart Living und das ausführende Smart Home eine *Vernetzung und Automatisierung* von Geräten notwendig sind. Diese Vernetzung und Automatisierung kann auf unterschiedlichen technischen Standards beruhen. Grob lassen sich Übertragungsstandards via Funk (bspw. WLAN, Bluetooth), Datenleitung und Stromleitung unterscheiden, d.h. es ist nicht zwingend eine Verbindung zum Internet notwendig, sondern auch eine Übertragung über andere Leitungen möglich. Die Vernetzungsstandards beeinflussen die Kompatibilität der Systeme sowie die Installationsmöglichkeiten. In den folgenden Abschnitten werden technische Standards und Unterschiede in der Installation genauer beleuchtet.

#### UNTERSCHEIDUNG VON TECHNISCHEN STANDARDS

Für das Internet der Dinge im Allgemeinen und Smart Home-Anwendungen im Speziellen gibt es viele unterschiedliche, teils konkurrierende und untereinander inkompatible technische Standards. Für Unternehmen stellt die Vielzahl technischer Standards eine Herausforderung dar, da strategisch entschieden werden muss, welche Standards das Produkt unterstützen soll (Gazis, 2017). Ähnlich zu Software, kann auch bei Standards die Entwicklung eingestellt werden, der Standard setzt sich am Markt nicht durch oder Sicherheitsschwächen werden gefunden.

#### INSTALLATION DER SMART LIVING-ANWENDUNGEN

Die Installation der genannten Smart Living-Anwendungen kann grob in zwei Arten unterteilt werden. Zum einen gibt es *Komplettlösungen*, die die Steuerung der gesamten Wohneinheit zentral regeln (z.B. Qivicon, digitalSTROM oder eQ-3). Branchenführer agieren in diesem Bereich bereits seit zehn Jahren erfolgreich, jedoch bisher in einem Nischenmarkt. Diese Komplettlösungen sind in ihrer Anschaffung kostspieliger und werden vornehmlich von Haus- und Wohnungsbesitzerinnen und -besitzern vorgenommen. Darüber hinaus ist es nicht vorgesehen, dass die Installation der Systeme durch die Nutzerinnen und Nutzer selbst vorgenommen wird, sondern, dass Fachpersonal diese durchführt.

Die andere Installationsart, die in den vergangenen Jahren an Bedeutung gewonnen hat, ist das sogenannte „*Plug-and-Play*“, das heißt die Selbstinstallation der Smart Home-Anwendung durch Nutzerinnen und Nutzer. Diese Anwendungen können im Gegensatz zu den Komplettlösungen kleinteiliger angeschafft werden und sind somit (einzeln betrachtet) kostengünstiger. Darüber hinaus entfallen externe Installationskosten.

### 2.1.3 ANWENDUNGSBEREICHE

Die *Anwendungsbereiche* für Smart Living-Anwendungen sind vielfältig. Die oben genannten Definitionen beinhalten drei wesentliche Zielsetzungen, nämlich Steigerungen in den Bereichen Komfort,

Sicherheit und Energieeffizienz. In diesem Gutachten erweitern wir diese Zielsetzungen und überführen sie in sieben Anwendungsbereiche:[1]

1. Unterhaltungselektronik
2. Haushaltsgeräte und Heimtechnik
3. Energiemanagement
4. Sicherheits- und Kontrollsysteme
5. Sprachassistenzsysteme
6. Wearables und vernetzte Kleidung
7. Häusliche Pflegeunterstützung („Ambient Assisted Living")

Die Zuordnung der einzelnen Anwendungen in die Kategorien wird nach dem Hauptzweck der Anwendung vorgenommen. Dennoch gilt es zu berücksichtigen, dass auch Anwendungen existieren, die mehrere Zwecke erfüllen.

Zu den Anwendungen im Bereich **Unterhaltung** zählen vernetzte elektronische Geräte, die in der Freizeit der Verbraucherinnen und Verbraucher genutzt werden und beispielsweise Angebote aus dem Internet laden können (Integration von Streaming-Diensten). So existieren auf dem Markt beispielsweise vernetzte Fernseher, Audiosysteme wie Lautsprecher und Spielzeug für Kinder und Haustiere („Smart Toys").

Zu den **Haushaltsgeräten und** der **Heimtechnik** zählt die „Weiße Ware", die durch Vernetzung eine effizientere Bedienung ermöglicht. So existieren bereits smarte Reinigungs- oder Kochgeräte. Ebenfalls können dieser Kategorie bestimmte Sensoren oder Bewässerungsanlagen zugeordnet werden.

Weiterhin existiert eine Vielfalt an Anwendungen, die das **Energiemanagement** im Haushalt erleichtern sollen. Die Anwendungen zur Steuerung von Heizungen, Raumklima, Licht oder Strom bieten Verbraucherinnen und Verbrauchern die Möglichkeit, den Verbrauch zu regeln.[2]

Im Bereich **Sicherheits- und Kontrollsysteme** reichen die Anwendungen von vernetzten Kameras, über Schließsysteme bis hin zu Warnmeldern. Sie sollen beispielsweise überwachen, wer sich im Bereich des Heims aufhält, wem Zutritt zum Haus oder der Wohnung gewährt wird oder bei Gefahr durch Brände oder Überschwemmungen eine Warnung aussprechen.

Ein Spezialfall im Bereich der Smart Living-Anwendungen, der getrennt betrachtet werden sollte, sind digitale **Sprachassistenzsysteme**, die über Spracherkennung und -ausgabe eine Mensch-Maschine-Kommunikation ermöglichen. Die Systeme basieren hauptsächlich auf lernenden Algorithmen und werden in eigene Hardware-Architekturen integriert. Die Sprachsteuerung sollte somit als unabhängiges Produkt betrachtet werden, das beispielsweise in Lautsprecher oder das Smartphone integriert wird, jedoch nicht auf sie beschränkt ist.

---

[1] Die Anwendungsbereiche 1 bis 5 folgen einer ähnlichen Einordnung wie der Smart Home Index 2017. Anwendungsbereich 6 ist als Smart Living-Anwendung gesondert zu betrachten, da diese sich nicht auf das Wohnumfeld beschränkt. Anwendungsbereich 7 richtet sich an eine gesonderte Ziel- bzw. Anwendergruppe, beinhaltet jedoch die oben genannten Anwendungsbereiche.

[2] Der Bereich Energiemanagement sollte nicht mit Smart Metering, d.h. der Erfassung von Energieverbrauchswerten durch intelligente Zähler, verwechselt werden (SmartHome Initiative Deutschland, 2017, S. 52) der zwar zum Bereich Smart Living gezählt werden kann, sich jedoch in Deutschland in der Beschaffung und Regulierung unterscheidet.

Auch im Bereich **Wearables** und **vernetzte Kleidung** gibt es einige Angebote, wie Armbanduhren oder Kleidungsstücke, die beispielweise Funktionen zur Überwachung der Gesundheit oder Telekommunikation integrieren.

Unter **Ambient Assisted Living (AAL)** werden beispielsweise Produkte zusammengefasst, die den Alltag von älteren oder physisch eingeschränkten Menschen erleichtern sollen. Hierzu zählen Systeme, die die Vitalfunktion überwachen, Sensoren oder aber auch Kommunikationsgeräte.

Tabelle 1 fasst die Anwendungsbereiche zusammen und listet zusätzlich auf dem Markt befindliche Produktbeispiele auf.

| Anwendungsbereiche | Produktbeispiele |
|---|---|
| Unterhaltung | • Fernseher<br>• Audiosysteme, Lautsprecher, Kopfhörer<br>• Spielzeug für Kinder oder Haustiere |
| Haushaltsgeräte und Heimtechnik | • Küchengeräte wie Kaffeekocher, Mixer, Mikrowellenöfen, Kühlschrank und Gefriergeräte<br>• Wäschepflege wie Waschmaschine, Trockner oder Bügeleisen<br>• Reinigungsgeräte wie Staubsauger oder Poolsauger<br>• Bewässerungsanlagen |
| Energiemanagement | • Temperatureinstellung wie Thermostat oder Klimaanlage<br>• Lichteinstellung bzw. Beleuchtung wie Glühbirne oder Rollläden<br>• Strommanagement wie Steckdose, Zwischenstecker oder Smart Meter |
| Sicherheits- und Kontrollsysteme | • Überwachung wie Sensoren, Videokamera oder Mikrofon<br>• Zugangsmanagement wie Schlösser, Garagenöffner oder Fenster- und Türverriegelung<br>• Rauchmelder, Überschwemmungsmelder |
| Sprachassistenzsysteme | • Alleinstehend, bspw. in Lautsprecher oder Smartphone integriert |
| Wearables und vernetzte Kleidung | • Smart Watch<br>• Kleidungsstücke mit integrierten Lautsprecher oder zur Überwachung von Vitalparametern<br>• Smart Glasses |
| Ambient Assisted Living | • Unterstützung von eingeschränkten oder alternden Personen<br>• Umfasst alle Anwendungskategorien mit einem Fokus auf spezielle Bedürfnisse |

Tabelle 1: Anwendungsbereiche und Produktbeispiele für Smart Living-Anwendungen

## SPEZIALFALL ROUTER

Im Smart Home kommt dem Internetrouter eine besondere Bedeutung zu, da dieser in der Regel die Schnittstelle zum Internet für jegliche Smart Home-Anwendungen darstellt. Als Ende 2016 Internetrouter der Deutschen Telekom großflächig aufgrund eines Hacks ausfielen, hatte dies auch Auswirkungen auf die Smart Home-Anwendungen der betroffenen Benutzerinnen und Benutzer (Schmidt, 2016). Daher hängt die Sicherheit und Funktionsfähigkeit eines Smart Homes sehr stark von der Sicherheit und Funktionsfähigkeit des eingesetzten Internetrouters ab. Dies ist zentraler Grund, weswegen das Bundesamt für Sicherheit in der Informationstechnik (BSI, 2016) ein Konzept zur Sicherheitsüberprüfung von Internetroutern veröffentlicht hat. Weiterhin wurde durch das BSI 2017 eine Arbeitsgruppe zur Entwicklung einer Technischen Richtlinie für Internetrouter ins Leben gerufen, die konkrete Anforderungen an die Sicherheit eines Internetrouters definieren soll (vgl.

Greis, 2017). Aufgrund seiner kritischen Rolle für die Sicherheit aller vorhandenen Smart Home-Anwendungen, ergibt es Sinn, dass dem Internetrouter nicht nur durch das BSI vermehrt Aufmerksamkeit geschenkt wird. Durch diese zentrale Rolle, lässt sich der Internetrouter keiner der zuvor aufgelisteten Kategorien zuordnen, sondern stellt als Schnittstelle zwischen Smart Home und Internet eine Sonderkategorie dar.

## 2.2 ROLLE VON BIG DATA IN ANWENDUNGEN

Bevor die Rolle von Big Data im Bereich Smart Living analysiert werden kann, ist es notwendig, das Konzept als solches zu definieren und Eigenschaften von Big Data vorzustellen. Traditionell bezieht sich Big Data auf die sogenannten drei Vs, Volume, Variety und Velocity (z.B. Wissenschaftliche Dienste des Deutschen Bundestages, 2013).

- Volume bzw. die Menge der Daten ist grundsätzlich groß, wobei sie sich je nach Definition unterscheiden kann.
- Variety bzw. die Vielfalt der Daten kann unterschiedlich ausfallen. So gibt es strukturierte und unstrukturierte Informationen, die in Big Data enthalten sein können.
- Velocity bzw. die Geschwindigkeit der Daten ist oftmals hoch, bspw. in Echtzeit.

Darüber hinaus beinhalten einige weitergehende Definitionen auch die unternehmerischen Faktoren Veracity und Value, die die Vs zu den 5Vs komplementieren (IBM Big Data Hub, 2013; Marr, 2015):

- Veracity bzw. die Richtigkeit steht in diesem Kontext für den Grad in der Sicherheit der Herkunft der Daten.
- Value bzw. (Mehr-)wert steht für die Fähigkeit, einen Nutzen aus den Daten zu erzeugen.

Die Untersuchung des Branchenverbands Bitkom (2015b, S. 13) nennt zur Erzeugung des wirtschaftlichen Nutzens von Big Data zusätzlich die Methodik zur Auswertung der Daten:

- Analytics bzw. Analytik steht hierbei für das Erkennen von Datenzusammenhängen wie Mustern mittels statistischer Verfahren oder Optimierungsalgorithmen.

Die Verbindung zwischen Big Data und Smart Living liegt auf der Hand. Durch die steigende Vernetzung der Hausgeräte sowie Wearables und mobiler Endgeräte entstehen immer mehr Datenpunkte, die nicht nur zügig, sondern auch sinnvoll analysiert und umgesetzt werden können. So gab es in den letzten Jahren die ersten Unternehmen, die vernetztes Spielzeug mit IBMs künstlicher Intelligenz „Watson“ verbunden haben, um Fragen eines Kindes altersgerecht beantworten zu können (Moynihan, 2015). Ebenso experimentieren Hersteller von Smart TVs, in welchem Umfang sie Sehgewohnheiten und Vorlieben der Nutzerinnen und Nutzer sammeln und auswerten dürfen, um die gewonnen Erkenntnisse an Dritt-Unternehmen weiterzugeben (Federal Trade Commission, 2017a).

Um Big Data im Smart Living-Kontext nutzen zu können, existieren eine Reihe an technischer Voraussetzungen. Hierzu gehören (1) eine nahtlose, verlässliche Verbindung, (2) die Möglichkeit, große Mengen (unstrukturierter) Daten zu speichern, (3) eine ausreichende Qualität, die Daten zu analysieren und dies (4) in einer kurzen Zeit zu tun (Ahmed et al., 2017, S. 463-464).

In den Experteninterviews wurde Big Data-Anwendungen bereits jetzt eine bedeutende Rolle zugeschrieben und für die Zukunft eine Zunahme prognostiziert. Als Grund hierfür wurde zum einen genannt, dass die technischen Herausforderungen bezüglich Speichermengen oder Datenformaten immer effizienter überwunden werden. Zum anderen wurde auf die Effizienz der datenbasierten

Geschäftsmodelle hingewiesen, die die Datengrundlage passgenauer nutzbar machen. Diese werden in Kapitel 3 zur Markt- und Anbieterlandschaft genauer beleuchtet.

Unabhängig vom Einfluss von Big Data auf die Marktlandschaft wurden in den Experteninterviews drei übergeordnete Rollen von Big Data bei Smart Living-Anwendungen benannt, die sich daraus ergeben, dass durch die Masse an Daten Zusammenhänge (Korrelationen) besser erkannt werden können:

1. Big Data macht eine **Profilbildung** einfacher.
2. Die **Wünsche** von Verbraucherinnen und Verbrauchern können besser erkannt und befriedigt werden.
3. Eine **Verhaltenssteuerung** durch datenbasierte Smart Living-Anwendungen wird einfacher und effizienter.

Die ersten beiden Punkte werden auch in der Publikation von Bouchard et al. (2016) erwähnt. So stellt Big Data nach Ansicht der Autoren den Ursprung neuer Anwendungsarten im Smart Home dar und kann durch das Ermöglichen von Profilbildung besser auf Verbraucherwünsche eingehen. Als Beispiel nennen die Autoren die Nutzung von Smart Home-Daten im Gesundheitsbereich, durch die Krankheiten besser erkannt, verstanden und auf sie reagiert werden kann (S. 2).

Der dritte Punkt hat Berührungspunkte mit der Nutzbarmachung von Big Data im Bereich des Nudgings[3] oder der Verhaltensbeeinflussung im Allgemeinen. Ziel ist es somit die Wirkung eines Nudges durch Big Data-Methoden zu erhöhen. Hierdurch können Nudges effektiver personalisiert und dynamisch gestaltet werden – sogar in Echtzeit. Die Anwendungsbereiche von Big Data und Nudging sind vielfältig im Smart Home vorstellbar, beispielsweise bei der Förderung von nachhaltigem Konsum durch Stromsparmaßnahmen.

## 2.3 VERBRAUCHERPERSPEKTIVE

Bevor in Kapitel 3 die Anbieterseite des Smart Living-Marktes beleuchtet wird, werden die Einsatzbereiche und Nutzungsszenarien aus Verbraucherperspektive analysiert. Nach Auswertung des allgemeinen Kenntnisstands wird auf Grundlage von Verbraucherbefragungen der Verbreitungsgrad (Status Quo) und das Nutzungsinteresse (Prognose) vorgestellt. Hiernach werden Hürden diskutiert, die einer Verbreitung von Smart Home-Anwendungen auf dem Massenmarkt bisher im Weg standen.

### 2.3.1 KENNTNIS DER ANWENDUNGEN UND INFORMIERTHEIT

Um die Verbraucherperspektive besser zu verstehen, ist es notwendig zu analysieren, welchen Kenntnisstand Verbraucherinnen und Verbraucher beim Thema Smart Living bzw. Home haben. In einer Umfrage im Rahmen des aktuellen Smart Home Index 2017 geben 80% der Befragten an, den Begriff Smart Home zu kennen (Connected Living, 2017, S. 2). In einer Befragung von PwC (2017, S. 4) zeigt sich auch eine hohe Bekanntheit digitaler Sprachassistenzsysteme in der deutschen Be-

[3] Nudging wird von Thaler und Sunstein (2009) definiert als „(...) alle Maßnahmen, mit denen Entscheidungsarchitekten das Verhalten von Menschen in vorhersehbarer Weise verändern können, ohne irgendwelche Optionen auszuschließen oder wirtschaftliche Anreize stark zu verändern.“ (Thaler und Sunstein, 2009, S. 15)

völkerung. So geben 78% der Befragten an, Amazon Echo mindestens zu kennen. Bei Apple Siri sind es 70%, beim Assistenten von Google 64% und Microsoft Cortana hat einen Bekanntheitsgrad von 62%. Im D21-Digital-Index 2017/2018 geben außerdem 77% der Befragten an, dass sie intelligente Küchenmaschinen (z.B. Vorwerk Thermomix) kennen und 83% sagen, dass ihnen Roboter (z.B. Spielroboter, Saugroboter, Roboter am Arbeitsplatz) bekannt seien (Initiative D21, 2018, S. 39).

Der Bekanntheit der Anwendungen steht die Informiertheit der Verbraucherinnen und Verbraucher gegenüber. So zeigt eine Befragung im Auftrag von Statista (2016b), dass sich Verbraucherinnen und Verbraucher nicht gut beim Thema Smart Home informiert fühlen. 22% geben an „gar nicht gut" und 42% „eher nicht gut" informiert zu sein. 29% der Befragten fühlen sich „eher gut" und lediglich 7% „sehr gut" informiert. Auch der erste Kontakt von Verbraucherinnen und Verbrauchern mit dem Smart Home ist unterschiedlich. So geben knapp 24% der Befragten des Smart Home Monitors 2017 an, dass sie Anwendungen aus der Werbung kennen. Ähnlich hoch (22%) ist jedoch der Anteil der Befragten, die nicht mehr wissen, wann sie das erste Mal mit dem Smart Home in Berührung gekommen sind. Weitere Verbreitungskanäle wie Zeitschriften, Nachrichten oder persönliche Kontakte werden mit jeweils um die 10% weniger häufig als Informationsquelle angegeben.

### 2.3.2 AKTUELLE VERBREITUNG DER ANWENDUNGEN

Die Auswertung des Smart Home Index 2017 kam zusammenfassend zu dem Schluss, dass die Verbreitung von Smart Home-Anwendungen derzeit relativ gering sei und man nicht von einem Massenmarkt sprechen könne. Diese Erkenntnisse decken sich auch mit den Ergebnissen von Verbraucherumfragen, die im Folgenden zusammengefasst werden.

45% der Befragten des Smart Home Index 2017 geben an, mindestens ein und maximal fünf smarte Geräte zu besitzen, während 15% der Befragten bereits sechs oder mehr Anwendungen besitzen (Connected Living, 2017, S. 6). Der Anteil der Nicht-Nutzer liegt somit bei 40%. In der Befragung für den D21-Digital-Index 2016 ist der Anteil der Nutzerinnen und Nutzer weitaus geringer. So geben 6% der Befragten an, Smart Home-Anwendungen beispielweise zur Heizungssteuerung zu nutzen. Jedoch ist unklar, ob in die Fragekategorie auch smarte Unterhaltungsmedien wie Fernseher oder Lautsprecher zählen, die über einen höheren Verbreitungsgrad verfügen (vgl. Initiative D21, 2017).

Der Besitz von Smart Living-Anwendungen unterscheidet sich laut Smart Home Index 2017 ebenfalls stark zwischen den Anwendungsbereichen. So geben 54% der Befragten mit mindestens einer smarten Anwendung an, dass sie ein smartes Gerät aus dem Bereich der Unterhaltungselektronik besitzen.[4] 25% der Smart Home-Anwenderinnen und -Anwender geben an, eine Anwendung im Bereich Energiemanagement zu besitzen und der Anteil im Bereich Sicherheit beträgt 21%. Smarte Haushaltsgeräte werden von 19% der Smart Home-Anwenderinnen und -Anwender genutzt und auf die Kategorie „Sonstiges" (bspw. Gartenanwendungen) entfallen 14%. Der DSiN-Sicherheitsindex 2017 erhebt in der Befragung lediglich die Nutzung von Unterhaltungselektronik und Heimtechnik. Insgesamt geben 11% der Befragten an, dass sie vernetzte Unterhaltungselektronik nutzen und im Bereich der vernetzten Heimtechnik beträgt der Anteil der Nutzerinnen und Nutzer 4%. Im aktuellen D21-Digital-Index 2017/2018 wird außerdem explizit nach Smart TVs gefragt. Hier geben 18% der Befragten an, einen intelligenten Fernseher zu nutzen (S. 14).

[4] Hierzu zählen im Smart Home Index 2017, neben den in Abschnitt 2.1.3 definierten Unterhaltungsgeräten wie Fernseher und Musikanlagen, auch die Sprachassistenzsysteme.

In einer deutschen Bevölkerungsbefragung zu digitalen Sprachassistenten geben bei den vier bekanntesten Anbietern jeweils um die 20% der Befragten an, einen Sprachassistenten bereits zu nutzen oder in Zukunft nutzen zu wollen (PwC, 2017, S. 4). Im D21-Digital Index 2017/2018 geben außerdem 10% der Befragten an, einen Sprachassistenten regelmäßig, in diesem Fall ein bis mehrmals pro Woche, zu nutzen (Initiative D21, 2018, S. 16).

Unter den Verbraucherinnen und Verbrauchern, die im Smart Home Monitor 2017 angaben, eine Smart Home-Anwendung zu nutzen, unterscheidet sich die Verbreitung zwischen den verschiedenen Anwendungsbereichen ebenfalls stark. So geben knapp 60% der Smart Home-Besitzerinnen und -Besitzer an, dass sie Energiemanagement-Anwendungen nutzen. 56% nutzen Unterhaltungselektronik und 36% Hausautomation und Komfortfunktionen. Sicherheitsanwendungen liegen mit 32% knapp dahinter, während lediglich 16% der Befragten AAL-Anwendungen nutzen.

Gefragt nach dem Kauf der ersten Smart Home-Anwendung geben im Smart Home Monitor 2017 lediglich 13% der Smart Home-Nutzerinnen und -Nutzer an, diese vor 2014 erworben zu haben. 31% der Verbraucherinnen und Verbraucher kauften ihre erste Anwendung in den Jahren 2014 oder 2015 und die Mehrheit, nämlich 56%, nutzt Smart Home-Anwendungen erst seit 2016 oder 2017.

### 2.3.3 INTERESSE AN DEN ANWENDUNGEN

Das Interesse an Smart Home-Anwendungen ist unter Verbraucherinnen und Verbrauchern prinzipiell hoch. Zahlen einer Online-Befragung von Statista (2016c) zeigen, dass nur 16% der Befragten vernetztes Wohnen *gar nicht interessant* finden. Weitere 24% geben an, dass diese Anwendungen *weniger interessant* sind. Der Anteil der interessierten Verbraucherinnen und Verbraucher liegt höher. So geben 39% an, Anwendungen *interessant* zu finden und 21% finden sie sogar *sehr interessant*.

Auch Schulze-Sturm (2016) zeigt auf, dass viele Verbraucherinnen und Verbraucher grundsätzlich ein Interesse an Smart Home-Lösungen haben. Als Gründe für dieses Interesse werden in seiner Befragung vor allem Energieeffizienz und die Steigerung von Sicherheit und Komfort genannt (S. 10). Dieses Bild deckt sich mit den Gründen für ein Interesse am Smart Home, die von Lübbeke (2016) identifiziert wurden. Die Erleichterung des Alltags, Komfortsteigerungen und Energieeffizienz werden von Befragten genannt (S. 23).

Im Rahmen des BDEW-Energiemonitors 2016 wurden Verbraucherinnen und Verbraucher ebenfalls dazu befragt, welche Art Smart Home-Anwendungen sie als sinnvoll erachten. Auf dem ersten Rang befindet sich mit 92% Zustimmung der Anwendungsbereich der medizinischen Assistenzsysteme (vgl. AAL). 68% finden Anwendungen aus der Sicherheitstechnik sinnvoll und 59% fernsteuerbare Heizungen. Rollläden und Fenster, die vernetzt sind, bewerten 52% als sinnvoll und 46% Beleuchtungstechnologien. Auf dem letzten Rang mit 21% liegen Haushaltsgeräte (BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., 2016).

Auch bei der Nutzung von Sprachassistenten bzw. intelligenten Lautsprechern existiert auf der Verbraucherseite ein Interesse. In einer Befragung des Branchenverbands Bitkom (2017) geben 39% der Befragten an, dass sie sich vorstellen könnten, einen digitalen Sprachassistenten zu nutzen und in einer Befragung zu intelligenten Lautsprechern geben 78% der Befragten an, dass Sie Vorteile in deren Nutzung sehen (PwC, 2017, S.6). Zu den häufigsten Nutzungsszenarien von intelligenten Lautsprechern geben Befragte an, diese zum Abspielen von Musik (52%), zum Abrufen von Informa-

tionen (48%) und der Beantwortung von Wissensfragen (44%) nutzen zu wollen. Auch die Unterstützung bei der Termin- (37%) oder Fahrtenplanung (31%) ist ein potentieller Use-Case und weitere 30% geben an, intelligente Lautsprecher potentiell zur Steuerung des Smart Homes zu nutzen (PwC, 2017, S.5).

### 2.3.4 VERBRAUCHERHÜRDEN

Trotz der Interessensbekundungen von Verbraucherinnen und Verbrauchern und den genannten Gründen für die Nutzung von Smart Home-Anwendungen existieren Hürden, die eine Verbreitung auf dem Massenmarkt bisher eingeschränkt haben. In einer Veröffentlichung aus dem Jahr 2003 wurden eine Reihe von Hürden diskutiert, die Verbraucherinnen und Verbraucher – zum damaligen Zeitpunkt – an der Adaption von Smart Home-Anwendungen in Europa zu hindern schienen (Aldrich, 2003, S. 29):

1. Alter Hausbestand: Insgesamt ist es einfacher einen Neubau mit Smart Home-Technologie auszustatten als einen bestehenden Bau nachträglich.
2. Kein einheitliches Protokoll: Da die unterschiedlichen Systeme nicht kompatibel genutzt werden können, müssen sich Nutzerinnen und Nutzer oftmals für ein System entscheiden.
3. Kosten: Da die Kosten der Ausrüstung hoch sind und Verbraucherinnen und Verbrauchern der Nutzen möglicherweise unbekannt ist, wird weniger investiert.
4. Mangelnde Evaluation der Nutzbarkeit durch Anbieter: Wenn die Nutzbarkeit der Anwendungen sich nicht verbessert und die Anbieter auch Anwendungen auf den Markt bringen, die den Kundenwünschen nicht entsprechen, werden Verbraucherinnen und Verbraucher Technologien nicht nutzen.
5. Anbieter berücksichtigen die Wünsche der Kundinnen und Kunden nicht: Einhergehend mit dem vorherigen Grund, werden beispielsweise Angebote auf den Markt „gepusht", für die keine Nachfrage existiert. Nur weil Anwendungen technologisch machbar sind, heißt dies nicht automatisch, dass diese gekauft werden.

Diese Verbraucherhürden aus dem Jahr 2003 bestätigen sich auch in aktuelleren Betrachtungen. So werden die oben genannten Aspekte auch in der Analyse des BMWi (2016) aufgezählt. Eine ähnliche Bestätigung ist aus den Ergebnissen von Verbraucherbefragungen aus dem Jahr 2017 zu ziehen. So ist die Abwägung zwischen Kosten und Nutzen von Smart Home-Anwendungen auch in jüngster Zeit noch ein Hauptgrund für die Nicht-Nutzung von Smart Home-Anwendungen. Die Befragten des Smart Home Monitor 2017 geben beispielsweise als die drei häufigsten Gründe für mangelndes Interesse an Smart Home-Anwendungen an, dass die Anschaffung (78%), der Einbau (74%) und der Betrieb (73%) ihnen zu teuer ist. Auch Schulze-Sturm (2016) und Lübbeke (2016) zeigen auf, dass vor allem der Preis von Anwendungen eine Rolle für die Nicht-Adaption spielt. Die Untersuchung des Zukunftsinstituts für Siemens (2015) analysierte die Bereitschaft von Verbraucherinnen und Verbrauchern einen Aufpreis für smarte Geräte – im speziellen smarte Haushaltsgeräte – zu zahlen, wenn diese Geräte im Vergleich zum nicht-vernetzten Gegenstück gesonderte Aufgaben übernehmen würden. Hier lässt sich vor allem ein großer Unterschied zwischen jüngeren und älteren Befragten feststellen. Während in der Gruppe der unter-35-jährigen 16% angeben, keinen Aufpreis für smarte Technologien zahlen zu wollen, ist der Anteil der über-35-jährigen mit einem Drittel sehr viel höher (vgl. S 20, 28, 44).

Lübbeke (2016) weist außerdem darauf hin, dass Verbraucherinnen und Verbraucher ihr mangelndes Interesse mit einer mangelnden Notwendigkeit der Anwendung an sich begründen. Im Smart

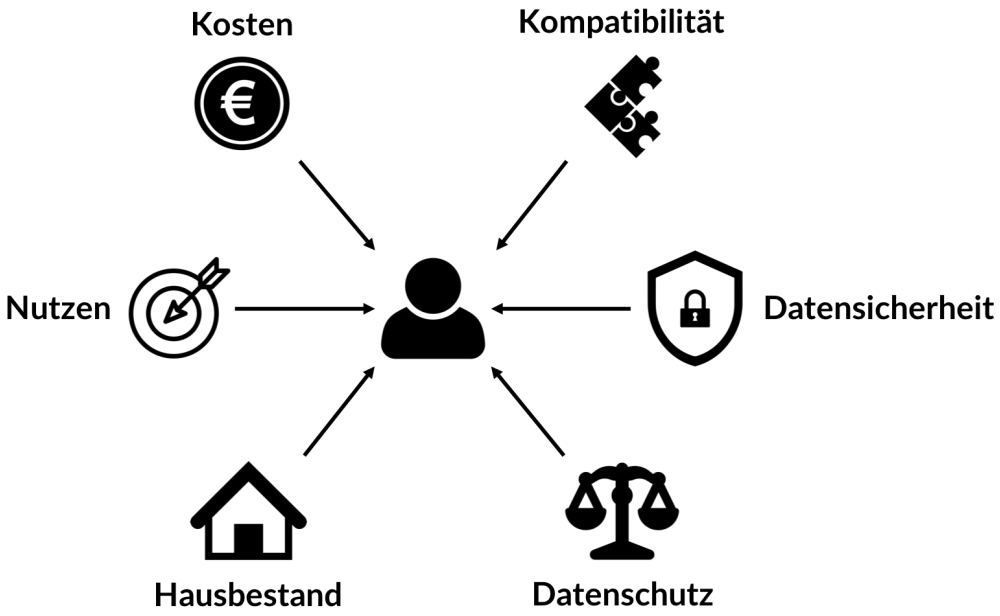
Home Monitor 2017 geben weiterhin 40% der Befragten, die kein Smart Home nutzen, an, dass ihr mangelndes Interesse darin fußt, dass sie die Anwendungen nicht kennen. Sind die Kosten zu hoch oder der Nutzen nicht bekannt bzw. zu niedrig, entscheiden sich Verbraucherinnen und Verbraucher gegen Smart Home-Anwendungen. Ein weiterer Aspekt, der im Smart Home Monitor 2017 bestätigt wird, ist die **mangelnde Nutzbarkeit** von Smart Living-Anwendungen. So geben immerhin 41% der Befragten an, dass die Bedienung der Anwendungen ihnen zu kompliziert erscheint. Auch die Vielzahl der unterschiedlichen **Protokolle** scheint ein relevanter Faktor zu sein. So geben 38% der Befragten an, dass die Geräte verschiedener Hersteller nicht zusammen funktionieren, was das Interesse an Smart Home-Anwendungen schmälert.

Zusätzlich zu den Gründen, die bereits in Aldrich (2003) eine Rolle spielten, nennen Verbraucherinnen und Verbraucher im Smart Home Monitor 2017 auch **emotionale Gründe** für die Nicht-Nutzung - 69% geben an, dass sie eine steigende Automatisierung unheimlich finden. Im DSiN-Sicherheitsindex 2017 geben 21% der Befragten an, dass sie Haus- und Heimvernetzungstechnologien mindestens gefährlich einstufen und auch **Sicherheits- und Privatsphärebedenken** spielen eine Rolle bei der Adaption von Smart Home-Anwendungen (Deutschland sicher im Netz e.V. (DsiN), 2017). Im Smart Home Monitor 2017 werden Sicherheit und Privatsphäre von 61% bzw. 58% der Befragten als Nicht-Nutzungsgrund genannt. Dies bestätigt auch Schulze-Sturm (2016), in dessen Befragung 11% Bedenken bezüglich der **Datensicherheit** äußern (S 10) und auch in einer Befragung zu digitalen Sprachassistenten werden Bedenken bezüglich Privatsphäre und Sicherheit genannt (PwC, 2017, S.8). Die häufigsten Bedenken werden hierbei in Bezug auf Hackerangriffe und daraus folgende Manipulations- und Datendiebstahlgefahren genannt (70%). Bedenken zum „gläsernen Kunden“ zu werden, äußern 69% und 66% äußern Bedenken, abgehört zu werden.

Eine Hürde, die in Aldrich (2003) ebenfalls genannt wurde, ist, dass Anwendungen nicht mit den **Wünschen der Kunden** übereinstimmen. In einer Untersuchung des Zukunftsinstituts für Siemens (2015) wird der erkennbare Mehrwert für Kundinnen und Kunden ebenfalls als zentral bewertet und spielt deshalb für die Adaption von vernetzten Hausgeräte eine große Rolle.

Abbildung 1 fasst die Verbraucherhürden grafisch zusammen.

Abbildung 1: Verbraucherhürden im Smart Home




(Eigene Darstellung)

## 2.4 ENTWICKLUNGSTENDENZEN

Trotz der genannten Hürden und des geringen Kenntnisstands der Verbraucherinnen und Verbraucher wurde in den Experteninterviews einstimmig davon gesprochen, dass Smart Living-Anwendungen in den kommenden Jahren eine sehr starke Verbreitung finden werden. Laut einer Prognose von Gartner (2014) könnten im Jahr 2022 mehr als 500 smarte Anwendungen in einem Haushalt existieren. Um diese breite Anwendung zu erreichen, sind im Smart Home Index 2017 mehrere notwendige Schritte definiert (S. 12). Diese Schritte adressieren zum großen Teil die Verbraucherwünsche, die sich aus den oben genannten Verbraucherbefragungen ergeben:

1. So zählt zu den Erfolgstreibern zum einen die *Individualisierung* der Angebote, um technisch-machbare Lösungen mit den Verbraucherinteressen in Einklang zu bringen.
2. Um auf dem bisherigen Erfolg der Smart Home-Anwendungen im Unterhaltungselektronik-Markt aufbauen zu können, sollten künftige, vernetzte Geräte die *Unterhaltungsfunktionalität* in ihren Anwendungsfällen kombinieren.
3. Je höher die *Kompatibilität* der Anwendungen, desto höher ist die Kundenbindung und somit die Nutzbarkeit der Smart Home-Anwendungen, die sich auf dem breiten Markt durchsetzen werden.

Dass die Verbraucherwünsche immer besser adressiert werden, spiegelt sich auch in den Kaufabsichten der Nutzerinnen und Nutzer wieder, die laut Smart Home Index 2017 stark vom aktuellen Besitz von Smart Home-Anwendungen abhängen (S. 7). So geben Verbraucherinnen und Verbraucher, die bereits sechs oder mehr Anwendungen besitzen, zu 60% an, dass sie auch Interesse an weiteren Anwendungen haben und 25% von ihnen äußern eine explizite Kaufabsicht. Bei Verbrau-

cherinnen und Verbrauchern, die zwischen einer und fünf Anwendungen besitzen, liegt das Interesse bei 51% und die Kaufabsicht bei 9%. Verbraucherinnen und Verbraucher, die bisher kein vernetztes Gerät besitzen, äußern ihr Interesse an Smart Home-Produkten zu 40%. Eine positive Kaufabsicht haben lediglich 4%.

Im Smart Home Monitor 2017 wurden Daten zu den Kaufabsichten von Verbraucherinnen und Verbrauchern veröffentlicht, die bisher keine Smart Home-Anwendungen nutzen. Über ein Drittel der Befragten gab hierbei an, dass sie im kommenden Jahr Interesse an der Steuerung von Heizung, Geräten oder Beleuchtung hätten. Auch die Überwachung des Hauses war für 28% der Befragten interessant und 26% gaben an, dass eine Mitteilung über offene Türen oder Fenster eine interessante Anwendung sei. Zu den Top-Anwendungen gehören außerdem weitere Sicherheitsanwendungen, Saugroboter und Steuerungsmöglichkeiten von Beleuchtung oder Audio. Im D21-Digital-Index 2017/2018 sind außerdem Zahlen zu digitalen Sprachassistenten veröffentlicht. Hier liegt die Zahl der potentiellen Nutzerinnen und Nutzer bei 25% (Initiative D21, 2018, S. 39).

In den Experteninterviews wurden außerdem weitere Entwicklungen für den Smart Home-Markt prognostiziert. Zum einen wurde von den Expertinnen und Experten angemerkt, dass Smart Home-Systeme bzw. sogenannte Komplettlösungen in Neubauten sehr viel aktiver mitgedacht und umgesetzt werden. Zum anderen wurde eine Fortsetzung im Anstieg der „Plug-and-Play"-Anwendungen vorhergesagt. Zwar werden keine neuen Arten von Geräten prognostiziert, jedoch ein besseres Zusammenspiel der Einzelfunktionen.

Ein weiterer Aspekt, der in Zukunft auf dem Smart Home-Markt eine Rolle spielen wird, ist die *Integration* von Funktionen, die bisher *außerhalb des Hauses* lagen. Während beispielsweise der Einkauf von Lebensmitteln, mit vereinzelten Ausnahmen im Bereich der Lieferdienste, analog und außerhalb des Hauses oder der Wohnung stattfand, könnten bald durch die Integration von eCommerce-Anbietern in die Smart Home-Anwendungen auch Einkäufe zentral gesteuert und ausgeführt werden.

Ein weiterer funktionaler Trend, der im Smart Home-Markt zu erwarten ist, ist die *Veränderung der Steuerung*. Wie beschrieben, sind vor allem Anwendungen, die durch Sprache gesteuert werden, auf dem Vormarsch. Diese Entwicklungen werden sich auch in Zukunft weiter durchsetzen und durch weitere Steuerungsmöglichkeiten komplementiert werden. So legt auch Gartner (2014) den Fokus auf die Art der Produktsteuerung und nennt neben Sprachbefehlen auch Gestensteuerung als Möglichkeit, die Nutzbarkeit der Anwendungen für Verbraucherinnen und Verbraucher attraktiver zu machen.

## 2.5 ZUSAMMENFASSUNG

Das zweite Kapitel zeigt, dass bereits eine Vielzahl unterschiedlicher Smart Living-Anwendungen auf dem Markt existieren. Zwar ist die Verbreitung der Anwendungen bisher relativ gering, es gibt jedoch ein immenses Potential für Smart Living-Anwendungen auf dem Massenmarkt. Big Data spielt dabei bereits eine große Rolle und wird auch in Zukunft immer intensiver genutzt werden, um Smart Living-Dienste zu optimieren. Aus der Perspektive der Verbraucherinnen und Verbraucher existieren derzeit noch eine Reihe von Hürden für die Nutzung von Smart Living-Anwendungen. Neben dem Preis, der mangelnden Nutzbarkeit und inkompatiblen Protokollen werden Sicherheits- und Privatsphärebedenken genannt. Um diese Hürden zu überwinden, werden auf dem Markt Bestrebungen beobachtet, wie den Wünschen der Verbraucherinnen und Verbraucher besser begegnet werden kann. So werden Anwendungen in Zukunft besser zusammenspielen und ermöglichen, auch

Funktionen, die bisher außerhalb des Hauses lagen, in das Haus zu integrieren. Zusätzlich und einhergehend mit technischen Entwicklungen wird außerdem prognostiziert, dass die Sprachsteuerung an Bedeutung gewinnen wird und auch die Gestensteuerung ein Potential für den Smart Living-Markt birgt.

Während der bisherige Fokus des Gutachtens auf der Anwendungs- und Verbraucherseite lag, wird im nächsten Kapitel die Anbieterseite genauer beleuchtet, um Einblicke zu relevanten Akteuren zu gewinnen und den Einsatz von Big Data aus Anbieterperspektive zu verstehen.

# 3 MARKT- UND ANBIETERLANDSCHAFT

Die „Markt-Historie“ des intelligenten Zuhauses kann auf die Mitte des 20. Jahrhunderts zurückgeführt werden und so zeigt sich in der Marktanalyse der Deutschen Telekom AG (2015), dass sich bereits damals erste Anbieter Gedanken zur Vernetzung des Wohnumfelds gemacht haben (S. 8). Auch in einem Buch, das vor 15 Jahren unter dem Titel „Inside the Smart Home“ veröffentlicht wurde, finden sich Anhaltspunkte zur „historischen“ Entwicklung des Smart Home-Markts (Harper, 2003 sowie Aldrich, 2003). So wird gezeigt, dass es zuerst Hersteller von Verteiler- oder Schaltsystemen waren, die auf dem Markt aktiv waren, um eine Automatisierung des Hauses zu ermöglichen. Hiernach folgten Technologieanbieter beispielsweise aus der Unterhaltungselektronik und Energieanbieter, die eigene Systeme auf den Markt brachten. Seitdem hat sich der Markt jedoch stark weiterentwickelt, so dass eine Unterscheidung von Verteiler- und Schaltsystemen, Unterhaltungselektronikanbietern und Energieunternehmen zu limitiert ist.

Im Folgenden werden die Marktakteure und deren Rollen genauer beleuchtet. Hiernach werden Veränderungen in der Akteurslandschaft diskutiert und Geschäftsmodelle vorgestellt. Im letzten Abschnitt wird dann akteursseitig auf die Rolle von Big Data eingegangen und Partnerschaften auf dem Smart Living-Markt diskutiert.

## 3.1 RELEVANTE MARKTAKTEURE UND DEREN ROLLEN

Smart Home-Anwendungen bestehen sowohl aus einem Teil **Hardware**, als auch aus der entsprechenden **Software**, die vernetzte Services ermöglicht. Aus den Experteninterviews und Marktanalysen von Raspin (2016, S. 14) und Bitkom (2015c) ergab sich, dass auch eine reine Unterscheidung in Hardware- und Softwarehersteller zu limitiert ist, da auf dem Smart Home-Markt Branchengrenzen verschwimmen und Anbieter sowohl Hardwareprodukte als auch die zugehörige Software herstellen und vermarkten können. Die folgende Unterteilung richtet sich deshalb nach den Branchen der aktuell auf dem Markt befindlichen Anbieter und beschreibt die Rollen auf dem Markt bzw. bei der Bereitstellung der Produkte:

1. **(Hardware-)Hersteller oder Originalausrüstungshersteller**: Hierzu gehören beispielsweise Sicherheitsgeräte-, Hausgeräte-, Unterhaltungselektronik- oder Hauselektronikhersteller, die primär (und historisch) physische Produkte fertigen und deren Vernetzung technisch ermöglichen. In einzelnen Fällen integrieren diese Anbieter auch die Serviceleistungen, d.h. die notwendige Software.
2. **Energieanbieter und Versorgungsunternehmen**: Zum Portfolio dieser Anbieter zählen beispielsweise vernetzte Verbrauchsmessungsinstrumente, sogenannte Smart Meter. Auch hier gibt es jedoch keine klare Trennung zwischen reinen Hardware- und Softwareherstellern. Manche Versorgungsanbieter stellen neben der Hardware auch Plattformen zum Management der Produkte zur Verfügung.
3. **Technologie- und Internetkonzerne:** Primäre Rolle dieser Anbieter ist die Bereitstellung der Software. Dies können eigene Kommunikationsstandards sein oder auch Applikationen zum Betreiben der Anwendungen. Auch bei diesen Anbietern verschwimmen die Rollen entlang der Wertschöpfungsketten. So bieten beispielsweise die großen Internetkonzerne Hardware an, die Softwareprodukte wie Sprachassistenten integriert.

4. Telekommunikationsanbieter: Telekommunikationsanbieter sind zum einen als Infrastrukturanbieter auf dem Markt aktiv. Sie stellen beispielsweise sicher, dass die Kommunikation der Geräte funktioniert (WLAN-Anwendungen, o.ä.). Darüber hinaus ändert sich deren Rolle dahingehend, dass sie Plattformen bereitstellen und als Bindeglied zwischen Hard- und Software fungieren (z.B. QIVICON der Deutschen Telekom AG).
5. Smart Home Systeme oder Plattformen: Diese Anbieter haben vor allem die Funktion des Servicemanagements mittels Softwareanwendungen wie der Bereitstellung von Kommunikationsstandards oder Schnittstellen zwischen Kommunikationsstandards.

Da den Smart Home-Systemen und -Plattformen in den Experteninterviews eine hohe Bedeutung beigemessen wurde, ist es notwendig, diese genauer zu beleuchten und deren Unterschiede herauszustellen. Beide Anbieterformen haben gemeinsam, dass sie das sinnvolle Zusammenspiel von Anwendungen ermöglichen. Die Relevanz leitet sich dabei auch aus den Kundenbedürfnissen, die in Abschnitt 2.4 eingeführt wurden, ab.

Tabelle 2 fasst die Unterschiede zusammen (vgl. BMWi, 2016, S.7):

| | Smart Home Systeme | Smart Home Plattformen |
|---|---|---|
| Prinzip | Ermöglichen das Zusammenspiel unterschiedlicher Anwendungen durch einen gemeinsamen Kommunikationsstandard | Ermöglichen das Zusammenspiel verschiedener Smart Home Systeme und erlauben so auch die Interoperabilität unterschiedlicher Kommunikationsstandards. |
| Beispiele | KNX, Z-Wave, TRON Smart Home, ZigBee oder die digitalSTROM-Allianz | Open Connectivity Foundation (einschließlich AllSeen Alliance), QIVICON der Deutschen Telekom. |

Tabelle 2: Unterscheidung von Smart Home-Systemen und -Plattformen

In der Analyse der Deutschen Telekom AG (2015) findet sich ein weiterer relevanter Akteur, der in Zukunft auf dem Smart Home-Markt aktiv werden wird (S. 19). So sollen Versicherungsunternehmen partizipieren und beispielsweise Versicherungspolicen am Smart Home ausrichten. Insgesamt sei so ein besseres Risikomanagement möglich und die Analyse sagt auch eine Reduktion der Schadensfälle voraus, da installierte Sicherheitsanwendungen das Haus besser schützen. Jedoch liegen derzeit keine konkreten Zahlen zur Marktentwicklung vor, so dass der Grad des Engagements abzuwarten bleibt.

### 3.1.1 VERÄNDERUNGEN IN DER AKTEURSLANDSCHAFT

Die Analyse des Branchenverbands Bitkom (2015c) findet für den speziellen Bereich der Consumer Electronics, dass klassische Anbieter (reine Hardwarehersteller) künftig nur noch bedingt auf dem Unterhaltungselektronikmarkt erfolgreich sein werden. Dafür werden datenfokussierte Anbieter, wie beispielsweise Internetkonzerne an Bedeutung gewinnen (S. 55). Diese Beobachtung wird von Branchenexperten auch für andere Sektoren, wie Energiemanagement oder Sicherheit, bestätigt.

Parallel zu der in Abschnitt 3.1 eingeführten Unterscheidung der Marktakteure, leiten sich aus Raspin (2016), Deutsche Telekom AG (2015), Bitkom (2015c) sowie den Experteninterviews folgende Veränderungen ab:

1. (Hardware-)Hersteller oder Originalausrüstungshersteller: Vor allem die Originalausrüstungshersteller sollen in Zukunft auf dem Smart Home-Markt eine bedeutendere Rolle spielen. Raspin (2016) prognostizieren hierbei, dass durch neue strategische Partnerschaften mit Serviceanbietern aus dem Softwarebereich innovative Lösungen hervorgehen können.
2. Energieanbieter und Versorgungsunternehmen: Die Marktprognose sagt vorher, dass die Rolle dieser Unternehmen stabil bleiben wird. Durch neue Technologien und Daten wird es möglich sein, Kundenwünsche besser zu erfüllen. Jedoch wird sich die Rolle der Anbieter nicht über den Energiesektor ausweiten.
3. Technologie- und Internetkonzerne: Vor allem für die Softwareanwendungen der Technologieunternehmen wird ein großes Wachstum prognostiziert. So wird es in Zukunft möglich sein, vernetzte Services weiter zu kommerzialisieren. Bei den Entwicklern von Applikationen zur Steuerung der Smart Home-Anwendungen wird jedoch ein Wandel vorhergesagt. Während derzeit viele Anwendungen in Smart Home-Apps auf dem Smartphone ausgeführt werden, werden die Services in Zukunft in die Cloud ziehen und von dort gesteuert werden.
4. Telekommunikationsanbieter: Auch die Rolle der Telekommunikationsanbieter wird in Zukunft immer wichtiger werden. So wird die Nachfrage nach leistungsfähiger Infrastruktur für Smart Home-Anwendungen immer bedeutsamer (Bitkom, 2015c, S. 55). Ein weiterer Grund für den Bedeutungsgewinn soll laut Raspin (2016) außerdem die Expansion der Telekommunikationsanbieter im Plattformbereich sein.
5. Smart Home Systeme oder Plattformen: Die Kommunikationssprache und Organisation der Interoperabilität ist sehr bedeutend für das Funktionieren des Smart Homes. Deshalb werden sich vor allem Plattformen, aufgrund ihrer hohen Interoperabilität in Zukunft zentral auf dem Smart Living-Markt positionieren.

Die künftige Relevanz der Plattformen wird so auch in der Marktanalyse der Deutschen Telekom AG (2015) betont und es wird prognostiziert, dass sich auf dem Smart Home-Markt in Zukunft plattform-basierte Modelle durchsetzen werden. Laut den Autoren sind bei dieser Entwicklung Parallelen zu den Entwicklungen der PC- und Smartphonemärkten zu erkennen. So wird die App-Plattform, Android, als Beispiel für eine erfolgreiche, offene Umgebung genannt, die durch Programmierschnittstellen (APIs) und Entwickler-Toolkits (SDKs) Interoperabilität ermöglicht. Über diese Analyse hinaus wurden in den Experteninterviews zu den Plattformen außerdem die Prognose gewagt, dass sich auf dem Smart Home-Markt, ähnlich wie auch bei den Smartphones (App-Stores), nur eine Handvoll Anbieter durchsetzen werden.

### 3.1.2 ERFOLGSFAKTOREN UND GRÜNDE FÜR VERÄNDERUNGEN IN DER AKTEURSLANDSCHAFT

Die Verschiebungen auf dem Smart Home-Markt und der Erfolg einiger Anbieter ist laut Meinung der interviewten Expertinnen und Experten vor allem auf die Erfüllung der Kundenwünsche zurückzuführen (vgl. Abschnitt 2.4). So ist zu beobachten, dass durch technologische Fortschritte Angebote immer kostengünstiger angeboten werden können. Gerade die großen Anwendungsplattformen von Google oder Apple und deren Sprachassistenten werden beispielsweise kostenlos angeboten.

Darüber hinaus kann beobachtet werden, dass auch der Nutzen der Anwendungen gewachsen zu sein scheint. So können nützliche Funktionen oder Steuerungsoptionen dank Datenanalyse und -auswertung angeboten werden und schaffen so für Nutzerinnen und Nutzer einen Mehrwert.

Auch der Branchenverband Bitkom (2015c) bestätigt diese Entwicklung im speziellen Bereich der Unterhaltungselektronik, weist aber auch darauf hin, dass die Nutzung von großen Datenmengen in Zukunft vor allem dann möglich sein wird, wenn Anbieter den vertrauenswürdigen Umgang mit Daten unter Beweis gestellt haben (S. 53).

## 3.2 AKTUELLE UND KÜNFTIGE GESCHÄFTSMODELLE

In der Marktanalyse der Telekom (2015) werden die aktuellen Geschäftsmodelle auf dem Smart Home-Markt diskutiert und Prognosen über zukünftige Geschäftsmodelle gewagt. Die Analyse stellt dar, dass derzeit vor allem **Hardware-Verkäufe** Gewinne auf dem Markt erzielen. Ähnlich erfolgreich könnten auch **Bezahlmodelle** oder Smart Home-**Abonnements** werden. Beim Smartphone ist dieses Zugangsmodell sehr verbreitet und so könnten Kundinnen und Kunden beispielsweise den Service eines sichereren oder komfortableren Zuhauses für eine monatliche Gebühr mieten.

Die Analyse prognostiziert weiterhin, dass sich entlang der **Wertschöpfungskette** einige Veränderungen auf dem Smart Home-Markt ergeben können. Ein Beispiel, das in der Analyse genannt wird, ist, dass Energieversorger in Zukunft nicht nur Rohstoffe liefern, sondern eine Leistung – Raumtemperatur, Helligkeit der Wohnung, o.ä. Diese Leistung würde dann neben den Rohstoffen auch das Equipment oder Wartungspakete umfassen. Ein weiteres Geschäftsmodell könnte die **Bündelung** von Smart Home-**Anwendungen und -Services** sein. Ein vernetzter Lautsprecher in Kombination mit einem Streaming-Dienst oder ein Smart TV gemeinsam mit einer Filmplattform. Letztlich können Smart Home-Anwendungen auch als **Kundenbindungsmaßnahme** in unternehmerische Geschäftsmodelle einfließen.

Für Anbieter aus dem Bereich der Technologie- und Internetkonzerne werden in der Untersuchung von Mücke, Sturm & Company (2015, S. 5) weitere Geschäftsmodelle aufgeführt, die den Eintritt in den Smart Home-Markt rechtfertigen. Neben den genannten Kundenbindungsmaßnahmen, die auch von Technologie- und Internetkonzernen verfolgt werden, zielen vor allem Software-Hersteller und datengetriebene Anbieter mit dem Markteintritt darauf ab, die **Sammlung und spätere Nutzung von Nutzerdaten** durch eigene Smart Home-Anwendungen zu verbessern. Außerdem ist es das Ziel der eCommerce-Anbieter durch Eintritt in den Markt **neue Vertriebswege** zu erschließen. Diese datengetriebenen Geschäftsmodelle werden im nächsten Abschnitt zu Big Data im Marktumfeld genauer beleuchtet.

## 3.3 DIE ROLLE VON BIG DATA FÜR ANBIETER

In der im Abschnitt 2.2 genannten Definition von Big Data zählt Value, also die Fähigkeit aus Daten einen Mehrwert zu generieren, zu den relevanten Eigenschaften. Ahmed et al. (2017, S. 466) beleuchtet diesen Mehrwert genauer und beschreibt die unternehmerischen Chancen, die sich in den letzten Jahren aus Big Data ergeben haben:

1. Wert entsteht daraus, dass Daten nicht nur gesammelt, sondern auch transparent und nutzbar gemacht werden.
2. Es können wertvolle Informationen über die Nutzerinnen und Nutzer extrahiert werden, die ohne Big Data und deren Auswertung nicht möglich gewesen wären.
3. Trends können besser vorhergesehen werden.
4. Durch eine steigende Effizienz in der Datenanalyse, beispielsweise durch Cloud-basierte Werkzeuge, werden die Kosten signifikant reduziert.

5. Diese Kostenreduktion geht auch damit einher, dass Unternehmen nicht mehr so stark von Datensilos und deren Betrieb abhängig sind.

In den Experteninterviews wurde die Rolle der Cloud-Anbindung ebenfalls als relevant erachtet und für den Erfolg von Big Data-Anwendungen im Smart Home verantwortlich gemacht. So verwundert es nicht, dass bereits 2016 die Hälfte aller analysierten Smart Home-Systeme und -Plattformen in einer Auswertung des BMWi (2016) Cloud-basiert waren.

Auch der Branchenverband Bitkom (2015b) beschreibt den Einsatz von Big Data-Geschäftsmodellen ausführlich (S. 114–116). Strategisch setzten Marktakteure Big Data entweder ein, um alte Geschäftsmodelle durch Daten effizienter zu gestalten oder neue Geschäftszweige zu erschließen. Hierfür werden entweder existierende Daten herangezogen oder neu erhoben. Auf dem Smart Home-Markt sind folgende Geschäftsmodelle relevant und werden deshalb im Folgenden genauer beleuchtet:

- Analytics-as-a-Service: Basierend auf geeigneten Infrastrukturen wie beispielsweise Cloud-Diensten stellen Anbieter Analyse- und Prognosedienste bereit. Für das Smart Home, sowie das Internet der Dinge existieren hierfür einige spezialisierte Anbieter.
- Data-as-a-Service: Ziel des Geschäftsmodells ist es, Nutzerdaten zu sammeln, zu aggregieren und Dritten zur Verfügung zu stellen. Die Daten können beispielsweise genutzt werden, um Werbung passgenauer zu gestalten. Hier ist denkbar, dass auch klassische Data Broker, wie Acxiom oder Experian, Smart Living-Anwendungen zukünftig als weitere Datenquelle nutzen werden (Crain, 2018). Ebenso sehen Werbetreibende das Internet der Dinge im Allgemeinen und Smart Home im Speziellen als neue Möglichkeit, Aufmerksamkeit für ein Produkt zu generieren (Aksu et al., 2018). Erste Versuche lassen sich zum Beispiel bei Amazons Echo Plattform beobachten, für die Amazon mit bestimmten Herstellern strategische Partnerschaften eingeht, um deren Produkte in Antworten von Alexa zu platzieren (Hirsch, 2018).
- Data-infused Products: Datengetrieben Produkte sind bestehende Produkte, die durch die Nutzung von Daten optimiert werden. Im Smart Home ist durch das komplementäre Auswerten der Daten beispielsweise eine effizientere Automation möglich und Kundenwünschen kann durch die Datengrundlage besser begegnet werden. Die Studie des Bitkom (2015b) zeigt an dieser Stelle außerdem auf, dass neben bereits existierenden, durch Daten ausgewerteten Produkten auch neue Produktklassen geschaffen werden. Hierzu werden die Wearables gezählt, deren Sensorik neue Nutzungsszenarien eröffnet.
- Datenmarktplätze: Das Geschäftsmodell dieser Anbieter basiert auf der Bereitstellung von Datenplattformen, die den Verkauf und die Nutzung von Daten ermöglichen. So können beispielsweise aggregierte Datensätze abgefragt werden und in eigene Anwendungen, z.B. im Smart Home, eingespeist werden.

## 3.4 PARTNERSCHAFTEN

Aus den genannten Geschäftsmodellen ergeben sich auch Möglichkeiten für Partnerschaften zwischen unterschiedlichen Akteuren auf dem Smart Home-Markt. In den Experteninterviews wurde beispielsweise bezüglich der datengetriebenen Geschäftsmodelle von neuen Partnerschaften gesprochen. So werden Partnerschaften zwischen Cloud- und Smart Home-Anbietern geschlossen, um Speicherplatz oder Rechenleistung für die Anwendungen zu schaffen. Auch bei der Datenanalyse existieren Partnerschaften, die gewährleisten, dass die gesammelten Smart Home-Daten nutzbar

gemacht werden können (vgl. Analytics-as-a-Service). In diesem Bereich gehen die Entwicklungen auf dem deutschen Markt jedoch laut Experten hin zur Inhouse-Analyse, beispielsweise durch Schaffung eigener Business Intelligence-Einheiten in den Unternehmen.

Auch im Bereich der Smart Home-Installation werden Partnerschaften auf dem Markt erwartet. Wie bereits in Abschnitt 2.1.2 vorgestellt sind Anwendungen in Komplettlösungen, mit hohem Installationsaufwand, und Plug-and-Play-Anwendungen mit einem geringen Installationsaufwand zu unterscheiden. Gerade wenn Smart Homes im Zukunft als Komplettlösung gedacht und in Neubauten integriert werden, sind Partnerschaften zwischen den **Herstellern der technischen Infrastruktur und Handwerkern** unabdingbar. So kann bereits jetzt beobachtet werden, dass (stationäre) Handwerker in den Installationsprozess einbezogen werden und so ein Zusammenspiel der Hardware ermöglicht wird (BMWi, 2016, S. 18).

Zuletzt seien auch noch einmal die **Plattformen** genannt, die in ihrer Sonderrolle bereits in Abschnitt 3.1 vorgestellt wurden. Diese Systeme oder Plattformen sind hierbei das technische und infrastrukturelle Bindeglied zwischen unterschiedlichen Hardware-Anwendungen und zielen darauf ab, möglichst viele Anwendungen zu vereinen. Im Fall der Telekommunikationsanbieter ergeben sich weitere infrastrukturelle Partnerschaften. So können beispielsweise über Router Verbindungen zwischen Anwendungen unterschiedlicher Anbieter geschaffen werden (BMWi, 2016, S. 18).

## 3.5 ZUSAMMENFASSUNG

Die Auswertung der relevanten Literatur und die Ergebnisse der Experteninterviews konnten zeigen, dass sich auf dem Smart Home-Markt viele unterschiedliche Akteure befinden, deren Rollen nicht nur streng nach Hardware und Software-Herstellern unterschieden werden können. Insgesamt kann beobachtet werden, dass Branchengrenzen verschwimmen und durch neue Partnerschaften den Wünschen der Verbraucherinnen und Verbrauchen besser begegnet werden kann. Ein weiteres Ergebnis der Auswertung ist, dass Plattformen, die die Interoperabilität der Anwendungen gewährleisten, eine bedeutende Rolle auf dem Smart Living-Markt der Zukunft spielen werden und auch der Einsatz von Big Data zur Generierung von Daten(mehr)werten ist entscheidend.

# 4 INFORMATIONELLE SELBSTBESTIMMUNG UND TRANSPARENZ

Als Recht auf informationelle Selbstbestimmung wird das Recht des Einzelnen verstanden, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Das geltende Datenschutzrecht in Deutschland (vgl. § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG)) sowie die im Mai 2018 in Kraft tretende Datenschutzgrundverordnung (DSGVO, vgl. Art. 6 Abs. 1) werden vom Grundsatz des Verbots mit Erlaubnisvorbehalt geprägt. Nur bei gesetzlichem Erlaubnistatbestand oder der Einwilligung des Betroffenen ist die Verarbeitung personenbezogener Daten erlaubt. Hierdurch soll die Privatsphäre des Individuums gestärkt und die Ausübung des Grundrechts auf informationelle Selbstbestimmung sichergestellt werden.

Die Einwilligung selbst unterliegt hierbei strengen Auflagen und muss, um wirksam zu sein, freiwillig, informiert und explizit erfolgen (vgl. § 4a BDSG, sowie Art. 6 Abs. 1 und Art. 7 DSGVO). Neben der Einwilligung existieren in der DSGVO grundsätzlich strenge Transparenzpflichten, die verständliche und zugängliche Texte verlangen (vgl. Art. 12 Abs. 1). So soll sichergestellt werden, dass Verbraucherinnen und Verbraucher über Datenverarbeitungen informiert sind. Doch gerade an der Informiertheit existieren in der Verbraucherrealität Zweifel, die beispielsweise in einer Studie von Kettner, Thorun und Vetter (2018) genauer beleuchtet werden. Die Relevanz des Datenschutzes für den Smart Living-Markt wird auch von der Befragung im Smart Home Monitor (2017) unterstrichen. Hier geben 58% der Befragten an, dass sie bisher keine Smart Home-Anwendung installiert haben, da sie sich um ihre Privatsphäre sorgen. Ähnlich verhält es sich mit digitalen Sprachassistenten (vgl. PwC, 2017, S.9). So äußern beispielsweise 69% Bedenken zum „gläsernen Kunden“ zu werden.

Wie begründet diese Verbrauchersorgen in Bezug auf das Smart Home sind, wurde bisher noch nicht systematisch untersucht. Die Mozilla Foundation (2017) liefert Anhaltspunkte für die Datenschutzpraktiken von Smart Home-Anwendungen für den amerikanischen Markt. Darüber hinaus existieren Forschungsprojekte, die sich mit Datenverarbeitungen von Apps beschäftigen, die auch auf dem Smart Home-Markt zum Einsatz kommen. Jedoch wurden noch keine systematischen Ergebnisse präsentiert (DATENSCHUTZscanner, 2018).

Ziel dieses Kapitels ist es deshalb, die aktuelle Verbrauchersituation im Bereich des Datenschutzes von Smart Living-Anwendungen zu untersuchen. Deshalb werden für drei Anwendungs- bzw. Produktbereiche (Anwendungs-Hot-Spots) die Datenschutzpraktiken relevanter Anbieter und ihre Datenschutzerklärungen geprüft und tiefergehend analysiert. In der Praxis ist das Vehikel, um Verbraucherinnen und Verbraucher über Datenverarbeitungen zu informieren, die Datenschutzerklärung. Sie muss vom verarbeitenden Anbieter zur Verfügung gestellt werden und bestimmte Voraussetzungen erfüllen. Neben den gesetzlichen Pflichten werden jedoch auch „weichere“ Untersuchungsdimensionen wie Gestaltungsparamente, Textinhalte sowie technische Zugriffe geprüft.

Im Folgenden wird zuerst die Auswertungsmethodik und die Stichprobe vorgestellt, hiernach werden die Bewertungskriterien festgelegt und diese dann für die ausgewählte Stichprobe analysiert.

## 4.1 METHODIK UND STICHPROBE

Zur Bearbeitung des Kapitels wurden zwei Methoden verwendet. Zum einen wurden mittels Desk Research, das heißt durch systematische Literatur- und Internetrecherche, die Faktoren, die zur

Ausübung der informationellen Selbstbestimmung mittels Datenschutztexten notwendig sind, identifiziert. Darüber hinaus wurde eine empirische Auswertung von Datenschutztexten vorgenommen. Bei der Auswertung handelt es sich um eine selektive und somit nicht repräsentative Auswertung, die für die Anwendungs-Hot-Spots Beleuchtung, Videokameras und Sprachassistenten durchgeführt wurde.

Hierbei ist es wichtig, auf die Steuerung der Produkte zu achten. Während smarte Beleuchtungen und Videokameras derzeit vor allem über das Smartphone bedient werden (Mittelsmann), sind Sprachassistenten auf einer anderen Steuerungsebene anzusiedeln, denn im Zentrum stehen die Sprachassistenzplattformen an sich und nicht ein Hardware-Produkt nebst Mittelsmann. Zwischen den Produktkategorien können somit nur begrenzt Vergleiche gezogen werden.

Grundlage für die Bewertung der Beleuchtungs- und Videokamera-Anwendungen sind die steuernden Apps und deren zugehörige Datenschutzerklärungen sowie die vorhandenen Produkt-Datenschutzerklärungen. Bei den Sprachassistenten werden die Datenschutzerklärungen der entsprechenden Plattformen ausgewertet.

## VORSELEKTION UND STICHPROBE

Während bei den Sprachassistenzsystemen alle N=4 auf dem deutschen Markt relevanten Angebote[5] ausgewertet wurden, wurde bei den Beleuchtungs- und Videokameraprodukten eine Vorauswahl getroffen. Voraussetzung für die Selektion der Produkte war:

a) Das Smart Home-Produkt muss in Deutschland käuflich zu erwerben sein.
b) Es liegen Daten vor, dass das Produkt relevant ist, d.h. von einem relevanten Anbieter auf dem Markt betrieben wird.[6]

Durch die Vorselektion wurden insgesamt N=8 Beleuchtungsprodukte ausgewählt und deren App- bzw. Produktdatenschutzerklärung ausgewertet. Bei den Videokameras ist die Fallzahl N=10.[7]

## ANALYSE DER DATENSCHUTZPRAKTIKEN

Nachdem die Anbieter bzw. Produkte vorselektiert wurden, wurden in der Analyse folgende Schritte absolviert: (1) Suche der Datenschutzerklärung im Playstore bzw. auf der Anbieterwebseite, (2) Dokumentation des Umfangs und der Gestaltung der Datenschutzerklärung, sowie bei deutschsprachigen Datenschutzerklärungen eine Auswertung der Lesedauer[8] und der Lesbarkeit der Inhalte[9], (3)

[5] Die analysierten Anwendungen werden im Appendix aufgelistet (vgl. Tabelle 12).
[6] Wenn keine Marktdaten zur Verbreitung der Anwendungen vorhanden waren, wurde die Anzahl der App-Downloads im Playstore, der aus Verbrauchersicht relevantesten App-Plattform, als Proxy für die Verbreitung verwendet. Die Anzahl der App-Downloads im Playstore wird global angegeben, d.h. sie ist nicht nur für den deutschen Markt relevant. Deshalb können die Gesamtdownloads nur einen Anhaltspunkt liefern, wie groß die Verbreitung der App tatsächlich in Deutschland ist. Insgesamt werden in unserer Auswertung nur Apps berücksichtigt, die mindestens 50.000 Downloads haben.
[7] Die analysierten Anwendungen werden im Appendix aufgelistet (vgl. Tabelle 12).
[8] Für die durchschnittliche Lesedauer wurden 220 Worte pro Minute angenommen. Eine Erläuterung dieser Annahme findet sich in Kettner et al. (2018).

bei App-gesteuerten Anwendung zusätzlich eine Dokumentation der technischen Zugriffe laut Playstore-Angaben.

## 4.2 FESTLEGUNG DER BEWERTUNGSKRITERIEN

Bei der Festlegung der Bewertungskriterien sind zum einen gesetzliche Vorgaben relevant, zum anderen sollte jedoch auch die Verbraucherrealität berücksichtigt werden. Im Folgenden werden deshalb zuerst die gesetzlichen Rahmenbedingungen in zwei Bewertungskriterien und für die Analyse relevante Indikatoren überführt. Hiernach werden fünf situationale Kriterien aus Ergebnissen von Verbraucherumfragen zu Datenschutztexten abgeleitet und die zugehörigen Indikatoren für die Prüfung definiert. Im letzten Schritt werden drei weitere Kriterien nebst Indikatoren zu technischen Zugriffen eingeführt. Orientierung bieten hierbei die Ergebnisse zweier Forschungsprojekte zum Datenschutz im Allgemeinen (vgl. DATENSCHUTZscanner, 2018; Kettner et al., 2018) sowie einer Auswertung der Mozilla Foundation zu Smart Home-Anwendungen im Speziellen (Mozilla Foundation, 2017).

### 4.2.1 NOTWENDIGE BEDINGUNGEN - DATENSCHUTZERKÄRUNG VORHANDEN UND IN DEUTSCHER SPRACHE

Grundsätzlich müssen Anbieter Nutzerinnen und Nutzer über die Verarbeitung von persönlichen Daten informieren. Dies gilt somit auch für Smart Home-Anwendungen, die Daten erheben und verarbeiten. Liegt **keine Datenschutzerklärung** vor, handelt es sich somit um einen Gesetzesverstoß, denn Verbraucherinnen und Verbrauchern ist es nicht möglich, sich ausreichend über Datenverarbeitungen zu informieren.[10]

Eine weitere gesetzliche Verpflichtung ist, dass verständlich über die Verarbeitung der personenbezogenen Daten informiert werden muss.[11] Dies würde bei strikter Auslegung bedeuten, dass in Deutschland auch eine **deutschsprachige Datenschutzerklärung** erforderlich ist.[12] Somit können für das erste Bewertungskriterium zur Verfügbarkeit der Datenschutzerklärung folgende Indikatoren abgeleitet werden (vgl. Tabelle 3):

---

[9] Zur Überprüfung der Lesbarkeit wurde das Online-Tool von Lenhard und Lenhard (2017) verwendet, welches auf Basis des sogenannten LIX Lesbarkeitsindex nach Björnson die Schwierigkeit von Texten bestimmt. Zur Überprüfung der Inhalte wurde der „DATENSCHUTZscanner Analyzer“ ein Tool aus dem Forschungsprojekt PrivacyGuard verwendet, welches ermöglicht beliebige, deutschsprachige Datenschutztexte automatisch zusammenfassen zu lassen (DATENSCHUTZscanner, 2018).

[10] Im Falle von Apps findet sich in den Leitlinien der Article 29 Data Protection Working Party (2017a) eine Erläuterung des Sachverhalts (Beispiel, S. 8): „For apps, the necessary information should also be made available from an online store prior to download.“ Dieser Aspekt wird in übernächsten Abschnitt unter „Zugänglichkeit“ separat geprüft.

[11] Art 12 Abs 1 (DSGVO) „Informationen (…), die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“.

[12] Dieser strikten Auslegung zur Sprache folgt auch das Analyseraster der Stiftung Warentest, die zu einzelnen Apps juristische Prüfungen vornimmt (bspw. Stiftung Warentest (2017) und (2018)).

| Bewertungskriterium | Indikatoren |
|---|---|
| Verfügbarkeit der Datenschutzerklärung | - Verlinkung auf Webseite bzw. im App-Store<br>- Ist die Datenschutzerklärung für das Produkt an sich bestimmt oder für einen anderen Zweck?<br>- Sprache |

Tabelle 3: Bewertungskriterium und Indikatoren zu notwendigen Bedingungen

### 4.2.2 KONTAKTMÖGLICHKEITEN FÜR DATENSCHUTZRECHTLICHE ANLIEGEN

Wann immer personenbezogene Daten erhoben werden, haben Verbraucherinnen und Verbraucher besondere Rechte. Insbesondere Auskunft, Berichtigung und Löschung zählen zu diesen Betroffenenrechten und müssen laut Gesetz einfach ausgeübt werden können. Anbieter sind deshalb verpflichtet, direkte Kontaktmöglichkeiten anzugeben.[13] Das Bewertungskriterium und der Indikator lauten wie folgt (vgl. Tabelle 4):

| Bewertungskriterium | Indikator |
|---|---|
| Kontaktmöglichkeit für datenschutzrechtliche Anliegen | - In der Datenschutzerklärung angegeben, bspw. als direkter Mail-Link oder Adresse |

Tabelle 4: Bewertungskriterium und Indikator zu Kontaktmöglichkeiten für datenschutzrechtliche Anliegen

### 4.2.3 VERBRAUCHERREALITÄT UND SITUATIONALE FAKTOREN

Das „Privacy Paradox" ist eine viel zitierte Beobachtung, die beschreibt, dass Verbraucherinnen und Verbraucher zwar angeben, dass ihnen der Schutz ihrer persönlichen Daten wichtig ist, sie jedoch in der Realität kein datensparsames Verhalten an den Tag legen und sich nicht ausreichend informieren (Norberg, Horne & Horne, 2007). So teilen Verbraucherinnen und Verbraucher persönliche Daten beispielsweise freiwillig in sozialen Netzwerken und der Branchenverband Bitkom (2015a) weist in einer Befragung darauf hin, dass die Mehrheit der Verbraucherinnen und Verbraucher (79%) Datenschutzerklärungen zustimmen, ohne sie gelesen zu haben. Die Gründe für dieses Verhalten sind vielfältig.

Eine Erklärung für dieses Verhalten können sogenannte situationale – der Entscheidungssituation entspringenden – Faktoren sein, die dafür sorgen, dass Verbraucherinnen und Verbraucher sich nicht oder nur begrenzt mittels Datenschutzerklärungen über Datenverarbeitungen von Diensten informieren (Kettner et al., 2018). Vor allem die **Textlänge**, der **Schwierigkeitsgrad** der verwendeten Sprache und die **Gestaltung** der Datenschutzerklärung scheinen eine Rolle zu spielen. In einer Befragung des Deutschen Institut für Sicherheit und Vertrauen im Internet (DIVSI) (2015, S.28) wünschen sich 74% der Befragten kürzere Datenschutztexte, 66% eine einfachere Sprache und 48% eine übersichtlichere Gestaltung des Textes / Layouts.

Über diese Faktoren hinaus spielt auch die (physische) **Zugänglichkeit** zur Datenschutzerklärung eine entscheidende Rolle (vgl. Article 29 Data Protection Working Party, 2017a, S. 8). In der Realität

[13] Art. 13 Abs. 1 DSGVO.

ist oftmals zu beobachten, dass Informationen über Datenverarbeitungen zwar vorhanden sind, jedoch schwer für Verbraucherinnen und Verbraucher zu finden sind oder sich hinter Hyperlinks auf Webseiten verbergen. In einer verhaltenswissenschaftlichen Studie für die Europäische Kommission beobachten Elshout et al. (2016), dass die Datenschutzerklärung nur von 9% der Verbraucherinnen und Verbraucher geöffnet wird, wenn sich diese in einem separaten Fenster befindet. In der Feldstudie von Kettner et al. (2018) ist dieser Anteil noch geringer und es kann beobachtet werden, dass weniger als 1% der Kundinnen und Kunden in einem Online-Shop die Datenschutzerklärung öffnen, wenn sich diese hinter einem Link „versteckt".

Die genannten Bewertungskriterien lassen sich, wie in Tabelle 5 dargestellt, durch eine Reihe von Indikatoren messen:

| Bewertungskriterien | Indikatoren |
|---|---|
| Textlänge | - Anzahl der Wörter<br>- Lesedauer<br>- Seitenumfang |
| Schwierigkeitsgrad der verwendeten Sprache | - Lesbarkeitsindex (LIX) unter Berücksichtigung der durchschnittlichen Satzlänge und dem Anteil langer Wörter |
| Gestaltung | - Unterteilung der Datenschutzerklärung durch (Zwischen-) Überschriften<br>- Darstellung in Tabellenform<br>- Verwendung von Bildsprache |
| Zugänglichkeit | - Ort der Datenschutztexte (Verlinkung an relevanter Stelle versus Anzeige per Default)<br>- Suchaufwand |

Tabelle 5: Bewertungskriterien und Indikatoren zu situationalen Faktoren

### 4.2.4 INHALTE DER DATENSCHUTZTEXTE

Das oben genannte Bewertungskriterium zum Schwierigkeitsgrad der verwendeten Sprache ist vor allem mit der Vollständigkeit und Rechtssicherheit der Datenschutztexte korreliert. Je technisch und juristisch präziser die Datenschutzerklärung, desto umfangreicher ist sie auch. Eine oftmals von Anbietern gewählte Strategie zur Verkürzung von Datenschutztexten ist die Verwendung von **ungenauen Formulierungen**. Der Hinweis „Wir erheben z.B. Ihren Namen, Adresse und Standort" oder „Grundsätzlich erheben wir Ihre Nutzungsdaten für …" lässt jedoch auch einen Spielraum für die Erhebung weiterer Daten oder für andere Zwecke.

Hieraus leitet sich, wie in Tabelle 6 aufgelistet, ein weiteres Bewertungskriterium nebst Indikatoren ab:

| Bewertungskriterium | Indikator |
|---|---|
| Ungenaue Formulierungen | - Unvollständige Aufzählungen<br>- Verwenden von „z.B.“, „in der Regel“ oder „grundsätzlich“ |

Tabelle 6: Bewertungskriterium und Indikatoren zu ungenauen Formulierungen

### 4.2.5 TECHNISCHE ZUGRIFFE UND BERECHTIGUNGSEINSTELLUNGEN ZUR DATENERHEBUNG (APP-SPEZIFISCH)

Welche technischen Daten bei Smart Home-Anwendungen erhoben werden, sind zum einen von der Anwendung an sich abhängig, zum anderen von der Steuerungsoberfläche. So kann das Gerät beispielsweise Audioaufnahmen vornehmen und wiedergeben, mittels Kamera die Raumumgebung aufnehmen oder Daten aus dem Internet laden und wiedergeben (Mozilla Foundation, 2017; Nickel, 2018). Die Steuerungsoberfläche für aktuelle Smart Home-Anwendungen ist, wie bereits erwähnt, unterschiedlich. Es kann beispielsweise eine zentrale Steuerung per Schalter erfolgen, aber auch die Steuerung mittels Sprache und Smartphone haben eine hohe Relevanz.

In den Kategorien Beleuchtung und Videokamera findet die Steuerung – vor allem von Plug-and-Play-Geräten – mittels App-Steuerung statt und ein Zugriff auf Funktionen des Smartphones ist somit möglich. Da Sprachassistenten übergeordnete Anwendungen sind, die meist nicht per App, sondern über das entsprechende Betriebssystem eingebunden sind, werden diese bei der Auswertung der Zugriffe nicht berücksichtigt.

Für die Auswertung der Zugriffe auf Smartphone-Funktionen sind drei Bereiche besonders relevant (vgl. Ingenrieth & Kettner, 2017):

1. Identifikation der Nutzerin / des Nutzers: Durch Auslesen von Konten auf dem Smartphone oder Erheben von Geräte-IDs und Anrufinformationen ist es prinzipiell möglich, Nutzungsverhalten über mehrere Anwendungen und einen längeren Zeitraum nachzuverfolgen. Im Spezialfall von statischen Gerätekennungen wird eine anonyme Nutzung der App und der durch sie gesteuerten Smart Home-Anwendung erschwert. Laut Richtlinien der Smartphone-Betriebssystemhersteller ist eine Erhebung statischer Gerätekennungen jedoch bei sensiblen Services und für Sicherheitszwecke erlaubt.
2. Nutzungsverhalten innerhalb und außerhalb der Anwendung: Auch durch Aufzeichnung des Nutzungsverhaltens mittels Zugriff auf den Geräte- und App-Verlauf ist es möglich, Nutzungsprofile zu erstellen. So können vertrauliche Protokolldaten anderer Apps oder der Verlauf angesehener Webseiten ausgelesen werden und durch eine App verarbeitet werden. Falls die Zugriffe anonym verwendet werden und an einen plausiblen Zweck gebunden sind, beispielsweise zur Optimierung der Anwendung, ist ein solcher Zugriff weniger problematisch. Wenn jedoch eine Verknüpfung von Daten aus anderen auf dem Smartphone befindlichen Apps oder mit dem allgemeinen Webseitenverlauf möglich ist, sind diese Zugriffsberechtigungen kritisch zu sehen.
3. Zugriffe auf Sensoren oder gespeicherte Inhalte des Smartphones: Die Apps, die zur Steuerung der Anwendungen genutzt werden, können Zugriff auf Kamera, Mikrofon, Standort, Kontakte oder Medien wie Fotos erhalten. Auch in diesem Fall gibt es Unterschiede in der Plausibilität der Erhebung. Manche Zugriffe können durch Funktionen gerechtfertigt wer-

den, beispielsweise wenn der Mikrofon-Zugriff eine Sprachsteuerung ermöglicht. Bei anderen Zugriffen, die den Zweck der Verarbeitung nicht sinnvoll begründen, ist die Plausibilität des Zugriffs jedoch unklar.

Bei der Beurteilung sollten zwei Aspekte berücksichtigt werden. Zum einen ist, wie bereits erwähnt, die Plausibilität der Zugriffe relevant, die stark vom Nutzungskontext abhängt. Idealerweise wird der Zweck der Erhebung in der Datenschutzerklärung im App-Store benannt. Zum anderen geht eine Zugriffsberechtigung nicht zwingend mit der Nutzung oder Auswertung der erhobenen Daten einher. Auch hier sollte die Erläuterung der Erhebung mittels Datenschutzerklärung aufschlussreich sein.

Die genannten Bewertungskriterien und die zugehörigen Indikatoren basieren auf den Berechtigungsgruppen im Playstore (Google-Play Hilfe, 2018) und lassen sich folgendermaßen zusammenfassen (vgl. Tabelle 7):

| Bewertungskriterien | Indikatoren |
|---|---|
| Identifikation der Nutzerin / des Nutzers | Erhebung von<br>- Geräte-IDs<br>- Anrufinformationen |
| Nutzungsverhalten innerhalb oder außerhalb der Anwendung | Zugriff auf<br>- Geräte-Verlauf<br>- App-Verlauf |
| Zugriffe auf Sensoren oder gespeicherte Inhalte | Zugriff auf<br>- Kamera<br>- Mikrofon<br>- Kontakte<br>- Standort<br>- Fotos / Medien / Dateien |

Tabelle 7: Bewertungskriterien und Indikatoren zu technischen Zugriffen

## 4.3 ERGEBNISSE

Im Folgenden werden die Ergebnisse der Textanalysen vorgestellt. Hierbei ist es wichtig zu beachten, dass die Ergebnisse nicht repräsentativ für die Anwendungskategorien sind und lediglich einen Anhaltspunkt über Datenschutzpraktiken geben können. Dennoch kann gezeigt werden, dass bereits in der kleinen Stichprobe zu sehen ist, dass Transparenzpflichten zum Teil nicht erfüllt werden und Verbraucherinnen und Verbraucher vor vielfältigen situationalen Herausforderungen stehen.[14]

### 4.3.1 NOTWENDIGE BEDINGUNGEN – DATENSCHUTZERKLÄRUNG VORHANDEN UND IN DEUTSCHER SPRACHE

Tabelle 8 zeigt die Ergebnisse der Überprüfungen der notwendigen Bedingungen und zur allgemeinen Einhaltung gesetzlicher Verpflichtungen. Die Datenschutztexte schließen hierbei sowohl die App-gestützten als auch die produktspezifischen Datenschutzerklärungen mit ein.

[14] Im Folgenden sind die Ergebnisse zur besseren Lesbarkeit auf ganze Zahlen gerundet.

Insgesamt sind die Ergebnisse unbefriedigend. So stellen zwei der acht Beleuchtungs-Apps lediglich für ihre allgemeine Webseite einen Datenschutztext zur Verfügung, nicht jedoch für ihre Anwendung bzw. App. Auch bei den Videokameras erfüllen nicht alle Anbieter die gesetzlichen Vorgaben. Auch hier stellen drei der zehn geprüften Anwendungen keine eindeutige Datenschutzerklärung für das Produkt bzw. die App zur Verfügung. Bei den Sprachassistenten ist dies anders. Hier stellen alle Anbieter eine Datenschutzerklärung zur Verfügung.

Lediglich zwei der acht Beleuchtungs-Apps bieten auf Anhieb eine deutsche Datenschutzerklärung an. Weitere zwei Anwendungen verlinken an der entsprechenden Stelle im Playstore zwar eine englische Datenschutzerklärung, es ist jedoch möglich mit einem gewissen Suchaufwand eine deutschsprachige Datenschutzerklärung ausfindig zu machen. Vier der acht Beleuchtung-Apps hingegen bieten nur eine englische Datenschutzerklärung an. Bei den Videokameras ergibt sich ein ähnliches Bild. Vier der zehn Anwendungen verlinken direkt eine deutsche Datenschutzerklärung, drei von zehn bieten diese nach einem gewissen Suchaufwand an und drei der zehn haben keine deutschsprachige Datenschutzerklärung. Bei den Sprachassistenten ist dies anders. So werden in allen Fällen deutschsprachige Datenschutzerklärungen angeboten, die auch einfach zu finden sind.

| Indikator | Beleuchtung (N=8) | Videokamera (N=10) | Sprachassistent (N=4) |
|---|---|---|---|
| Datenschutzerklärung für Produkt oder App vorhanden | | | |
| Zutreffend in % | 75% | 70% | 100% |
| Sprache | | | |
| Deutsch in % | 25% | 40% | 100% |
| Deutsch mit Suchaufwand in % | 25% | 30% | 0% |
| Englisch in % | 50% | 30% | 0% |

Tabelle 8: Ergebnisse zu notwendigen Bedingungen

### 4.3.2 KONTAKTMÖGLICHKEITEN FÜR DATENSCHUTZRECHTLICHE ANLIEGEN

Die nächste Bewertungskategorie betrifft die Möglichkeit für Nutzerinnen und Nutzer, ihre Betroffenenrechte im Falle eines Falles ausüben zu können. Deshalb wurde geprüft, wie viele der Datenschutztexte (sowohl App-gesteuert, als auch produktspezifisch) Kontaktmöglichkeiten anbieten. Die Ergebnisse sind in Tabelle 9 abgebildet. In die Auswertung fließen die deutschsprachigen und die englischsprachigen Datenschutzerklärungen mit ein.

Bei den Beleuchtungs-Apps sind bei sieben der acht Anwendungen Kontaktmöglichkeiten angeben, bei den Videokameras sind es sieben von zehn. Bei Sprachassistenten sind die notwendigen Kontaktdetails für datenschutzrechtliche Anliegen in allen geprüften Fällen vorhanden.

| Indikator | Beleuchtung (N=8) | Videokamera (N=10) | Sprachassistent (N=4) |
|---|---|---|---|
| Kontakt vorhanden in % | 88% | 70% | 100% |

Tabelle 9: Ergebnisse zu Kontaktmöglichkeiten für datenschutzrechtliche Anliegen

### 4.3.3 VERBRAUCHERREALITÄT UND SITUATIONALE FAKTOREN

Tabelle 10 gibt einen Überblick über die Analyse der situationalen Faktoren zur Bewertung der Datenschutztexte. Für die Bewertungskriterien Länge, Gestaltung und Zugänglichkeit wurden alle Datenschutztexte berücksichtigt. Für das Bewertungskriterium zum Schwierigkeitsgrad der verwendeten Sprache wurden nur die deutschen Datenschutztexte bewertet, da das LIX-Tool ausschließlich für deutschsprachige Texte verwendet werden kann.

| Indikator | Beleuchtung (N=8) | Videokamera (N=10) | Sprachassistent (N=4) |
|---|---|---|---|
| Länge | | | |
| Durchschnittliche Wortanzahl | 1.942 | 1.844 | 3.289 |
| Durchschnittliche Lesedauer | 8 Minuten 50 Sekunden | 8 Minuten 23 Sekunden | 14 Minuten 57 Sekunden |
| Durchschnittliche Anzahl Seiten in 10pt | 3,9 | 3,60 | 6,3 |
| Schwierigkeitsgrad der verwendeten Sprache | | | |
| LIX-Score[15] | 61,35 (Fachliteratur) | 64,26 (Fachliteratur) | 61,05 (Fachliteratur) |
| Gestaltung | | | |
| Besonderheiten | 1 von 8 Anbietern nutzt interaktive Navigationsleiste für Überschriften | 1 von 10 Anbietern verwendet Navigation via Drill-Down-Menü | 4 von 4 verwenden ansprechende, einfach navigierbare Datenschutzerklärungen bspw. Drill-Down-Menü, Navigationsleiste |
| Zugänglichkeit | | | |
| Link ohne zusätzlichen Suchaufwand erreichbar | 100% | 80% | 100% |

Tabelle 10: Ergebnisse zu situationalen Faktoren

#### LÄNGE

Die durchschnittliche Länge der Datenschutzerklärungen der ausgewählten Beleuchtungs- und Videokamera-Anwendungen bzw. -Apps ist mit knapp unter 2.000 Worten ähnlich lang. Hieraus

[15] Der LIX-Score kann nur für deutsche Datenschutzerklärungen berechnet werden; Dies sind bei den Beleuchtungsanwendungen N=4, bei den Videokameras N=7 und bei den Sprachassistenten N=4

ergibt sich für die beiden Produktkategorien eine durchschnittliche Lesedauer von über 8 Minuten und ein Seitenumfang zwischen drei und vier DIN-A4-Seiten. Die Datenschutztexte für die Sprachassistenzsysteme sind mit über 3.000 Wörtern länger und im Druck mit über sechs Seiten umfangreicher. Dies spiegelt sich auch in der durchschnittlichen Lesedauer von fast 15 Minuten wieder.

## SCHWIERIGKEITSGRAD DER VERWENDETEN SPRACHE

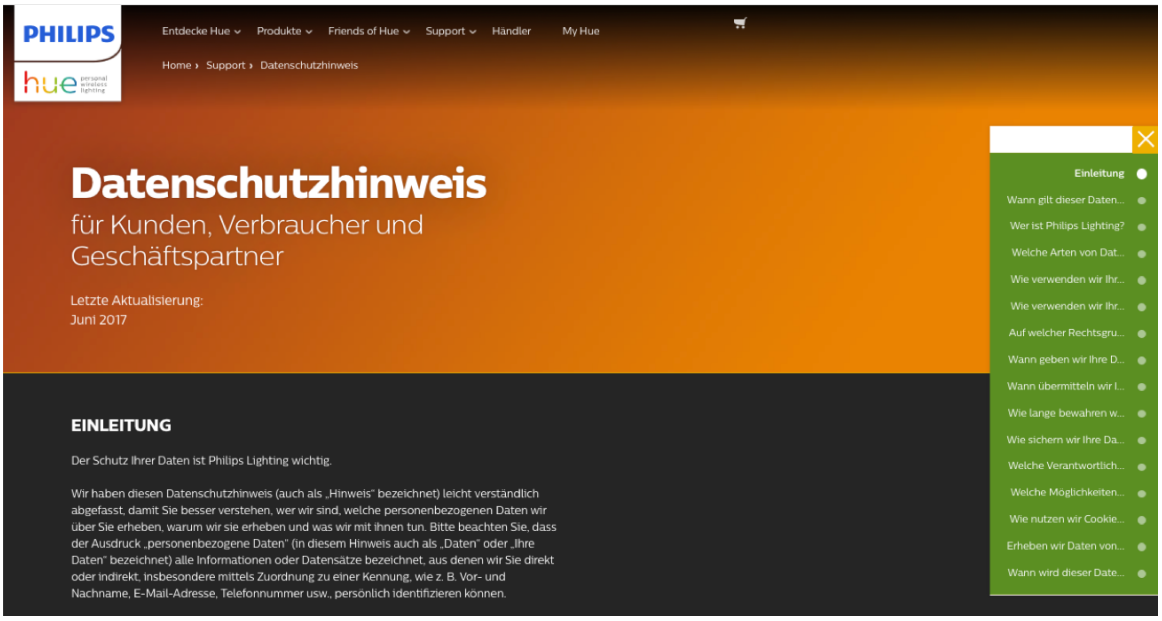
Sowohl die Datenschutzerklärungen der deutschsprachigen Beleuchtungs- und Videokamera-Apps, als auch die der Sprachassistenten entsprechen in ihrer Schwierigkeitsstufe, die aus dem Lesbarkeitsindex (LIX) abgeleitet werden kann, der Kategorie „Fachliteratur". Aus dem Rahmen fällt hierbei eine Datenschutzerklärung einer smarten Glühbirne, die einen sehr kurzen Text verwendet, der nur einen mittleren Schwierigkeitsgrad aufweist, jedoch wirkt sich dies auf die Vollständigkeit aus und somit auf die Präzision.

## GESTALTUNG

Die Gestaltung der Datenschutzerklärungen der Beleuchtungs-Apps und Videokameras ist mit wenigen Ausnahmen durch Überschriften gegliedert. Jedoch wird vorzugsweise Fließtext verwendet. Darüber hinaus werden in den meisten Fällen keine Navigationselemente eingebunden, die das Lesen der Nutzerinnen und Nutzer unterstützen könnten. Bei den Beleuchtungsprodukten gibt es lediglich einen Anbieter, der die Navigation durch die Datenschutzerklärung mittels eines Inhaltsverzeichnisses ermöglicht (vgl. Abbildung 2). Bei den Videokameras verwendet eines der Produkte ein Drill-Down-Menü zur Navigation durch die Datenschutzerklärung (vgl. Abbildung 3).

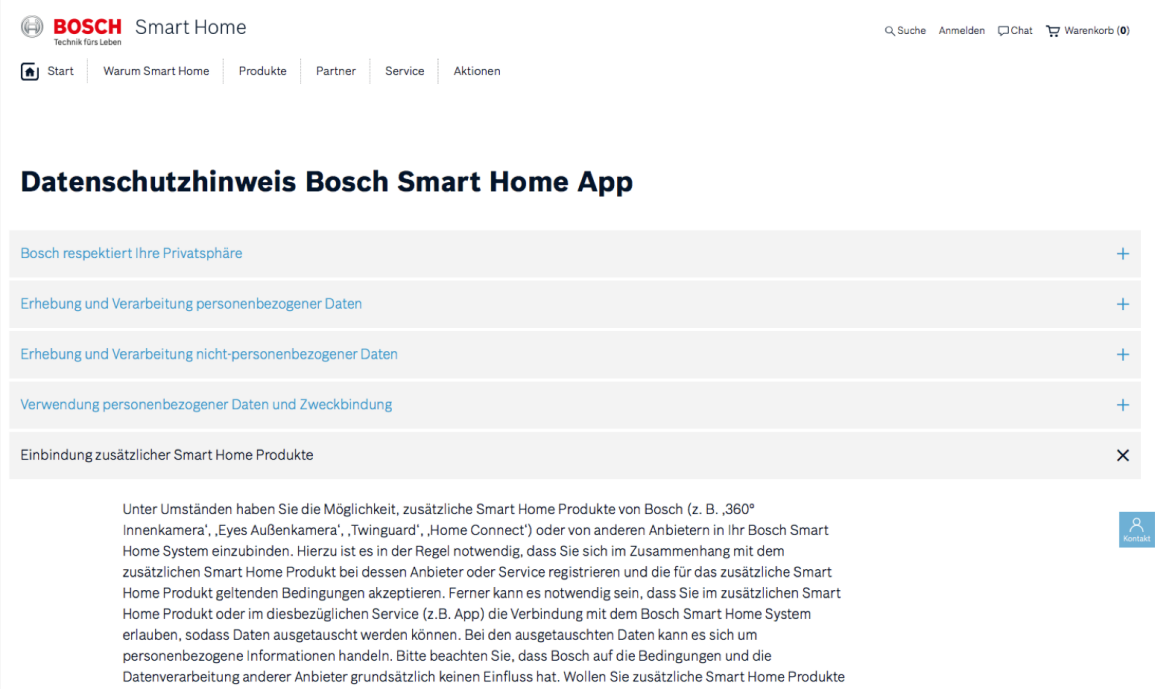
Bei den Sprachassistenzsystemen ist die Gestaltung im Allgemeinen ansprechender. Alle Dienste erleichtern das Lesen, indem sie entweder Navigationselemente wie Drill-Down-Menüs oder navigierbare Überschriften verwenden. Außerdem werden Produktinformationen durch bildliche Darstellungen komplementiert.

Abbildung 2: Beispiel - Datenschutzerklärung mit Navigationsleiste



(Philips, 2017)

Abbildung 3: Beispiel - Datenschutzerklärung mit Drill-Down-Menü




(Bosch, 2018)

## ZUGÄNGLICHKEIT

Sowohl bei den geprüften Beleuchtungsprodukten als auch bei den Sprachassistenten war die Datenschutzerklärung an der vorgesehenen Stelle und somit ohne zusätzlichen Suchaufwand vorzufinden. Für die App-gesteuerten Produkte gab es hierzu einen funktionalen Link in der Playstore-Beschreibung. Eine Anzeige per Default wurde jedoch für keine der geprüften Anwendungen gefunden. Bei zwei der zehn Videokamera-Produkte war die Verlinkung im Playstore mangelhaft und die Datenschutzerklärung war lediglich über eine eigene, unabhängige Suche zu finden.

## 4.3.4 INHALTE DER DATENSCHUTZTEXTE

In allen Datenschutzerklärungen wurden unvollständige Aufzählungen verwendet. Hierbei konnte beobachtet werden, dass der Grad der Vollständigkeit nur teilweise mit der Textmenge der Datenschutzerklärungen zusammenhängt.

Auch wenn dieses Ergebnis keine juristische Prüfung der Texte beinhaltet und nicht technisch nachvollzogen werden kann, welche Daten tatsächlich und für welchen Zweck verarbeitet werden, existiert für Verbraucherinnen und Verbraucher insgesamt betrachtet eine Unsicherheit bezüglich der Datenschutzpraktiken der geprüften Anwendungen.

### 4.3.5 TECHNISCHE ZUGRIFFE UND BERECHTIGUNGSEINSTELLUNGEN ZUR DATENERHEBUNG (APP-SPEZIFISCH)

Die Auswertung der technischen Zugriffe bezieht sich auf die App-gesteuerten Smart Home-Produkte aus der Beleuchtungs- bzw. Videokamera-Kategorie. Auch Sprachassistenten werden zum Teil per App gesteuert, sie sind jedoch auch in den meisten Fällen an das Betriebssystem der jeweiligen Endgeräte geknüpft. Deshalb werden die Sprachassistenten nicht ausgewertet.

#### IDENTIFIKATION DER NUTZERIN / DES NUTZERS

Die Hälfte der Beleuchtungs-Apps sind mittels Auslesen von Konten oder Erhebung von Gerätekennungen oder Anrufinformationen prinzipiell in der Lage, Nutzerinnen und Nutzer durch die App zu identifizieren. Bei den Videokameras sind es sogar 80%.

#### NUTZUNGSVERHALTEN INNERHALB UND AUßERHALB DER ANWENDUNG

Auch auf das Nutzungsverhalten auf dem Smartphone können einige der Steuerungsanwendungen zugreifen. So können 25% der Beleuchtungs-Apps auf den Geräte- und App-Verlauf zugreifen, bei den Videokameras liegt der Anteil bei 40%. Bei zwei der zehn Videokameras konnte außerdem festgestellt werden, dass diese „vertrauliche Protokolldaten“ auslesen können.

#### ZUGRIFFE AUF FUNKTIONEN

Sowohl bei den App-gesteuerten Lampen als auch bei den Videokameras greifen knapp zwei Drittel auf die Kamerafunktion des Smartphones zu. Die Hälfte der Lampen nutzt den Mikrofonzugriff und auch 80% der Videokamera-Apps ermöglichen dies. Auch beim Zugriff auf die Kontakte ist ein Unterschied zwischen Beleuchtungsprodukten und Videokameras festzustellen. So greifen 25% der Lampen auf Konten, die in den Kontakten gespeichert sind, zu. Bei den Videokameras sind es 80%, wobei von diesen mehr als die Hälfte neben den Konten auch die Kontakte an sich auslesen können. Auf den Standort können 75% der Beleuchtungsprodukte und 40% der Videokameras zugreifen, bei Fotos, Medien und Dateien haben 75% der Beleuchtungsprodukte und 100% der Videokameras einen Zugriff, d.h. können diese mindestens auslesen. Im Durchschnitt greifen die Beleuchtungs-Apps auf 2,9 und Videokamera-Apps auf 3,6 Berechtigungen zu.

Tabelle 11 fasst die Ergebnisse zusammen:

| Indikator | Beleuchtung (N=8) | Videokamera (N=10) | Sprachassistent |
|---|---|---|---|
| Identifikation der Nutzerin / des Nutzers | | | |
| Zugriff auf Konten und/oder Geräte-IDs oder Anrufinformationen | 50% | 80% | n/a |
| Nutzungsverhalten innerhalb und außerhalb der Anwendung | | | |
| Zugriff auf den Geräte- und App-Verlauf | 25% | 40% | n/a |
| Zugriff auf Funktionen | | | |
| Kamera | 62,5% | 60% | n/a |
| Mikrofon | 50% | 80% | n/a |
| Kontakte | 25% | 80% | n/a |
| Standort | 75% | 40% | n/a |
| Fotos/Medien/Dateien | 75% | 100% | n/a |
| Durchschnittliche Zugriffe | 2,9 | 3,6 | n/a |

Tabelle 11: Ergebnisse zu technischen Zugriffen

Wie bereits eingangs erwähnt, kann hierbei nicht die Plausibilität der Erhebung der Daten beurteilt und auch nicht überprüft werden, ob ein Zugriff tatsächlich technisch erfolgt. Dennoch ergeben sich aus dieser Vielzahl von Zugriffen Fragen für Verbraucherinnen und Verbraucher.

## 4.4 WEITERE FAKTOREN / PERSONALE FAKTOREN

Neben den DSE-inhärenten Faktoren, die in der vorgestellten Analyse berücksichtigt wurden, existieren in der verhaltenswissenschaftlichen Literatur weitere Faktoren, die die Informiertheit der Verbraucherinnen und Verbraucher beeinflussen. Hierzu zählen psychologische Aspekte, die in Abbildung 4 aufgezählt werden (vgl. Kettner et al., 2018).

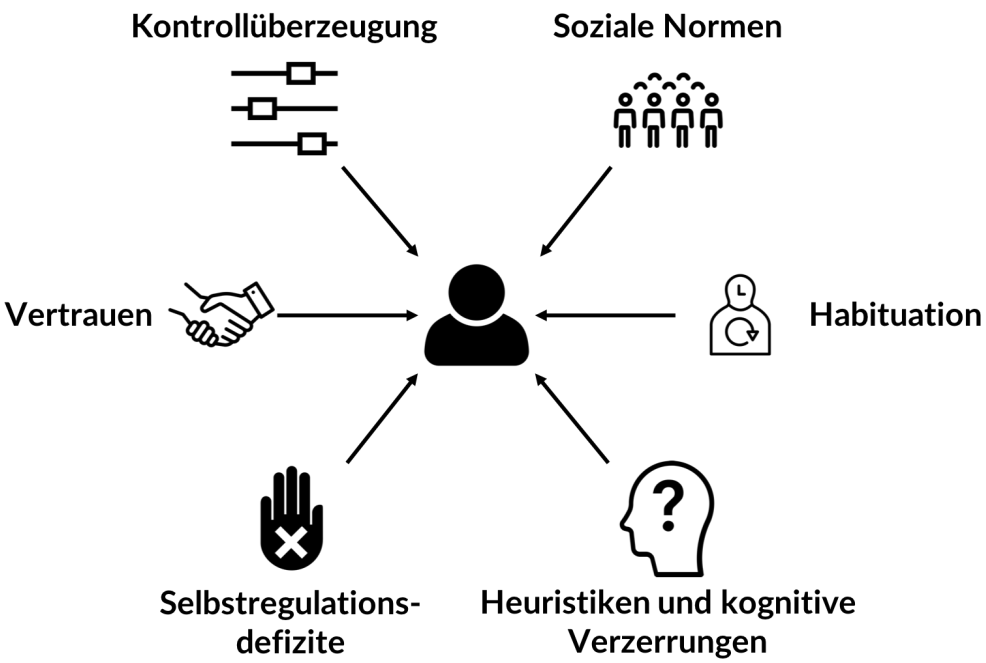
1. Kontrollüberzeugung: Oftmals empfinden Verbraucherinnen und Verbraucher bei Datenverarbeitungen keine wirkliche Wahlfreiheit und dementsprechend keine Kontrolle. Zwar bleibt es ihnen frei, den Datenverarbeitungen nicht zuzustimmen und auf die Nutzung eines Dienstes zu verzichten; diese „Friss oder stirb"-Alternative hilft im konkreten Entscheidungsfall jedoch kaum weiter.
2. Soziale Normen: Soziale Normen sind Annahmen über das Verhalten anderer, die sich als „Orientierungshilfe" auf das eigene Verhalten auswirken. Wenn Verbraucherinnen und Verbraucher also annehmen, dass andere Datenschutztexte nicht oder kaum lesen, so rechtfertigt dies auch das eigene Nicht-Lesen.
3. Habituation: Sogenannte Gewohnheitseffekte wirken ebenfalls stark auf das Leseverhalten von Verbraucherinnen und Verbrauchern. Je öfter sie beispielsweise mit Texten konfrontiert werden, desto mehr gewöhnen sie sich hieran und verringern ihre Aufmerksamkeit, wenn neue Datenschutztexte präsentiert werden.
4. Heuristiken und kognitive Verzerrungen: Auch kognitive Verzerrungen können Hürden für die Informiertheit von Verbraucherinnen und Verbrauchern darstellen. Beispielsweise urteilen Verbraucherinnen und Verbraucher danach, wie sehr ein Entscheidungsumfeld einem repräsentativen Prototyp entspricht (Repräsentativitätsheuristik). Ist eine Website oder App z.B. vertrauenswürdig gestaltet, nehmen Verbraucherinnen und Verbraucher an, dass auch

Datenschutzpraktiken vertrauenswürdig sind und sparen sich das Lesen der Datenschutztexte.

5. Selbstregulationsdefizite: Verbraucherinnen und Verbraucher haben die Fähigkeit, sich selbst zu regulieren, beispielsweise indem sie Belohnungen aufschieben. So stehen im Fall des Datenschutzes Kosten in Form des Lesens der Texte einer Belohnung (sofortige Nutzung eines Dienstes oder App) entgegen. Wird diese Fähigkeit überstrapaziert, weil Texte besonders lang sind, kann sich dies negativ auf das Lesen auswirken.
6. Vertrauen: Wenn das Verbrauchervertrauen besonders hoch ist, beispielsweise wenn Datenschutztexte durch positive Rahmung und gezielte vertrauensschaffende Formulierungen Vertrauenswürdigkeit signalisieren, setzen Verbraucherinnen und Verbraucher sich weniger häufig mit Datenschutztexten auseinander.

Die genannten psychologischen Faktoren stellen lediglich einen Teilausschnitt dar und können um weitere Hürden erweitert werden. In der Studie von Kettner, Thorun und Vetter (2018) finden sich hierzu weitere Beispiele und empirische Belege für die beobachtbaren Verhaltenstendenzen.

Abbildung 4: Psychologische Faktoren, die die informationelle Selbstbestimmung beeinflussen




(Eigene Abbildung auf Grundlage von Kettner et al., 2018)

## 4.5 ZUSAMMENFASSUNG

Die Auswertung ausgewählter Datenschutztexte in Bereich smarter Beleuchtung, Videokameras und Sprachassistenten zeigt, dass diese oftmals hinter gesetzlichen Vorgaben zurückbleiben. So haben einige Produkte keine Datenschutzerklärung oder nur in englischer Sprache. Die Texte sind außerdem insgesamt sehr lang und komplex und nur selten werden gestalterische Elemente eingesetzt, die das Lesen der Verbraucherinnen und Verbraucher unterstützen. Bei App-gesteuerten Produkten fällt außerdem auf, dass technische Zugriffe auf das Smartphone gewährt werden, bei denen Zwei-

fel bestehen, ob diese erforderlich sind. Auch wenn die Ergebnisse nicht repräsentativ sind, werfen sie einige Fragen für den Datenumgang von Smart Home-Anwendungen auf.

Neben den Prüfergebnissen wurde außerdem diskutiert, dass personale Faktoren eine Auswirkung auf die Informiertheit der Verbraucherinnen und Verbraucher haben können. Hierzu zählen beispielsweise eine mangelnde Kontrollüberzeugung, soziale Normen, Habituation, Heuristiken, Selbstregulationsdefizite und Vertrauen.

Da bisher lediglich die Erhebungsseite der datenverarbeitenden Anbieter beleuchtet wurde, ist es im nächsten Kapitel notwendig die Zwecke der Erhebung genauer zu analysieren.

# 5 UMGANG MIT NUTZERDATEN: USER-PROFILING UND DATENWEITERGABE

Ziel dieses Kapitels ist die Analyse des Umgangs mit Nutzerdaten, die im Smart Home erhoben werden. Hierbei wird zuerst der Zweck der Datenerhebung beleuchtet und die Konsequenzen der möglichen Profilbildung dargestellt. Im nächsten Schritt wird die Frage beantwortet, wie anbieterseitig der Datenhandel betrieben wird und ob und in welcher Form Daten an Dritte weitergegeben werden. Hierbei spielen auch Handelsplattformen eine Rolle.

## 5.1 BEDEUTUNG UND ZWECKE DES USER-PROFILINGS AUS ANBIETERPERSPEKTIVE

Bei Online-Diensten im Allgemeinen und sozialen Netzwerken im Speziellen haben sich viele Nutzerinnen und Nutzer daran gewöhnt, dass der Dienst zwar "kostenlos" zur Verfügung gestellt wird, dass Unternehmen jedoch mit den erfassten Nutzungsdaten Geld verdienen. So können Anbieter mehr Geld für Werbeplätze verlangen, je genauer und umfangreicher die Profile der Nutzerinnen und Nutzer auf der Plattform sind. So erwirtschaftete Facebook im zweiten Quartal 2017 $9,16 Milliarden an Werbeeinnahmen (Swant, 2017). Bei Online-Diensten erfolgt User-Profiling vorrangig mit dem Ziel, höhere Preise für Werbeplätze, durch exakte und umfassende Nutzerprofile, zu erzielen. So definiert die EU Datenschutzgrundverordnung Profiling als *„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen"*. (Art. 4 Abs. 4 DSGVO)

Die Artikel-29-Datenschutzgruppe, die die Europäische Kommission in Datenschutzfragen unabhängig berät, schreibt weiterhin zu Profiling: *„Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar."* (Article 29 Data Protection Working Party, 2017b)

Diese Art der Datenerhebung und -auswertung mit dem klaren Ziel, mehr über *Nutzerinnen und Nutzer* als Personen zu erfahren findet zwar in bestimmten Kategorien von Smart Home-Anwendungen statt (beispielsweise Sprachassistenten, Smart-TVs) im Allgemeinen scheint es jedoch keineswegs so umfassend, tiefgreifend und allgegenwärtig stattzufinden, wie bei Online-Diensten und Apps. Bei User-Profiling im Smart Home lässt sich derzeit nicht eindeutig beantworten, welche Rolle es spielt. Die meisten Smart Home-Geräte erheben Daten und senden diese mit unterschiedlicher Häufigkeit an den Hersteller bzw. den Betreiber zurück. Wie tiefgehend und für welchen Zweck diese Daten ausgewertet werden, scheint jedoch stark vom Unternehmen abzuhängen. Im Folgenden werden einige der zentralen Gründe für eine Datenerhebung und -auswertung durch Smart Home-Geräte aufgelistet:

- Durch die Datenerhebung und Auswertung werden detaillierte Nutzerprofile erstellt, um die eigene Dienstleistung besser an den Kundinnen und Kunden anzupassen (Personalisie-

rung) und / oder die Profile an Dritt-Unternehmen zu verkaufen („Klassisches“ User-Profiling, wie es von Online-Diensten und sozialen Netzwerken bekannt ist).
- Die Datenanalyse erfolgt vorranging, um das eigene Produkt zu verbessern.
- Ähnlich zu Industrieanwendungen, kann die Datenauswertung auch für *Predictive Maintenance*, der Prognose von Verschließerscheinungen, genutzt werden.
- Die gewonnenen Erkenntnisse werden (aggregiert) an Drittanbieter im Zuge einer strategischen Partnerschaft verkauft oder kostenfrei weitergegeben, ohne dass eine unmittelbare Profilerstellung geschieht.

Eine Besonderheit bei Smart Home-Anwendungen ist, dass ein Profiling unter Umständen auch durch externe Dritte, also nicht den Hersteller oder Betreiber selbst, erfolgen kann. Mehrere Studien und Untersuchungen haben gezeigt, dass eine externe Überwachung und Analyse des reinen Datenverkehrs der Smart Home-Anwendungen teils tiefgehende Aufschlüsse über die Lebensgewohnheiten von Smart Home-Nutzerinnen und -Nutzern geben können (Hill & Mattu, 2018). Dies ist möglich, indem das Muster des Datenverkehrs, der durch verschiedene Smart Home-Geräte erzeugt wird, passiv analysiert wird (Copos et al., 2016). Dieses Vorgehen ist selbst bei verschlüsseltem Datenverkehr möglich und stellt potentiell eine neue Dimension des User-Profilings dar (Apthrope et al., 2017). Hierfür wäre jedoch die Überwachung des Internetanschlusses eines Smart Homes nötig, weswegen vermutlich auch zukünftig das unrechtmäßige User-Profiling durch Dritte eher eine Randerscheinung bleiben wird.

## 5.2 DATENHANDEL UND -WEITERGABE AN DRITTE

Wie zuvor erwähnt, gibt es eine Vielzahl an Smart Home-Plattformen, von denen die meisten einen “Walled-Garden” erschaffen: Innerhalb eines bestimmten Ökosystems können Geräte miteinander problemlos kommunizieren. Sind einzelne Smart Home-Geräte jedoch nicht Teil des Ökosystems oder unterstützen einen bestimmten Standard nicht, müssen sie separat angesteuert und verwaltet werden. Dieser Umstand wurde ebenso im Expertenworkshop als eines der zentralen Probleme für die Weiterentwicklung des Smart Home identifiziert. Der Komfortverlust ist einer der Gründe, weswegen die Idee eines Smart Homes erst langsam auf ernsthaftes Interesse bei Verbraucherinnen und Verbrauchern trifft. Die derzeitige Realität ist, dass Smart Home-Geräte von unterschiedlichen Herstellern meist eigene Apps zur Steuerung und eigene Accounts benötigen. Diese derzeitig extrem heterogene und zerstückelte Landschaft bei Smart Home-Anwendungen erklärt wiederum, weswegen sich bisher keine dominanten Handelsplattformen zum User-Profiling herausgebildet haben. Einzelne Hersteller experimentieren über strategische Partnerschaften mit Data Brokern, dies scheint jedoch keinesfalls der Standard zu sein.

Gleichzeitig sind mehrere Entwicklungen hinsichtlich Datenhandel und -weitergabe bei Smart Home-Anwendungen zu beobachten:

### 5.2.1 PUNKTUELLER DATENHANDEL DURCH EINZELNE HERSTELLER

Wenn bei einzelnen Geräten durch den Hersteller oder den Betreiber eine Datenweitergabe an Dritte stattfindet, geschieht dies meist intransparent und ohne Wissen der Nutzerinnen und Nutzer. So wurde Vizio, zeitweise einer der populärsten Hersteller für Smart TVs am US-amerikanischen Markt, durch die US Federal Trade Commission (FTC, 2017a) vorgeworfen die Privatsphäre seiner

Nutzer zu verletzen. In Tests wurde nachgewiesen, dass Vizio Smart TVs jede Sekunde den Bildinhalt überprüfen, um zu identifizieren, was Nutzerinnen und Nutzer gerade sehen. Diese Informationen wurden dann, zusammen mit der IP-Adresse des Gerätes, an das Unternehmen zurückgesendet. So hatte Vizio ein umfassendes Bild von den Sehgewohnheiten von über 11 Millionen Nutzerinnen und Nutzern. Diese Daten wurden dann vollständig an Werbeunternehmen verkauft, um Nutzerinnen und Nutzer über die ebenfalls geteilte IP-Adresse eindeutig identifizieren zu können. Durch Datenhändler und Vizio wurden diese Datensätze weiter angereichert: Adresse, Geschlecht, Einkommen, etc. (FTC, 2017b). All dies geschah ohne die Einwilligung oder das Wissen der Nutzerinnen und Nutzer. Letztlich musste Vizio $2,2 Millionen an Strafe zahlen, jegliche Datenerhebung beenden und einen Großteil der erhobenen Daten löschen. Der Vizio-Fall veranschaulicht, dass die Intransparenz bzgl. Datenhandel und -weitergabe, die Nutzerinnen und Nutzer bereits von Online-Diensten und Apps kennen, zukünftig ebenso gut Einzug ins Smart Home nehmen wird.

### 5.2.2 MACHTKONZENTRATION BEI SPRACHASSISTENTEN

Wie zuvor erwähnt, sind Sprachassistenten, wie Google Home oder Amazon Echo, eine Smart Home-Anwendung, die auf großes Interesse bei Nutzerinnen und Nutzern stößt (Billboard, 2017). Nicht zuletzt, da sie es teils erst ermöglichen, eine Vielzahl anderer Smart Home-Anwendungen zentral zu managen. Die beiden derzeit dominanten Akteure sind Amazon und Google. Beide besitzen jedoch schon umfassende Nutzerprofile, um Verkaufsangebote respektive Werbung besser zu platzieren. In beiden geschlossenen Ökosystemen spielt User-Profiling daher eine zentrale Rolle. Der Sprachassistent wird schlicht als weitere Möglichkeit der Datenerfassung zur Profilbildung genutzt und so die jetzt schon vorhandene Machtposition, zumindest bei Google und Amazon, weiter ausgebaut.

### 5.2.3 MARKTPLÄTZE

Auch, wenn derzeit Handelsplattformen (Data Broker) bei Smart Home-Anwendungen nur eine untergeordnete Rolle spielen, ist es denkbar, dass zukünftig Marktplätze für Smart Home-Daten entstehen. Ein solcher Ansatz wird derzeit durch den IOTA Marktplatz pilotiert (Sønstebø, 2017). Teilnehmerinnen und Teilnehmer des Marktplatzes können ihre Sensordaten als Live-Streams anbieten, bezahlt wird direkt über das Netzwerk (IOTA, 2018), das ähnlich zu einer Blockchain funktioniert. Wenn zukünftig jedes Haus Luft-, Wärme- oder CO2-Sensoren besitzt, sehen die Anbieter, einen Sinn darin, diese über einen zentralen Marktplatz abrufen zu können. Hierbei geht es weniger um Profiling einzelner Nutzerinnen und Nutzer. Vielmehr wären solche Marktplätze interessant, um Sensordaten geographisch zu vergleichen.

## 5.3 KONSEQUENZEN DES USER-PROFILINGS FÜR VERBRAUCHERINNEN UND VERBRAUCHER

Artikel 13 des Deutschen Grundgesetzes postuliert die Unverletzlichkeit der Wohnung und so spricht das Bundesverfassungsgericht in mehreren Entscheidungen vom Recht des Einzelnen in seiner Wohnung "in Ruhe gelassen zu werden".[16] Dieses Recht wird durch die zunehmende Vernetzung des privaten Alltags jedoch immer stärker beschränkt. Unternehmen haben schon lange er-

[16] siehe u.a. BVerfGE 27, 1 - Mikrozensus; BVerfGE 51, 97 - Zwangsvollstreckung I

kannt, dass die Erhebung, Verarbeitung und Auswertung von Daten im Smart Home potentiell umfassende Rückschlüsse auf Lebensgewohnheiten, -umstände und Präferenzen zulässt. Wie diese datenbasierten Erkenntnisse über den einzelnen Nutzerinnen und Nutzer dann eingesetzt werden, scheint einzig vom jeweiligen Geschäftsmodell des Unternehmens abhängig zu sein. So können Smart Home-Geräte, wie Sprachassistenten, Smart TVs oder auch Internetrouter dafür genutzt werden, ein vollständigeres Nutzerprofil zu erstellen – gerade, wenn die erhobenen Daten durch weitere Datensätze seitens des Unternehmens angereichert werden (Crain, 2016).

Viele Datenschutz- und Nutzungsaspekte sind ähnlich, zu denen von und bei Online-Diensten. Gleichzeitig führen bestimmte Charakteristika des Smart Home dazu, dass bestimmte Daten bzw. deren Auswertung und der Umstand ihrer Erhebung besondere Beachtung erfahren sollten (Jacobsson et al., 2016). Im Folgenden werden drei zentrale Gefahren des User-Profilings in Smart Homes beleuchtet:

### 5.3.1 INTRANSPARENZ UND MANIPULATION

Bei Sprachassistenten und vernetztem Spielzeug, mit dem sich Kinder unterhalten können, ist es für die Nutzerinnen und Nutzer bisher nicht erkennbar, woher das Wissen und die Erkenntnisse stammen, die durch die Geräte wiedergegeben werden. So sorgt Amazons Alexa immer wieder für mediales Aufsehen, aufgrund von Antworten die der Sprachassistent gibt (Kühl, 2018). Einige rechtskonservative US Amerikaner beschweren sich, dass Alexa "links-liberales und feministisches Gedankengut" verteile, da es die Black Lives Matter-Bewegung und Feminismus unterstütze (Sist, 2017). Letztlich zeigen die bisherigen Ereignisse, dass bei sprachbasierten Smart Home-Anwendungen die Quelle der Informationen wesentlich schwieriger nachzuvollziehen ist, als bei Online-Diensten. Welche Antworten ein Sprachassistent auf gesellschaftlich kontrovers diskutierte Themen gibt, entscheidet derzeit nur der Hersteller.

Durch das fehlende Display bei Sprachassistenten kommen Suchergebnissen ebenso eine stärkere Bedeutung zu. So scheint Amazon in verschiedenen Produktsparten strategische Partnerschaften mit Herstellern einzugehen, um deren Produkte zu platzieren. Wird Alexa (zumindest in den USA) beauftragt, Zahnpasta zu kaufen, erwidert der Sprachassistent: *"Okay, I can look for a brand, like Colgate. What would you like?"* (Hirsch & Castillo, 2018). Dass Colgate vorgeschlagen wird, liegt an einer Partnerschaft zwischen Amazon und dem Zahnpastahersteller. Dieses Ergebnis könnte unter Umständen zukünftig durch persönliche Präferenzen oder Bewertungen auf Amazon.com beeinflusst werden – nichtsdestotrotz verschleiert es jedoch den Nutzerinnen und Nutzer, dass hinter dem Vorschlag eine Geschäftsbeziehung steht.

Diese Intransparenzen über Geschäftsbeziehungen, Informationen und Einflussnahme auf die Nutzerinnen und Nutzer sind nicht neu, jedoch gewinnen sie im Smart Home an Bedeutung. Wenn ein Smart Home-Gerät eine Information präsentiert, etwas erklärt oder einen Vorschlag macht, werden sich Nutzerinnen und Nutzer zukünftig daran gewöhnen müssen, dieses Verhalten zu hinterfragen und es nicht als "neutrale" oder "objektive" Information wahrzunehmen – ganz ähnlich zum heutigen Konsum von Informationen auf Websites und sozialen Netzwerken. Findet dies nicht statt, wird es Herstellern von Smart Home-Anwendungen leichter fallen, Nutzerinnen und Nutzer zu beeinflussen.

### 5.3.2 STAATLICHE ZUGRIFFSMÖGLICHKEITEN

Derzeit spielen **Sprachassistenten** eine zentrale Rolle in Smart Homes, da Nutzerinnen und Nutzer durch sie viele andere vernetzte Geräte zentral steuern können. (Lautsprecher, Thermostat, Licht, Steckdosen, etc.) Daher kommt ihnen hinsichtlich Datenschutz und Datenerhebung eine besondere Bedeutung zu. So forderte 2017 in Arkansas, USA die Staatsanwaltschaft Amazon auf, Daten eines bestimmten Amazon Alexa Accounts freizugeben, um bei der Aufklärung eines vermeintlichen Mordfalls zu helfen (Dywer, 2017). Amazon hatte sich gegen die Anfrage gewehrt, die Daten nicht herausgegeben und einige Monate später wurde die Mordanklage fallengelassen. Selbst, wenn Sprachassistenten das gesprochene Wort nur nach bestimmten Befehlen aufnehmen ("OK, Google" oder "Alexa"), zeigt es doch, wie tief Sprachassistenten Einblicke in Lebensumstände der Nutzerinnen und Nutzer erlauben.

Ähnlich zu Sprachassistenten könnten Strafverfolgungsbehörden auch Zugriff auf Videos von privaten **Überwachungskameras** in Smart Homes verlangen (O'Toole, 2014). Da die meisten vernetzten Überwachungskameras den Videostream für eine bestimmte Zeit in der Cloud des Anbieters bzw. Betreibers speichern, wäre es für Strafverfolgungsbehörden ohne Probleme möglich, diese Daten anzufragen. Je nach Jurisdiktion mit unterschiedlichen erforderlichen Nachweisen bzw. Beschlüssen. Einerseits bedeutet es, dass Straftaten wie Diebstahl oder Einbruch in Smart Homes leichter aufgeklärt werden können. Andererseits besteht erhöhtes Potential der "Selbstbelastung", aufgrund unzähliger Datenspuren, die im Smart Home hinterlassen werden (Berkman Center for Internet & Society at Harvard University, 2016).

### 5.3.3 KOMPLEXITÄT DES SMART HOMES

Bei Online-Diensten und Apps definiert der Hersteller bzw. Betreiber den "Raum" in dem sich der Nutzer bewegt. Facebook definiert, was und wie man auf der Plattform interagieren kann. Im Fokus liegt daher immer lediglich die Aktivität der Nutzerinnen und Nutzer. Eine Smart Home-Anwendung muss jedoch zunächst seine Umgebung verstehen: Ein Saugroboter erkundet immer mehr Winkel der Wohnung. Ein Sprachassistent muss zwischen verschiedenen Stimmen unterscheiden. Eine Überwachungskamera erkennt Objekte und Personen. Statt auf dem Individuum liegt bei Smart Home-Anwendungen der Fokus auf der Umgebung – dem Zuhause. Dies birgt jedoch viele Herausforderungen hinsichtlich User-Profiling, Datenschutz und Schutz der Privatsphäre Dritter:

- Opfer häuslicher Gewalt könnten durch Smart Home-Anwendungen, wie Überwachungskameras oder Sprachassistenten ungewollt stärker kontrolliert und unterdrückt werden. Diese Fragestellungen werden jedoch erst jetzt wissenschaftlich untersucht (Tanczer et al., 2018).
- Ebenso fallen Gäste oder unbeteiligte Dritte, unter Umständen unfreiwillig, unter die Datenanalyse des Smart Homes. Im Expertenworkshop wurde ausgiebig über die potenziellen Gefahren hinsichtlich Datenerhebung und -analyse von Dritten und Schutzbedürftigen diskutiert. Laut Expertinnen und Experten des Workshops hat dies nicht nur Auswirkungen auf die jeweiligen Persönlichkeitsrechte. Darüber hinaus entstehen auch Herausforderungen für die Datenanalyse an sich, da die Geräte in der Lage sein müssen, unterschiedliche Personen zu unterscheiden bzw. auseinander zu halten.

## 5.4 ZUSAMMENFASSUNG

User-Profiling durch Smart Home-Anwendungen geschieht derzeit punktuell und für die unterschiedlichsten Zwecke. Hinsichtlich Umfang, Häufigkeit und Marktdominanz ist es keineswegs vergleichbar mit gängigem User-Profiling durch Online Dienste und Apps. Dies liegt unter anderem daran, dass sich bisher weder dominante Smart Home-Plattformen, noch dominante Smart Home-Data Broker etabliert haben. Dies kann sich jedoch in den kommenden Jahren durch ein Anwachsen des Smart Home-Marktes durchaus ändern. Wie die verschiedenen Fallbeispiele verdeutlichen, lassen sich schon heute Gefahren für die Privatsphäre der Nutzerinnen und Nutzer ablesen: User-Profiling im Smart Home ist potenziell tiefgreifender, intransparenter und weniger kontrollierbar durch Nutzerinnen und Nutzer sowie Dritte. Unter anderem ist noch ungeklärt, inwieweit unbeteiligte Dritte (Gäste, Dienstleister, etc.) und Kinder unter diese Art der Datenerfassung und -auswertung fallen dürfen.

# 6 SICHERHEITSRISIKEN

Ziel dieses Kapitels ist es zunächst, die derzeitigen Sicherheitsrisiken zu beleuchten, die der Einsatz heutiger Smart Home-Geräte mit sich bringt. Hierbei werden die ausgewählten Anwendungs-Hot-Spots genauer analysiert, konkrete Gefahren beschrieben und Ursachen für den Mangel an Sicherheit in Smart Home-Anwendungen identifiziert.

## 6.1 RELEVANTE SICHERHEITSRISIKEN UND BEISPIELE

Indem Geräte und Maschinen mit dem Internet verbunden werden, sind sie automatisch allen potentiellen Angriffen aus dem Internet ausgesetzt. Das Smart Home ermöglicht es Angreifern durch Manipulation von Daten direkte physische Auswirkungen zu erzielen: Durch das Hacken eines smarten Türschlosses können Hausbewohnerinnen und -bewohner ein- oder ausgesperrt werden. Durch das kompromittieren eines vernetzten Herdes könnte eine Überhitzung provoziert werden, die einen Brand auslöst. Im Smart Home verbindet sich daher IT-Sicherheit *(Security)* mit physischer Sicherheit *(Safety)*, wodurch neue Sicherheitsrisiken entstehen.

Dies stellt auch Gerätehersteller vor neue Herausforderungen, da nicht mehr nur die physische Sicherheit eines Produkts, sondern auch dessen IT-Sicherheit bei der Entwicklung beachtet werden muss. Gerade bei Smart Home-Produkten geschieht dies jedoch regelmäßig nicht, da sowohl kriminelle Hacker als auch unabhängige Sicherheitsforscher immer wieder eklatante Sicherheitslücken und grundsätzliche Fehler bei der Softwareentwicklung in Smart Home-Produkten finden (Consumers International, 2017). Im Folgenden werden einige Fälle gezeigt, in denen Smart Home-Anwendungen erfolgreich kompromittiert wurden. Der Fokus liegt hierbei vor allem auf den Produktgruppen Kameras (Baby-Monitore, Überwachungskameras, Webcams), vernetzte Beleuchtung und Sprachassistenten.

Smarte Baby-Monitore: Für Eltern ist es sehr komfortabel, den Video-Stream des Baby-Monitors auf dem Handy ansehen zu können. So haben in den letzten Jahren immer mehr Hersteller internetfähige Baby-Monitore angeboten. Technisch bedeutet dies jedoch, dass der Baby-Monitor über das Internet ansprechbar sein muss und dadurch auch potentiell angreifbar ist. Untersuchungen haben gezeigt, dass auch hier einige Hersteller wenig Wert auf sichere Softwareentwicklung gelegt haben und Grundkonzepte der IT-Sicherheit nicht befolgt wurden (Stanislav & Beardsley, 2015). Dies hat zur Folge, dass es bei betroffenen Baby-Monitoren verhältnismäßig leicht für Fremde ist, diese über IoT-Suchmaschinen, wie Shodan (2018), aufzufinden und unberechtigt Zugang zum Videostream und damit dem Kinderzimmer zu erlangen (Porup, 2016). In den letzten Jahren gab es immer wieder Berichte von Eltern, die nachts eine Stimme aus dem Kinderzimmer gehört haben, ins Zimmer liefen und realisierten, dass eine fremde Männerstimme über den gehackten Baby-Monitor zum Baby sprach (Silverman, 2015).

Überwachungskameras: Ähnlich zu Baby-Monitoren sind auch immer mehr klassische Überwachungskameras aus Komfortgründen mit dem Internet verbunden – entweder direkt oder über einen digitalen Videorekorder (DVR). Ebenso, wie bei den Baby-Monitoren, sind auch die digitalen Überwachungskameras einiger Hersteller ungenügend abgesichert und verhältnismäßig leicht durch Dritte zu kompromittieren. Wie bei den Baby-Monitoren stellt dies zunächst ein direktes Risiko für die Privatsphäre der Nutzerinnen und Nutzer dar. Jedoch hat sich in den letzten Jahren gezeigt, dass solche ungesicherten Überwachungskameras und DVRs vor allem für *Botnetze* genutzt werden:

Kriminelle Hacker schreiben Schadsoftware, die sich selbstständig verbreitet, indem sie bekannte Schwachstellen oder Standard-Login-Daten bestimmter IoT-Geräten ausnutzt, sich auf den Geräten installiert und dann das Internet nach weiteren unsicheren Geräten selbstständig durchsucht. Sobald sich die Schadsoftware erfolgreich auf dem Gerät installiert hat, erlangt der Kriminelle vollständige Kontrolle über das Gerät. Für einen kriminellen Hacker stellt ein IoT-Botnetz letztlich kostenlose, weltweit verteilte Rechenkraft und Bandbreite dar. Botnetze wurden in der Vergangenheit benutzt, um Webseiten und Server lahmzulegen, für Click-Fraud (massenhaftes, automatisiertes Anklicken von Werbung, um Provision zu erhalten) oder als Miner von Cryptowährungen (Hallman et al., 2017). Ein Angriff eines solchen Botnetzes aus mehreren Hunderttausend kompromittierten Überwachungskameras und DVRs führte im Herbst 2016 zum zeitweisen Ausfall mehrerer Internetdienste wie Twitter, Soundcloud oder Netflix an der US-Ostküste (Antonakakis et al., 2017). Botnetze und deren Angriffe zeigen daher eindringlich die Drittbetroffenheit durch unsichere IoT-Geräte: Die Nutzerinnen und Nutzer merken meist gar nicht, dass ihre Kamera oder DVR Teil eines globalen Botnetzes ist und Angriffe durchführt. Den Schaden tragen daher andere. Durch die fehlende Betroffenheit der Smart Home-Nutzerinnen und -Nutzer mangelt es ebenso an Anreizen, sich um die Sicherheit des Smart Home-Gerätes zu kümmern.

Webcams: Laptops und PCs gehören weder zum Internet der Dinge noch zu Smart Home-Anwendungen. Jedoch lässt sich anhand der *Sextortion*-Fälle (Wortschöpfung aus *Sex* und *Extortion*, engl. Erpressung) der letzten Jahre ein zunehmendes Risiko im Smart Home erkennen. Vor mehr als zehn Jahren wurden die ersten Fälle öffentlich, in denen Männer die Computer von jungen Frauen und Mädchen gehackt haben, um über deren Webcams fortan unbemerkt Bilder und Videos aufzunehmen (Wittes et al., 2016). Diese Bilder und Videos, in denen die Frauen und Teenager meist wenig oder gar nicht bekleidet waren, wurden dann genutzt, um die Opfer zu erpressen: Sie mussten auf Befehl den Männern mehr Bildmaterial liefern oder Geld zahlen, sonst würden diese die Bilder und Videos veröffentlichen. Populärstes Opfer war 2013 Cassidy Wolf, die damalige Miss Teen USA Gewinnerin. Wolf wurde über Monate auf diese Weise von einem Klassenkameraden erpresst. Gerade in Smart Homes wird diese Art der Erpressung leichter sein, da schlichtweg mehr Kameras direkt mit dem Internet verbunden sein werden (Yacoob et al., 2017).

Vernetzte Beleuchtung: Viele Hersteller von vernetzter Beleuchtung setzen auf das *ZigBee Light Link*-Protokoll zur Kommunikation zwischen Lampen und Basisstation (Zigbee, 2018). Es wurde jedoch gezeigt, dass schon im Protokoll selbst unzureichend auf Sicherheit geachtet wurde (Morgner & Beneson, im Erscheinen). Weiterhin war es Sicherheitsforschern immer wieder möglich, vernetzte Beleuchtung verschiedenster Hersteller zu kompromittieren: Sicherheitsforscher aus Israel und Kanada entwickelten Schadsoftware, die sich selbstständig über eine Schwachstelle im *ZigBee Light Link*-Protokoll von LED-Leuchte zu LED-Leuchte verbreitete. Für die Erstinfektion mussten die Sicherheitsforscher nicht mal ins Gebäude, sondern es genügte mit einer Drohne am Haus vorbei zu fliegen (Ronen et al., 2017). Sobald sich der Wurm von LED-Leuchte zu LED-Leuchte vermehrt hatte, standen diese unter der vollständigen Kontrolle des Angreifers und konnten sogar permanent zerstört werden. Auch, wenn das Hacken von LED-Leuchten auf den ersten Blick nicht sonderlich gefährlich wirkt, birgt es doch konkrete Gefahren: Angreifer könnten die Leuchten so schnell flackern lassen, dass ein Stroboskop-Effekt entsteht, der bei Menschen, die unter Epilepsie leiden, zu epileptischen Anfällen führen kann (Ronen & Shamir, 2016). Die Angriffe auf vernetzte Beleuchtung zeigen exemplarisch das derzeitige Dilemma vieler günstiger Smart Home-Anwendungen: Um eine schnelle Marktdurchdringung zu erreichen, entwickeln Konsortien (meist bestehend aus Unternehmen) technische Standards, wie beispielsweise ZigBee Light Link, mit einem starken Fokus auf Kom-

patibilität und Komfort statt auf Sicherheit. Bei der Entwicklung eines Massenprodukts, wie der LED-Leuchte wird dann ebenso wenig auf Sicherheit geachtet.

Sprachassistent: Anders als bei vernetzten Kameras oder smarter Beleuchtung kommen die meisten Sprachassistenten von wenigen Herstellern (bisher vor allem Amazon Echo, Google Home und Apple HomePod), die Hard- und Software des Gerätes herstellen und pflegen. Hinsichtlich IT-Sicherheit ist das ein wichtiger Unterschied: Während bei vielen anderen Smart Home-Anwendungen Gerätehersteller und Betreiber unterschiedliche Unternehmen sind, ist dies bei Sprachassistenten bisher nicht der Fall. Dies bedeutet, dass Hersteller von Sprachassistenten potentiell deutlich schneller auf Sicherheitslücken reagieren können und Softwareupdates für die aktiven Geräte bereitgestellt werden. Viele andere Smart Home-Geräte, wie Kameras, Beleuchtung, Spielzeug oder Smart TVs werden von unterschiedlichen Betreibern unter unterschiedlichen Namen und Marken verkauft. Wenn der eigentliche Gerätehersteller (Original Equipment Manufacturer, OEM) nun ein Softwareupdate veröffentlicht, muss jeder Betreiber dies den eigenen Geräten zur Verfügung stellen. Dies führt in der Regel dazu, dass die Software von Smart Home-Geräten deutlich langsamer oder gar nicht aktualisiert wird.

Trotzdem gab es in der Vergangenheit auch bei Sprachassistenten Sicherheitslücken, die zum potentiellen Verlust von Privatsphäre führten: Sowohl Google Home als auch Amazon Echo waren von BlueBorne betroffen – einer Schwachstelle in der Bluetooth-Verbindung (Armis, 2018). Diese ermöglichte es Angreifern über Bluetooth, vollständige Kontrolle über den Sprachassistenten zu erlangen. Eine andere Schwachstelle in älteren Amazon Echo Versionen erlaubte es Angreifern, ebenso vollständige Kontrolle über das Gerät zu erlangen, allerdings musste hierfür das Gerät geöffnet und manipuliert werden.

## 6.2 URSACHEN FÜR SICHERHEITSRISIKEN

Die zuvor angeführten Fälle sollen aufzeigen, wie breit das Feld an Sicherheitsrisiken im Smart Home ist. Die eigene Wohnung ist durch das Grundgesetz (Art. 13) besonders geschützt, jedoch wird sie durch unsichere IoT-Geräte wesentlich verletzbarer. Im Folgenden werden einige der zentralen Aspekte aufgezeigt, weswegen es für Verbraucherinnen und Verbraucher derzeit kaum möglich ist, verhältnismäßig vertrauenswürdige und sichere Smart Home-Geräte zu kaufen:

Best Practices werden ignoriert: Bei vielen Smart Home-Anwendungen scheinen Hersteller während des Entwicklungsprozesses kaum auf Best Practices hinsichtlich IT-Sicherheit zu achten. So wiederholen sich Fehler, die im IT-Bereich seit vielen Jahren kaum noch vorkommen: fest vergebene Passwörter, undokumentierte Remote-Schnittstellen, unverschlüsselte Client-Server-Verbindungen und vieles mehr. Viele der zuvor genannten Fälle wären nicht passiert bzw. nicht möglich gewesen, wenn die Hersteller sich an wenige, grundsätzliche Security-by-Design Prinzipien gehalten hätten. Einer der Gründe, weswegen bei Smart Home-Geräten Best Practices nicht befolgt werden, ist mangelndes Wissen und mangelnde Ressourcen seitens des Herstellers. Statt Personal entsprechend zu schulen oder neue Stellen auszuschreiben, werden Softwarekomponenten möglichst schnell und kostengünstig mit einem Fokus auf Features statt auf Sicherheit implementiert. Ebenso fehlt es an Anreizen für die Hersteller Best Practices zu befolgen, da sie im Falle eines Schadens durch eine Sicherheitslücke meistens nicht für die Kosten aufkommen müssen. Das fehlende wirtschaftliche Haftungsrisiko wirkt sich so indirekt auf die Produktsicherheit aus.

Hersteller werden oft erst aktiv, wenn es zu spät ist: Weiterhin drängt sich der Verdacht auf, dass Hersteller oftmals erst aktiv werden, wenn sie durch Dritte auf Schwachstellen aufmerksam ge-

macht werden. Und selbst dann ist die Reaktion unter Umständen defensiv bis ignorant. So haben Hersteller von Smart Home-Anwendungen immer wieder keine klaren Kontaktadressen (und etablierte, interne Prozesse), an die sich Sicherheitsforscher wenden können, wenn sie eine Schwachstelle gefunden haben (Rapid7, 2016).

Mangel an Software-Updates: Selbst wenn Softwareupdates durch den Gerätehersteller zur Verfügung gestellt werden, bedeutet dies nicht, dass die Geräte auch direkt die neuste Softwareversion erhalten. Dies hat vorrangig zwei Gründe: (1) **Die Update-Mechanismen der Smart Home-Geräte sind meist wenig intuitiv und kaum benutzerfreundlich.** Voll-Automatische Updates, wie man es von aktuellen Desktop-Betriebssystemen (Windows, macOS, Linux) kennt, sind nicht der Standard. Bei vielen Internet-Routern muss man beispielsweise noch manuell auf der Webseite des Herstellers nach Updates für das entsprechende Modell suchen, diese herunterladen, sich auf dem Router anmelden, dort die Datei hochladen und dann das Update ausführen. Dadurch wird es nur von wenigen Nutzerinnen und Nutzern tatsächlich gemacht. Ähnliches gilt für vernetzte Überwachungskameras und einige vernetzte Glühbirnen. (2) **Smart Home-Geräte werden oft durch OEMs (Original Equipment Manufacturer, deutsch vergleichbar "Erstausrüster") hergestellt** und an mehrere Unternehmen weiterverkauft, die diese dann erst an Endkundinnen und -kunden verkaufen. Ein OEM stellt beispielsweise einen DVR her und ein Sicherheitsforscher findet gravierende Sicherheitslücken in dessen Software (KerneronSecurity, 2016). Der OEM hat dieses Modell an über 70 Unternehmen verkauft, die das Modell in teils leicht abgeänderter Form an Endkundinnen und -kunden verkaufen. Selbst wenn der OEM nun ein Softwareupdate zur Verfügung stellt, müssten alle 70 Unternehmen dieses weitergeben. Die derzeitige OEM-Struktur gerade im niedrigpreisigen Smart Home-Bereich macht es daher schwierig, zeitnah Softwareupdates an Geräte zu verteilen. Wie schwierig es ist, Softwareupdates in einer vielschichtigen OEM-Struktur zu den Endkundinnen und -kunden zu bringen, sieht man bei Android Smartphones (Android, 2018): Derzeit nutzen noch über 10% der Android Smartphones Android 4.4, das im Herbst 2013 veröffentlicht wurde. Knapp 20% der derzeit aktiven Android Smartphones nutzen noch Android 5.1, das im Frühjahr 2015 veröffentlicht wurde. Veraltete Software bedeutet immer, dass Sicherheitslücken nicht geschlossen werden und im Laufe der Zeit Angreifer immer mehr Möglichkeiten haben, das Gerät zu kompromittieren.

Eine neue Dimension stellt die **Drittbetroffenheit bei Angriffen von Botnetzen** dar. Für kriminelle Hacker werden IoT-Geräte im Smart Home immer interessanter, da deren Leistungsfähigkeit und die zur Verfügung stehende Internetanbindung stetig steigen. Wie am Beispiel der Überwachungskameras gezeigt wurde, nutzen kriminelle Hacker immer öfter Smart Home-Geräte, um Botnetze aus mehreren Hunderttausend Geräten zu erschaffen. Diese global verteilte Rechenkraft, steht ihnen dann für verschiedenste Angriffe, Erpressung oder Betrug zur Verfügung. Da Kriminelle ein Interesse daran haben, dass das Botnetz möglichst konstant wächst, richten sich die Angriffe eines Botnetzes nie gegen "sich selbst" – also Geräte, die selbst Teil des Botnetzes sind werden nie angegriffen, sondern immer externe Server oder Websites. Dadurch stellen Botnetze für die Nutzerinnen und Nutzer von unsicheren Smart Home-Geräten selbst keine Gefahr dar, da die Angriffe der Botnetze sich immer gegen unbeteiligte Dritte richten. Dadurch sinkt jedoch gleichzeitig der Anreiz der Nutzerinnen und Nutzer, in Sicherheit zu investieren, wenn sie selbst nicht die Leidtragenden sind.

## 6.3 ZUSAMMENFASSUNG

Zusammenfassend kann konstatiert werden, dass der Markt derzeit regelmäßig versagt, Verbraucherinnen und Verbrauchern, verhältnismäßig vertrauenswürdige Smart Home-Geräte zur Verfügung zu stellen. Es besteht eine starke Informationsasymmetrie zwischen Verbraucherinnen und Verbrau-

chern und Herstellern hinsichtlich der Sicherheit eines Smart Home-Gerätes. Zu essenziellen Fragen zur Häufigkeit von Sicherheitsupdates oder dem Ende des Supportzeitraums für ein bestimmtes Produkt erhalten Verbraucherinnen und Verbraucher derzeit keine verbindlichen, belastbaren Antworten. Weiterhin können Hersteller die Kosten, die durch eine Sicherheitslücke im Schadensfall entstehen, fast vollständig externalisieren. Dadurch besteht wenig Anreiz, schon bei der Entwicklung auf Security-by-Design und Best Practices zu achten. So ist es wenig verwunderlich, dass viele Smart Home-Geräte durch kriminelle Hacker voll-automatisiert und umfassend kompromittiert werden können.

# 7 PROBLEMSYNTHESE, LÖSUNGSANSÄTZE UND HANDLUNGSEMPFEHLUNGEN

Ziel dieses Kapitels ist es, die vorgestellten Ergebnisse zu kondensieren und in Handlungsempfehlungen zu überführen. Deshalb werden für die drei Hauptkapitel des Gutachtens – informationelle Selbstbestimmung, User-Profiling und Datensicherheit – im ersten Schritt die existierenden Probleme und Konflikte thematisiert. Diese ergeben sich aus den identifizierten Praxisbeispielen (Ist-Zustand) und der Diskrepanz zum Soll-Zustand, der sich aus technischen, datenschutzrechtlichen, verhaltenswissenschaftlichen und verbraucherpolitischen Vorgaben ableitet. Hiernach werden mögliche Lösungsansätze präsentiert, die entweder denkbar sind oder aber bereits Anwendung finden und in der politischen Debatte Aufmerksamkeit erhalten. Die Lösungsansätze werden im nächsten Schritt auf ihre Wirksamkeit geprüft und in Handlungsempfehlungen überführt. Darüber hinaus werden übergeordnete Problemfelder angeschnitten und in Handlungsempfehlungen überführt.

## 7.1 INFORMATIONELLE SELBSTBESTIMMUNG

Aus den Ergebnissen von Kapitel 4 können vier übergeordnete Problemfelder abgeleitet werden, die die Ausübung der informationellen Selbstbestimmung für Verbraucherinnen und Verbraucher erschweren. Hierzu gehören zum einen das Nicht-Einhalten gesetzlicher Vorgaben und die sogenannten DSE-inhärenten Faktoren, die in den Praxisbeispielen suboptimal ausgestaltet sind. Außerdem ist aus verhaltenswissenschaftlicher Perspektive der Zugang zu den Datenschutztexten ein sehr relevanter Problembereich und auch bezüglich der Verbrauchermotivation und -bildung existieren Lücken. Im Folgenden werden die Problemfelder vorgestellt und zugehörige Lösungsansätze analysiert und bewertet.

### 7.1.1 RECHTLICHE VORGABEN KONSEQUENT DURCHSETZEN

Aus der Analyse in Kapitel 4 folgt, dass notwendige Rahmenbedingungen erfüllt sein müssen, damit Nutzerinnen und Nutzer sich über Datenverarbeitungen informieren können. Hierzu gehört insbesondere, dass eine Datenschutzerklärung vorhanden ist, dass sie in deutscher Sprache vorliegt und dass Kontaktmöglichkeiten für datenschutzrechtliche Anliegen vorhanden sind.

Die Auswertungsergebnisse der Datenschutzpraktiken ausgewählter Anbieter in Kapitel 4 haben jedoch gezeigt, dass in diesem Bereich Nachholbedarf existiert. Diese Ergebnisse werden auch durch eine Auswertung von Consumers International (2017, S. 10) bekräftigt. Die Autoren stellten hier fest, dass 59% der von ihnen getesteten IoT-Geräte nicht ordnungsgemäß über Datenverarbeitungen aufklären.

Über diese Verstöße hinaus existieren weitere Gestaltungsmöglichkeiten in der im Mai 2018 in Kraft tretenden DSGVO, die die Datenschutzsituation der Verbraucherinnen und Verbraucher verbessern könnten. Privacy by design und default, das Marktortprinzip sowie Einwilligungsanforderungen sollten deshalb ebenfalls konsequent durchgesetzt werden.

Damit diese rechtlichen Vorgaben umgesetzt werden, wurden in der DSGVO empfindliche Strafen für Verstöße verankert (Art. 83 und 84). So beträgt die maximale Geldbuße 20 Millionen Euro oder bis zu 4% des letztjährigen Jahresumsatzes.

**Wirksamkeit**

Den negativen, monetären Anreizen wurden im Expertenworkshop eine wichtige Rolle beigemessen, um die Rechtsdurchsetzung zu effektivieren. Jedoch liegen noch keine Informationen aus der Praxis vor, da die DSGVO erst im Mai 2018 in Kraft tritt. Einen Anhaltspunkt aus einem anderen Bereich könnte jedoch das Wettbewerbsrecht liefern, das über empfindliche Strafen erfolgreich Verstöße ahndet und vermeidet. Insgesamt ist die Wirksamkeit auch von der Ausstattung der verantwortlichen Behörden oder Verbraucherorganisationen abhängig. Je besser diese ausgestattet sind, desto erfolgreicher werden die Rechte von Verbraucherinnen und Verbrauchern auch durchgesetzt.

Aus diesen Ergebnisse ergibt sich die erste Handlungsempfehlung:

Handlungsempfehlung 1: Es bedarf einer konsequenten Rechtsdurchsetzung durch Behörden und Verbraucherorganisationen, um gesetzeswidrige Datenschutzpraktiken zu ahnden und auf Missstände hinzuweisen. Die neuen schärferen Sanktionsmöglichkeiten, die aus der Datenschutzgrundverordnung resultieren, sollten konsequent angewendet werden.

### 7.1.2 VERBESSERUNG DER INFORMIERTHEIT DURCH ÜBERWINDUNG DSE-INHÄRENTER HÜRDEN

Die bereits zitierte Befragung des DIVSI (2015) zeigt, dass sich Verbraucherinnen und Verbraucher gerade im Bereich der Länge, sprachlichen Komplexität und Gestaltung Verbesserungen für die Datenschutztexte wünschen. So geben knapp 71% der Befragten an, dass sie Informationstexten bereitwilliger zustimmen würden, wenn diese „besser und leichter verständlich aufbereitet“ wären (S. 28). Die Auswertung der derzeitigen Datenschutztexte in Kapitel 4 zeigt jedoch, dass die analysierten Datenschutztexte für Smart Home-Anwendungen hinter diesen Erwartungen zurückbleiben. So sind die Texte sehr lang und komplex und bis auf wenige Ausnahmen werden gestalterische Elemente nicht eingesetzt.

Die Befragung der Marktwächter Digitale Welt (2017) liefert Anhaltspunkte, wie diesen Verbraucherwünschen konkret begegnet werden könnte (S. 41). Zwar bezieht sich die Befragung auf Datenschutztexte von Bezahldienstleistern im Internet, jedoch treten auch hier, wie beim Smart Home, ähnliche Hürden bezüglich Textlänge und Komplexität auf. Gefragt nach Lösungsansätzen geben 36% der Befragten an, dass eine **einseitige Darstellung** mit „konkreter Auflistung“ am besten geeignet sei, Informationen zu transportieren. Hinzu kommt mit 13% die einseitige Darstellung mit „bildlichen Darstellungen“. 23% der Befragten geben außerdem an, dass **Siegel** von einer unabhängigen Stelle für sie am besten geeignet seien. 19% geben an, dass **interaktive Datenschutztexte**, d.h. erst kurz und dann detailliert, am besten geeignet seien, Verbraucherinnen und Verbraucher zu informieren.

Im Folgenden werden Datenschutzsiegel, einseitige Datenschutztexte, sogenannte One-Pager und interaktive Datenschutztexte vorgestellt und bewertet.

## DATENSCHUTZSIEGEL

Datenschutzsiegel stellen in kompakter Form dar, ob die Datenschutzpraktiken eines Anbieters einer bestimmten, vordefinierten Anforderungsliste entsprechen. Siegel werden etwa vom Unabhängigen Landesdatenschutzzentrum Schleswig-Holstein (2014), der TÜV IT (2006) sowie der Gesellschaft für transparenten Datenschutz (2018) angeboten. Abbildung 5 zeigt das Siegel der Gesellschaft für transparenten Datenschutz (2018).

Abbildung 5: Beispiel - Datenschutzsiegel

(Gesellschaft für transparenten Datenschutz, 2018)

**Wirksamkeit**

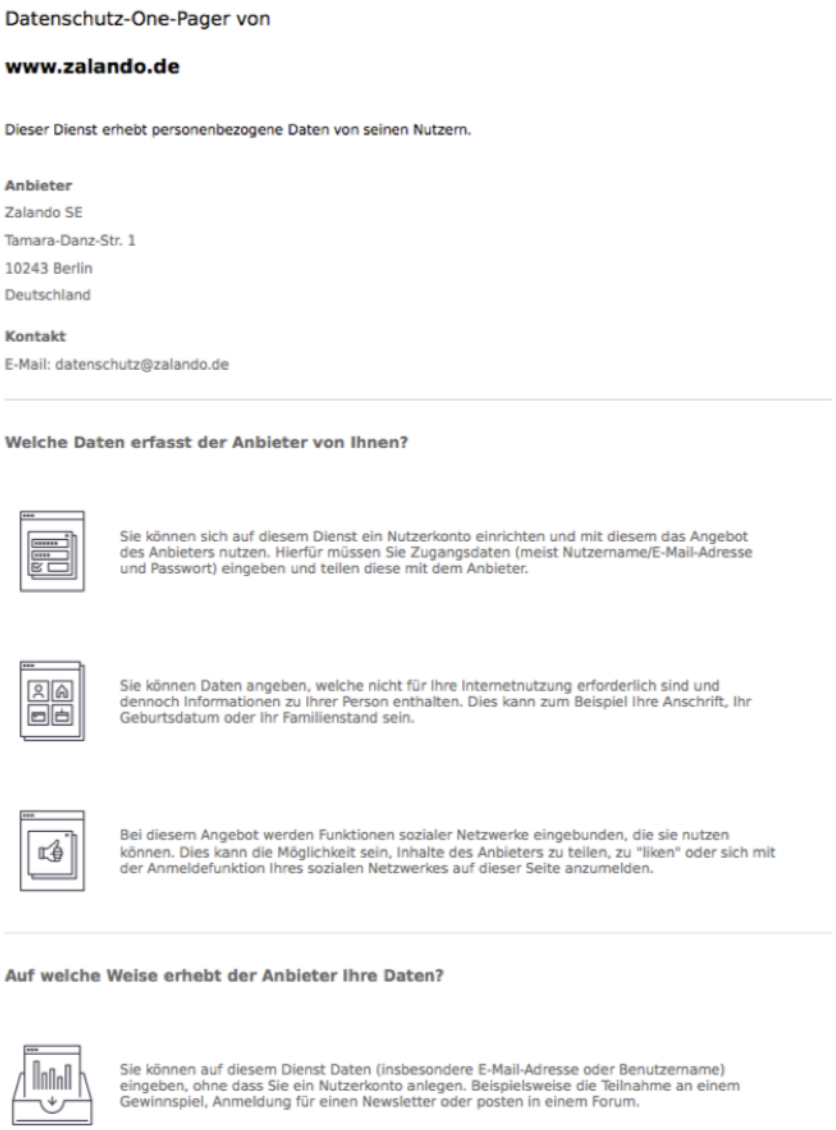
Vorteile von Datenschutzsiegeln sind, dass Verbraucherinnen und Verbraucher sich innerhalb kürzester Zeit über das Einhalten von definierten Datenschutzpraktiken informieren können. Dies erspart im besten Fall Lesezeit und reduziert so die Informationskosten. Jedoch ist die Wirksamkeit abhängig vom Anforderungskatalog und der Qualität des Siegels und so fällt es Verbraucherinnen und Verbrauchern oftmals schwer, die Aussagen eines Siegels vollständig zu überblicken. Im Expertenworkshop wurden ebenfalls Bedenken bezügliche der Signalwirkung von Siegeln geäußert. So suggerieren Siegel oftmals Schutz, können aber auch kontraproduktiv wirken. In einer verhaltenswissenschaftlichen Studie werden diese Bedenken bekräftigt. So finden die Autoren, dass beispielsweise Siegel, die lediglich über die Vollständigkeit der Datenschutztexte informieren sollen, von Verbraucherinnen und Verbrauchern fälschlicherweise als datensparsam interpretiert werden (Rifon, LaRose und Choi, 2005).

## ONE-PAGER-ANSATZ

Der One-Pager-Ansatz basiert auf den Ergebnissen einer Arbeitsgruppe zum Nationalen IT-Gipfel-Prozess 2015, die auf Initiative des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) initiiert wurde. Teil der Arbeitsgruppe waren neben politischen Vertretern auch Vertreter der Wissenschaft, Wirtschaft und Gesellschaft. Ziel des One-Pager-Ansatzes ist es, wie der Name bereits zeigt, die ausführliche Datenschutzerklärung auf einer DIN-A4-Seite zusammenzufassen und Verbraucherinnen und Verbrauchern zu ermöglichen, sich kompakt und in kurzer Zeit über die relevanten Datenverarbeitungen zu informieren. Der One-Pager komplementiert hierbei die ausführliche Datenschutzerklärung – ersetzt sie jedoch nicht. In der Praxis haben drei Unternehmen einen

One-Pager auf ihrer Webseite integriert (vgl. Deutsche Telekom AG, 2016, Otto GmbH & Co. KG, 2017, sowie Zalando SE, 2016). Ein Beispiel für einen One-Pager, der sich auch bildlichen Darstellungen bedient, ist in Abbildung 6 dargestellt.

Abbildung 6: Beispiel - One-Pager



Datenschutz-One-Pager von

**www.zalando.de**

Dieser Dienst erhebt personenbezogene Daten von seinen Nutzern.

**Anbieter**
Zalando SE
Tamara-Danz-Str. 1
10243 Berlin
Deutschland

**Kontakt**
E-Mail: datenschutz@zalando.de

**Welche Daten erfasst der Anbieter von Ihnen?**

Sie können sich auf diesem Dienst ein Nutzerkonto einrichten und mit diesem das Angebot des Anbieters nutzen. Hierfür müssen Sie Zugangsdaten (meist Nutzername/E-Mail-Adresse und Passwort) eingeben und teilen diese mit dem Anbieter.

Sie können Daten angeben, welche nicht für Ihre Internetnutzung erforderlich sind und dennoch Informationen zu Ihrer Person enthalten. Dies kann zum Beispiel Ihre Anschrift, Ihr Geburtsdatum oder Ihr Familienstand sein.

Bei diesem Angebot werden Funktionen sozialer Netzwerke eingebunden, die sie nutzen können. Dies kann die Möglichkeit sein, Inhalte des Anbieters zu teilen, zu "liken" oder sich mit der Anmeldefunktion Ihres sozialen Netzwerkes auf dieser Seite anzumelden.

**Auf welche Weise erhebt der Anbieter Ihre Daten?**

Sie können auf diesem Dienst Daten (insbesondere E-Mail-Adresse oder Benutzername) eingeben, ohne dass Sie ein Nutzerkonto anlegen. Beispielsweise die Teilnahme an einem Gewinnspiel, Anmeldung für einen Newsletter oder posten in einem Forum.

(Zalando SE, 2016)

## Wirksamkeit

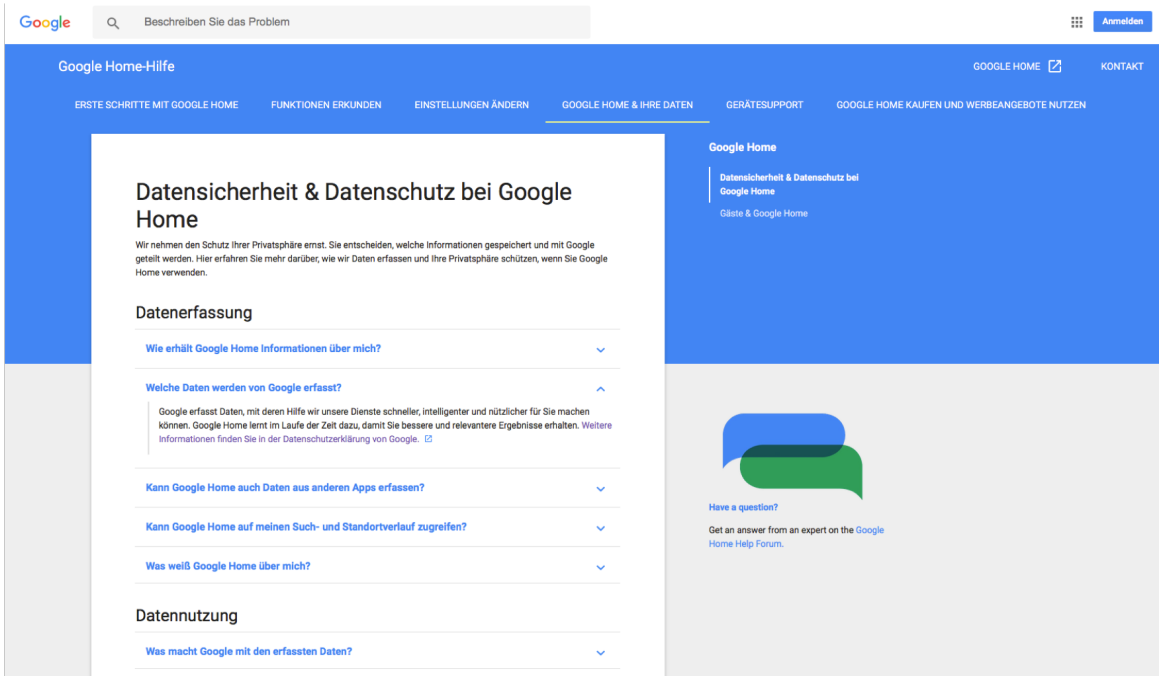
Der One-Pager reduziert die Textmenge und somit auch die Informationskosten für Verbraucherinnen und Verbraucher. Jedoch konnte in einem Online- und Feldexperiment nicht bestätigt werden, dass der One-Pager die Informiertheit der Verbraucherinnen und Verbraucher signifikant verbessert (Kettner et al., 2018). Denn auch wenn der One-Pager Faktoren wie Länge, Komplexität und Gestaltung verbessert, so erhöht er nicht den Zugang zu den Datenschutztexten, denn dieser wird durch

die Anbieter geregelt und so werden in der Praxis Datenschutzerklärungen häufig hinter einem Link „versteckt“.

## INTERAKTIVE DATENSCHUTZERKLÄRUNGEN

Interaktive Datenschutztexte ermöglichen durch aufklappbare Menüs oder Drill-Down-Funktionen, dass Verbraucherinnen und Verbraucher sich zuerst oberflächlich informieren können und hiernach gezielt an den Stellen, die besonders relevant für sie sind, mehr Details erfahren. Bei den Smart Home-Anbietern gibt es beispielsweise Google Home, das eine interaktive Informationsmöglichkeit bietet (vgl. Abbildung 7).

Abbildung 7: Beispiel - Interaktive Datenschutzerklärung




(Google, 2018)

### Wirksamkeit

Auch durch diese Herangehensweise werden Informationskosten reduziert. Denn Verbraucherinnen und Verbrauchern können bei den Textstellen, die für sie relevant sind, mehr Zeit investieren und diese bei uninteressanten Datenverarbeitungen einsparen. Durch die aktivierenden Elemente ist es außerdem möglich, die Motivation der Verbraucherinnen und Verbraucher zu steigern. Jedoch liegen zur Wirksamkeit wenig Belege vor. In der Feldstudie von Kettner et al. (2018) wurde ein interaktiver One-Pager zwar getestet, aufgrund der geringen Fallzahlen konnte jedoch nicht abschließend bewertet werden, inwieweit eine Aktivierung der Verbraucherinnen und Verbraucher tatsächlich stattfindet.

### 7.1.3 ZUGANG ZUR DATENSCHUTZERKLÄRUNG VERBESSERN

Neben der Länge, Komplexität der verwendeten Sprache und Gestaltung der Datenschutztexte spielte in der Analyse der Smart Home-Anwendungen auch die Zugänglichkeit eine Rolle. In der Praxis befinden sich die meisten Datenschutztexte hinter Links und so müssen Verbraucherinnen und Verbraucher diese „Klick-Barriere" erst überwinden, um sich informieren zu können. Die bereits genannten Siegel könnten diese Hürde überwinden, indem sie standardmäßig beim Kauf von Smart Home-Anwendungen angezeigt werden. Eine weitere Möglichkeit, es Verbraucherinnen und Verbrauchern einfach zu machen, sind die sogenannten Privacy Bots.

#### PRIVACY BOTS

Privacy Bots sind technische Lösungen, die Datenschutztexte automatisch und in standardisierter Form aufbereiten. Zusätzlich ermöglichen Privacy Bots den Abgleich der Datenschutztexte mit den persönlichen Präferenzen der Nutzerinnen und Nutzer. Verschiedene Privacy Bots werden auch in den Studien der Stiftung Datenschutz (2017) und Kettner et al. (2018) vorgestellt. Speziell für das Smart Home wurden bisher keine Bots veröffentlicht, jedoch ist die Übertragbarkeit bestehender Bots technisch denkbar.

**Wirksamkeit**

Der Vorteil der Privacy Bots liegt darin, dass Präferenzen von Verbraucherinnen und Verbrauchern mit den tatsächlichen Datenverarbeitungen abgeglichen werden und so automatisch geprüft wird, ob Nutzerinnen und Nutzer die entsprechenden Anwendungen nutzen sollten. Im Gegensatz dazu ist bei Siegeln lediglich eine Pauschalbewertung nach externen Vorgaben möglich.

Die persönlich zugeschnittene Auswertung minimiert überdies die Informationskosten für Verbraucherinnen und Verbraucher und die Zugänglichkeit zu den Datenschutztexten wird erhöht. Denn während bei anderen Vereinfachungsmethoden, wie dem One-Pager, die Datenschutzerklärung immer noch selbst durch Verbraucherinnen und Verbraucher gesucht werden muss, übernimmt der Privacy Bot diese Suche und spart hierdurch zusätzlich Kosten.

Es existieren jedoch auch Nachteile bei der Nutzung von Privacy Bots. So müssen Verbraucherinnen und Verbraucher initiativ ein solches Tool herunterladen und installieren und ihre Präferenzen hinterlegen, damit die Bots überhaupt genutzt werden können.

Aus den Ergebnissen folgt die zweite Handlungsempfehlung.

Handlungsempfehlung 2: Um die Komplexität zu reduzieren und den Zugang zu Datenschutzerklärungen zu erleichtern, sind Tools für Verbraucherinnen und Verbraucher hilfreich. Hierzu zählen insbesondere Privacy Bots, die den Verbraucherinnen und Verbrauchern mehr Selbstbestimmtheit und Kontrolle ermöglichen können. Die Entwicklung solcher Technologien sollte gefördert werden.

### 7.1.4 DATENMANAGEMENT DURCH PLATTFORMEN ERMÖGLICHEN

In Kapitel 3 wurde gezeigt, dass Plattformen, als Bindeglied zwischen unterschiedlichen Anwendungen im vernetzten Zuhause, in Zukunft eine besondere Rolle spielen werden. Diese übergeordnete Stellung könnte auch genutzt werden, um Verbraucherinnen und Verbrauchern technisch die Ausübung ihrer informationellen Selbstbestimmung zu erleichtern. Der Sachverständigenrat für Verbraucherfragen (2017) empfiehlt beispielsweise ein verbraucherzentriertes Datenportal (S. 8), das nicht nur Transparenz schaffen, sondern auch die Ausübung der Verbraucherrechte erleichtern soll.

**Wirksamkeit**

Zur Wirksamkeit von Datenportalen liegen derzeit keine empirischen Ergebnisse vor. Jedoch ist der Ansatz eines Datenportals aufgrund der Stellung der Plattformen vielversprechend.

Aus den Ergebnissen folgt Handlungsempfehlung 3.

Handlungsempfehlung 3: Intermediäre wie Smart Home-Plattformen oder Steuerungseinheiten sollten beim Datenschutz mehr in den Fokus genommen werden. So könnten diese beispielsweise das Gesamtrechtemanagement aller über die Plattform gesteuerten Smart Home-Anwendungen übernehmen. Auf diese Weise könnten die Privatsphärepräferenzen aller sich im Smart Home befindlichen Anwendungen effektiv gesteuert werden.

### 7.1.5 VERBRAUCHERMOTIVATION UND VERBRAUCHERBILDUNG STÄRKEN

In Abschnitt 4.4 wurde beschrieben, dass neben DSE-inhärenten Faktoren auch motivationale und kognitive Aspekte eine bedeutende Rolle beim Umgang von Verbraucherinnen und Verbrauchern mit ihren Daten spielen. Im Expertenworkshop wurde dieser Umstand ebenfalls hervorgehoben und auf die Problematik hingewiesen, dass Verbraucherinnen und Verbraucher eine Selbstverantwortung bei Themen, die ihre informationelle Selbstbestimmung betreffen, haben. So scheint es neben den notwendigen Anforderungen, wie dem einhalten gesetzlicher Pflichten, auch vielversprechend, in die Überwindung psychologischer Hürden zu investieren und Verbraucherinnen und Verbraucher mit dem relevanten Wissen auszustatten, wie sie ihre informationelle Selbstbestimmung wirksam ausüben können.

#### VERBRAUCHERMOTIVATION UND ÜBERWINDUNG PSYCHOLOGISCHER HÜRDEN

Während der Zugang zu Datenschutzinformationen zu den rechtlichen Pflichten gehört, ist die Sichtbarkeit in der Praxis oftmals nicht optimal ausgestaltet. So können die vorgestellten vereinfachenden Methoden, wie der One-Pager, kaum ihre Wirkung entfalten, wenn diese hinter einem Link versteckt werden. Dies bedeutet also nicht, dass die Vereinfachung an sich nicht wirksam ist, sondern die Gestaltung der Entscheidungssituation hinderlich ist. Als Lösungsmöglichkeit könnten Datenschutztexte vor Nutzung eines Dienstes bzw. vor dem Erheben der ersten Daten per Default an-

gezeigt werden. Durch diese erhöhte Sichtbarkeit hätten Verbraucherinnen und Verbraucher die Chance, sich zu informieren, ohne dass Suchkosten anfallen.

Darüber hinaus sind, wie bereits angesprochen, aktivierende Elemente oder die Umsetzung von Wahlmöglichkeiten in den Entscheidungsprozess vielversprechend. Diese können der mangelnden Kontrollüberzeugung (Friss oder stirb) der Verbraucherinnen und Verbraucher entgegenwirken. Differenzierte Wahlmöglichkeiten bzw. die differenzierte Einwilligung ist in der Datenschutzgrundverordnung (DSGVO) verankert, die im Mai 2018 in Kraft tritt. Bei Datenverarbeitungen, die nicht unter die gesetzlichen Erlaubnistatbestände fallen, würde dies bedeuten, dass für Datenerhebungen unterschiedlicher Zwecke auch separate Einwilligungen eingeholt werden müssen.

In der heutigen Praxis werden Differenzierungsmöglichkeiten durch vereinzelte Anbieter bereits forciert. So beschreibt Microsoft Cortana in den Datenschutzerklärungen für die Smartphone-Betriebssysteme iOS und Android beispielsweise, wie Zugriffsmöglichkeiten gesteuert werden können. Zwar müssen Nutzerinnen und Nutzer aktiv werden, jedoch werden ihnen die notwendigen Informationen bereitgestellt.

**Wirksamkeit**

Zur Wirksamkeit der „Anzeige per Default" liegen Daten einer verhaltenswissenschaftlichen Untersuchung im Auftrag der Europäischen Kommission vor (Elshout et al, 2016). So ist die Lesewahrscheinlichkeit bei Datenschutztexten, die hinter einem Link verborgen sind, sehr viel geringer, als bei der automatischen Anzeige der Texte. Während diese kurzfristigen Beobachtungen vielversprechend scheinen, ist jedoch über die langfristige Wirkung der Sichtbarmachung von Datenschutztexten nichts bekannt. So existieren Bedenken, dass sich auch hier eine Abstumpfung einstellen könnte.

Zur Wirksamkeit von differenzierten Wahlmöglichkeiten liegen bisher keine Ergebnisse vor. Im Zuge der Umsetzung und Anwendung der DSGVO bleibt also abzuwarten, wie Differenzierungsmöglichkeiten umgesetzt werden und welche Wirkung sie entfalten.

## VERBRAUCHERBILDUNG

Der Entwurf des Koalitionsvertrags zwischen CDU, CSU und SPD vom 7. Februar 2018 misst digitaler Bildung einen hohen Stellenwert bei und so findet sich im Text die Forderung nach „digitalen Fähigkeiten als Schlüsselkompetenz" (Z. 1613). Auch im Expertenworkshop wurde der Hebel der digitalen Verbraucherbildung als vielversprechend angesehen und Datenschutz zu den Schlüsselkompetenzen gezählt. So ist es notwendig, Verbraucherinnen und Verbraucher mit dem nötigen Wissen auszustatten, um zu verstehen, was Datenverarbeitung konkret bedeutet und welche Konsequenzen aus ihnen für ihre Privatsphäre folgen.

Wie bereits in Abschnitt 4.4 eingeführt, führen beispielsweise kognitive Verzerrungen dazu, dass Verbraucherinnen und Verbraucher die Gefahren von Datenverarbeitung fehleinschätzen. Der Trugschluss, dass gut gestaltete Smart Home-Oberflächen oder Produkt-Webseiten auch mit einem datensparsamen Angebot einhergehen, sollte beispielsweise aufgelöst werden. Außerdem sollten Verbraucherinnen und Verbraucher mit den Fähigkeiten ausgestattet werden, irreführende Textstellen zu identifizieren.

Beispiele aus dem Bereich der Verbraucherbildung sind die Angebote des BMJV (Verbraucherportal, 2018), von Deutschland sicher in Netz e.V. (2018) einem Verein, der neben IT-Sicherheit auch über

den Umgang mit personenbezogenen Daten in sozialen Netzwerken informiert, oder mobilsicher (2018), welches beispielsweise das Zugriffsmanagement auf Smartphones erklärt.

**Wirksamkeit**

Verbraucherbildung wurde im Expertenworkshop eine sehr hohe Relevanz beigemessen. Zur Frage, ob und wieweit sich gesteigerte Fähigkeiten im Bereich Datenschutz auf das Verhalten von Verbraucherinnen und Verbraucher auswirken ist jedoch nicht erforscht.

Aus den Ergebnissen zur Verbrauchermotivation und -bildung folgt Handlungsempfehlung 4.

Handlungsempfehlung 4: Der selbstbestimmte Umgang von Verbraucherinnen und Verbrauchern mit ihren personenbezogenen Daten sollte gestärkt werden, so dass die Motivation, sich mit Datenschutztexten auseinanderzusetzen und die Informiertheit gestärkt wird. Dies könnte beispielsweise durch Anzeige von Datenschutztexten by Default, der Ausgestaltung differenzierter Einwilligungssituationen oder Kampagnen für Verbraucherinformation erreicht werden.

## 7.2 UMGANG MIT NUTZERDATEN

Das Haus oder die eigene Wohnung sind ein besonders schützenswerter Lebensbereich und abzugrenzen vom Arbeitsplatz oder öffentlichen Räumen (Saizmaa & Kim, 2008). Dem Schutzbedürfnis von Bewohnerinnen und Bewohnern muss daher Rechnung getragen werden – wahrscheinlich stärker als in anderen digitalen Räumen. Wie in Kapitel 5 dargestellt, ist dezidiertes User-Profiling durch Smart Home-Anwendungen bislang bei Weitem nicht so umfassend, ausgeprägt und allgegenwärtig, wie bei Online-Diensten und Apps. Gleichzeitig lässt sich schon heute an verschiedenen Einzelfällen ablesen, welche Herausforderungen zukünftig auf Verbraucherinnen und Verbraucher und den Gesetzgeber zukommen werden. Weiterhin ist User-Profiling im Smart Home eng verknüpft mit der grundsätzlichen Datenschutz- und Profiling-Debatte im Zuge der Datenschutzgrundverordnung (vgl. Article 29 Data Protection Working Party, 2017b), Entwicklungen im Bereich Maschinelles Lernen und dem immer intensiver geführten Diskurs über die Nachvollziehbarkeit von Algorithmen.

- Datenschutzgrundverordnung: In den nächsten Jahren wird durch Präzedenzfälle und den Tätigkeiten der Datenschutzbehörden ein klareres Bild davon entstehen, welches Maß an User-Profiling in welchen Bereich und zu welchem Zweck als gesellschaftlich „akzeptabel“ betrachtet wird. Diese Entwicklung wird nicht nur für Online-Dienste und Apps zu beobachten sein, sondern wird sich auch bei Smart Home-Anwendungen abspielen. Auch wenn der derzeitige Fokus auf Online-Diensten und Apps liegt, so ist zu vermuten, dass Aufsichtsbehörden vermehrt Bußgelder gegen Hersteller und Betreiber von Smart Home-Geräten verhängen werden, sollten diese umfassendes Profiling betreiben (Unabhängiges Datenschutzzentrum Saarland, 2017).
- Maschinelles Lernen (ML): Wie in Kapitel 5.1 beschrieben, ist es auch für Dritte möglich, User-Profiling zu betreiben, indem der Datenverkehr eines Smart Homes mittels Mustererkennung (Traffic Pattern Analysis) analysiert wird. Entwicklungen im Bereich ML werden diese Art der massenhaften Analyse unstrukturierter Daten deutlich vereinfachen. In welchem Umfang dies Auswirkungen auf die Privatsphäre der Smart Home-Bewohnerinnen und Bewohner hat, ist heute noch nicht absehbar.

- Nachvollziehbarkeit von Algorithmen: Auch wenn die Hardware von Smart Home-Geräten immer leistungsfähiger wird, ist es sehr wahrscheinlich, dass zukünftig immer mehr Datenauswertung nicht im Gerät selbst, sondern in Rechenzentren des Herstellers oder Betreibers stattfinden wird. Auch für Smart Home-Geräte ist die derzeitige Debatte um Nachvollziehbarkeit von Algorithmen daher relevant, da Nutzerinnen und Nutzer ein Interesse daran haben, wie und warum verschieden Smart Home-Anwendungen zu bestimmten Rückschlüssen und Erkenntnissen kommen.

Wie zuvor erwähnt, ist User-Profiling im Smart Home teilweise zu unterscheiden von User-Profiling in gängigen Online-Diensten oder Apps. Im Folgenden werden daher drei zentrale Aspekte näher beleuchtet, die zukünftig Aufmerksamkeit durch Gesetzgeber und Verbraucherschützer benötigen.

### 7.2.1 ZUGESICHERTE FUNKTIONALITÄT

Schon heute wird ein Großteil der Funktionalität eines Smart Home-Gerätes über die Software definiert. Dies wird zukünftig noch weiter zunehmen. Daher gibt es Forderungen, dass Hersteller kenntlich machen, inwieweit ein Smart Home-Gerät gänzlich ohne Internetzugang betrieben werden kann (Offline-Funktionalität, vgl. #iotmark, 2017). Da immer mehr Hersteller bereits am Markt etablierte Produkte um User-Profiling oder zumindest umfassende Datenanalyse erweitern, stehen Nutzerinnen und Nutzer immer öfter vor der Entscheidung – entweder Funktionalität opfern oder der Datenanalyse zustimmen.

- iRobot Roomba: Der US Amerikanische Hersteller autonomer Staubsauger hatte angekündigt, dass die durch *Roomba* Staubsauger im Laufe der Zeit erstellten Wohnungspläne an Dritt-Unternehmen verkauft oder zumindest kostenlos zur Verfügung gestellt werden sollen (boinboing, 2015; Wolfe, 2017). Nach vielen negativen Reaktionen auf iRobots Geschäftspläne, hat das Unternehmen die Aussagen revidiert und die Pläne relativiert (Gewirtz, 2017). Das Beispiel zeigt jedoch, dass Hersteller von Smart Living-Anwendungen ihr Geschäftsmodell unter Umständen sehr schnell ändern oder erweitern, falls bestimmte Daten oder Erkenntnisse daraus monetarisiert werden können.
- SONOS Netzwerklautsprecher: Um die eigenen Netzwerklautsprecher an Sprachassistenten, wie Amazon Alexa oder Google Home, anzubinden, hatte der Hersteller SONOS seine Datenschutzerklärung geändert. Nutzerinnen und Nutzer, die ein Software-Update durchführen wollten, mussten zunächst den geänderten Datenschutzbestimmungen zustimmen. Falls dies nicht erfolgte, war ein Update nicht möglich und SONOS hatte schon via Pressemitteilung gewarnt, dass langfristig veraltete Geräte (ohne Software-Update) nicht mehr nutzbar sein würden (Whittaker, 2017). Nutzerinnen und Nutzer mussten der deutlich erweiterten Datenanalyse daher zustimmen, um die langfristige Nutzbarkeit ihres Produktes sicherzustellen.

Gerade bei Smart Home-Geräten, werden Nutzer zukünftig wohl immer häufiger vor der Entscheidung stehen, dass sie entweder einer zusätzlichen und erweiterten Datenanalyse zustimmen oder essenzielle Funktionalitäten des Gerätes verlieren. Schon vor dem Kauf sollte daher transparent sein, welche Funktionalität durch den Hersteller auch langfristig garantiert wird, ohne dass User-Profiling oder umfassende Datenanalyse stattfindet.

**Wirksamkeit**

Dass immer mehr Funktionalitäten eines Gerätes über Software definiert werden, bedeutet für Unternehmen, dass sie deutlich mehr experimentieren und auch nachträglich Geräte durch ein Software-Update verbessern können. Diese Innovationskraft und Flexibilität ist gut und wichtig – gerade in jungen Märkten, wie dem Smart Home. Gleichzeitig darf es nicht bedeuten, dass Nutzerinnen und Nutzer der Willkür des Unternehmens ausgeliefert sind, wie lange eine gewisse Funktionalität zur Verfügung gestellt wird.

Aus den Ergebnissen folgt die fünfte Handlungsempfehlung:

Handlungsempfehlung 5: Es braucht klare Regeln durch den Gesetzgeber, inwieweit zum Kaufzeitpunkt vorhandene und zugesicherte Funktionalität im Nachhinein durch den Hersteller an erweitere Datenanalyse oder User-Profiling geknüpft werden darf.

### 7.2.2 TRANSPARENZ ÜBER PARTNERSCHAFTEN SCHAFFEN

Gerade bei Sprachassistenten und vernetztem Spielzeug sind strategische Partnerschaften von entscheidender Bedeutung: Welche Zahnpasta ein Sprachassistent nach Aufforderung vorschlägt, ist vergleichbar mit dem ersten Platz einer Suchanfrage im Browser. Während man bei visueller Interaktion zu weiteren Vorschlägen (Zahnpasta anderer Unternehmen) weiterscrollen kann, ist dies bei sprachbasierter Interaktion zumindest mit deutlich mehr Aufwand verbunden. Gleiches gilt für vermittelte Informationen oder Wissen, zum Beispiel bei vernetztem Spielzeug. Wie zuvor erläutert ist es gerade bei kontrovers diskutierten Themen von entscheidender Bedeutung, aus welcher Quelle eine Information stammt.

**Wirksamkeit**

Um zu verstehen, warum ein bestimmtes Produkt vorgeschlagen wird oder warum eine bestimmte Information gegeben wird, benötigt es Transparenz über die strategischen Partnerschaften und Geschäftsbeziehungen zwischen dem Hersteller eines Smart Home-Gerätes und dritten Parteien. Für Nutzerinnen und Nutzer muss es ersichtlich sein, dass etwa Amazon Echo Colgate Zahnpasta vorschlägt, nicht weil sie „sehr gut“ getestet wurde, sondern weil es einen Vertrag zwischen Colgate und Amazon hinsichtlich der Produktplatzierungen gibt. Ebenso ist es für Eltern wichtig zu wissen, dass ein vernetztes Lernspielzeug seine Informationen aus Wikipedia oder anderen, proprietären Online-Quellen nimmt.

Aus diesen Ergebnissen leitet sich die Handlungsempfehlung 6 ab:

Handlungsempfehlung 6: Unternehmen sollten Auskunft über strategische Partnerschaften und Informationsquellen von Smart Home-Anwendungen geben. Die Informationen könnten beispielsweise über dieselbe Plattform zur Verfügung gestellt werden, über die Verbraucherinnen und Verbraucher auch ihre Accountdaten verwalten.

## 7.3 SICHERHEITSRISIKEN

Wie im Kapitel 6 dargestellt, benötigt es weniger neue Technologien, um Smart Home-Geräte abzusichern, sondern die konsequente Umsetzung bereits seit langem etablierter Sicherheitskonzepte, wie starke Ende-zu-Ende Verschlüsselung, sichere Authentifizierung oder signierte Software-Updates. Dass gerade bei Smart Home-Geräten vorhandene, etablierte Sicherheitskonzepte kaum oder nur unzureichend umgesetzt werden, liegt vor allem an **fehlenden ökonomischen Anreizen**:

1. Bisher können Hersteller von Smart Home-Geräten gegenüber Endkundinnen und Endkunden jegliche **Gewährleistung** bzgl. der Software ausschließen. Im Schadensfall, wenn also eine Softwareschwachstelle im Smart Home-Gerät durch kriminelle Hacker erfolgreich ausgenutzt wird, haftet der Hersteller nicht (Wendehorst, 2016). Im Schadensfall kann der Hersteller die Kosten also externalisieren, dadurch verringert sich automatisch ein ökonomischer Anreiz, sichere Softwareentwicklungsprozesse zu etablieren.

2. Weiterhin ist es für durchschnittliche Nutzerinnen und Nutzer unmöglich, von außen ein "sicheres" von einem "unsicheren" Smart Home-Gerät zu unterscheiden. Es besteht eine **Informationsasymmetrie** zwischen Nutzerinnen und Nutzern und Hersteller hinsichtlich der Sicherheit des Produktes. Selbst wenn in unabhängigen Tests die Softwarequalität überprüft würde, erlaubt dies noch keine Aussage über die Zukunft: *Wie lange wird der Hersteller dieses Produkt mit Sicherheitsupdates versorgen? Wie schnell werden die Sicherheitsupdates zur Verfügung gestellt werden?* Nur der Hersteller kann Antworten auf diese Frage geben – bisher geschieht dies jedoch regelmäßig nicht (Kleinhans, 2017).

Mangelnde Haftung des Herstellers im Schadensfall und starke Informationsasymmetrien hinsichtlich der Sicherheit eines Smart Home-Gerätes führen dazu, dass viele Verbraucherinnen und Verbraucher derzeit beim Kauf wenig Wert auf Sicherheit legen (können). Derzeit ist es für sie kaum möglich verbindliche Aussagen hinsichtlich IT-Sicherheit zu einem Smart Home-Gerät zu bekommen. Dadurch fließen vor allem andere Features in die Kaufentscheidung mit ein: Design, Leistungsfähigkeit, Komfortgewinn, u.ä. Durch diese Faktoren honoriert der Markt für Smart Home-Geräte derzeit kaum IT-Sicherheit, was Hersteller wiederum dazu veranlasst, sicherer Softwareentwicklung und -support kaum Ressourcen zu widmen, da diese Kosten durch den Markt nicht getragen werden. Aufgrund dieser falschen Rahmenbedingungen muss konstatiert werden, dass der Markt für Smart Home-Geräte derzeit darin versagt, verhältnismäßig vertrauenswürdige Produkte zu liefern.

In den letzten Jahren sind sich manche Hersteller ihrer Verantwortung bewusst geworden und haben interne Prozesse etabliert bzw. professionalisiert und verschiedene Konsortien und Institutionen haben **Guidelines und Best Practices** veröffentlicht (GSMA, 2018; ENISA, 2017). Wahrscheinlich auch, weil sie den Druck seitens der Regierungen spüren, so wurden durch die US Federal Trade Commission (FTC) bereits erste Geldbußen verhängt.

### 7.3.1 CAPACITY BUILDING UND BEST PRACTICES

Viele Hersteller von klassischen Haushaltsgeräten sind, wie auch viele andere Industrien, überfordert, ihre Produktpalette zügig zu digitalisieren und zu vernetzen. Wie zuvor erwähnt, folgt *Security* (IT-Sicherheit) einer anderen Logik, als *Safety* (Produktsicherheit): Hersteller müssen nun entscheiden auf welcher Hardware sie entwickeln wollen, welche Softwarebibliotheken und Frameworks sie einsetzen, usw. Das Etablieren eines sicheren Softwareentwicklungsprozesses ist eine zentrale Her-

ausforderung. Daher haben sowohl Unternehmen, als auch Konsortien, Behörden und Communities in den letzten Jahren viele verschiedene Guidelines und Best Practices veröffentlicht (Schneier, 2017).

**Wirksamkeit**

Gerade für kleinere Organisationen und Hersteller, die am Anfang der Vernetzung ihrer Produktpalette stehen, erleichtern entsprechende Guidelines die Orientierung. Gleichzeitig muss konstatiert werden, dass es entsprechende Guidelines und Best Practices (nicht nur für das Internet der Dinge und Smart Home-Anwendungen) schon seit vielen Jahren gibt. Es scheint jedoch bisher zumindest teilweise an Anreizen seitens der Hersteller zu fehlen, entsprechende Guidelines zu befolgen. Es mangelt daher nicht an Guidelines zur sicheren Entwicklung von Smart Home-Geräten, sondern eher am Willen, diesen zu folgen. Gleichzeitig hilft der Prozess an dessen Ende eine Guideline oder Richtlinien stehen, den verschiedenen Stakeholdern, sich untereinander besser zu verstehen.

Aus diesen Ergebnissen folgt Handlungsempfehlung 7:

Handlungsempfehlung 7: Es mangelt nicht an Sicherheits-Guidelines, vielmehr können die vorhandenen als Grundlage für weitere regulatorische Interventionen (Siegel, Mindestanforderungen) genommen werden. Der Fokus sollte darauf liegen, Anreize für Hersteller zu schaffen, die vorhandenen Best Practices zu befolgen.

### 7.3.2 INFORMATIONSASYMMETRIEN ZWISCHEN HERSTELLERN UND VERBRAUCHERINNEN UND VERBRAUCHERN ABBAUEN

Viele verschiedene Stakeholder arbeiten derzeit an Gütesiegeln für „sichere“ Smart Home-Geräte: Die Bundesregierung forderte schon in der Cyber-Sicherheitsstrategie 2016 die Entwicklung eines „Gütesiegels für IT-Sicherheit“ und der Bundestag hat die Bundesregierung 2017 aufgefordert, ein solches in einem offenen, abgestimmten Prozess zu entwickeln (Bundesministerium des Inneren, 2016; 2017). Ebenso möchte die EU Kommission mit dem vorgelegten Entwurf des Cybersecurity Acts europaweit gültige Gütesiegel für sichere IT-Produkte einführen (Europäische Kommission, 2017). Gleichzeitig gibt es Community-getriebene Initiativen wie das #iotmark (2017) oder das der IoT Security Foundation (2018). Zentrales Ziel jener Bestrebungen ist es, die Informationsasymmetrie zwischen Verbraucherinnen und Verbrauchern und Herstellern abzubauen. Dies kann mehrere positive Effekte zur Folge haben:

Verbraucherinnen und Verbraucher können durch das Siegel „sichere“ von „unsicheren“ Produkten am Markt unterscheiden. Dadurch kann IT-Sicherheit überhaupt erst zum potenziellen Kaufkriterium für Verbraucherinnen und Verbraucher werden. Gleichzeitig können sich Hersteller mit Produkten, die ein Siegel erhalten haben, von der Konkurrenz am Markt differenzieren. Über das Siegel können sie den Verbraucherrinnen und Verbrauchern beispielsweise versichern, wie lange Software-Updates zur Verfügung gestellt werden. Etabliert sich ein Siegel also langfristig am Markt, motiviert es immer mehr Hersteller dazu, auch dem Siegel zu folgen.

## Wirksamkeit

Unter optimalen Bedingungen *kann* ein Siegel die oben beschriebenen positiven Effekte erzielen. In anderen Bereichen, wie Nahrungsmitteln oder Mode, werden seit vielen Jahrzehnten Siegel zur Verbraucherkommunikation eingesetzt. Hier lassen sich einige potenzielle Herausforderungen ableiten:

So ist es möglich, dass der Markt von Siegeln überschwemmt wird, wodurch Verbraucherinnen und Verbraucher keine Orientierung mehr haben, welches Siegel nun wie viel „wert" ist (vgl. auch Abschnitt 7.1.2 zur Nutzerinterpretation von Datenschutzsiegeln). Dieser Problematik hat sich die Bundesregierung im Bereich Nachhaltigkeit schon vor vielen Jahren angenommen, etwa durch die Schaffung von Webseiten wie siegelklarheit.de oder label-online.de, auf denen Verbraucherinnen und Verbraucher über die Vielfalt und Bedeutung von Siegeln aufgeklärt werden sollen (BMZ, 2018; Verbraucher Initiative, 2018). Im schlimmsten Fall droht langfristig ein ähnlicher Effekt bei IT-Sicherheit, wodurch Verbraucherinnen und Verbraucher durch die Vielzahl an Siegeln überfordert wären.

Darüber hinaus benötigt es Zeit und Kommunikationsarbeit, damit Verbraucherinnen und Verbraucher Vertrauen in ein Siegel aufbauen. Sollte beispielsweise ein europaweit einheitliches Siegel für sichere Smart Home-Geräte eingeführt werden, müsste dies durch intensive Kommunikationsarbeit und Aufklärungskampagnen begleitet werden.

Für das Vertrauen der Verbraucherinnen und Verbraucher ist ebenso entscheidend, was hinter dem Siegel steht: Ist es eine Selbstauskunft des Herstellers (potenziell weniger vertrauenswürdig), oder eine externe Zertifizierung des fertigen Produktes durch unabhängige Dritte (potenziell eher vertrauenswürdig)?

Außerdem ist es fraglich, ob Siegel die Problematik der Drittbetroffenheit (siehe Botnetze) adäquat adressieren können. Wenn den Verbraucherinnen und Verbrauchern durch ein kompromittiertes Gerät zunächst kein Schaden entsteht, warum sollten sie dann mehr für ein Gerät mit Siegel ausgeben?

Ein Siegel ist statisch: Entweder hat ein Produkt ein entsprechendes Siegel (das Produkt ist „sicher") oder es hat kein Siegel (das Produkt ist „unsicher"). IT-Sicherheit ist jedoch ein dynamischer Prozess, der konstante Aufmerksamkeit des Unternehmens verlangt. Wenn ein Produkt zum Zeitpunkt X alle Kriterien eines Siegels erfüllt hat, kann eine Woche später durch eine neu entdeckte, schwerwiegende Softwareschwäche, trotzdem die gesamte Sicherheit des Produktes kompromittiert sein. Wie soll ein Siegel diese Dynamik sinnvoll abbilden können?

Hieraus folgt die achte Handlungsempfehlung:

**Handlungsempfehlung 8:** Siegel sollten lediglich als *ein* Baustein einer nachhaltigen IT-Sicherheitspolitik betrachtet werden. Damit sie tatsächlich Informationsasymmetrien zwischen Herstellern und Verbraucherinnen und Verbrauchern abbauen, müssen die Rahmenbedingungen richtig gesetzt werden.

### 7.3.3 UNVERHÄLTNISMÄßIG UNSICHERE GERÄTE VOM MARKT AUSSCHLIEßEN

Mit der CE-Kennzeichnung hat die EU eine *Mindestanforderung* an die physische Produktsicherheit für verschiedene Produktgruppen definiert. Bestimmte Produkte benötigen eine CE-Kennzeichnung, um im Binnenmarkt vertrieben werden zu dürfen. Ein „CE" auf einem Produkt bedeutet jedoch keineswegs, dass dieses Produkt sicher ist, sondern vielmehr, dass es nicht unverhältnismäßig unsicher für den europäischen Binnenmarkt ist (Zwetsloot et al., 2011). Ähnliche Überlegungen einer Mindestanforderung bzgl. IT-Sicherheit an internetfähige Produkte finden sich im aktuellen Koalitionsvertrag der CDU/CSU und SPD (2018), als auch als ein mögliches langfristiges Ziel des Cybersecurity Acts auf EU-Ebene. Ziel wäre es, unverhältnismäßig unsicheren Smart Home-Geräten den Marktzutritt zu verweigern. Weiterhin wurde 2017 durch mehrere US-Senatoren ein Gesetzesentwurf vorgelegt, nach dem IoT-Hersteller Nachweise erbringen müssen, dass sie sich an gewisse Mindeststandards hinsichtlich IT-Sicherheit gehalten haben, falls sie an einer öffentlichen Ausschreibung zur IT-Beschaffung von US-Behörden teilnehmen wollen (U.S. Senate, 2018).

**Wirksamkeit**

Eine Mindestanforderung bzgl. IT-Sicherheit für Smart Home-Geräte als Marktzutrittsbarriere kann die Verbreitung unverhältnismäßig unsicherer Geräte deutlich eindämmen. Hierfür müssen jedoch die richtigen Rahmenbedingungen gesetzt werden:

Die zuständigen Conformity Assessment Bodies (Testlabore) müssen entsprechende Ressourcen und technisches Fachwissen haben, um die Masse an heute schon und zukünftig verfügbaren Smart Home-Geräten testen zu können. Außerdem benötigt es eine responsive und effektive Marktüberwachung, um zügig Geräte zu identifizieren, die nicht (mehr) den Mindestanforderungen entsprechen.

Falls ein CE-Konformitätstest um Aspekte der IT-Sicherheit erweitert werden sollte, müsste die Überprüfung der IT-Sicherheit wesentlich häufiger und punktueller erfolgen, als es gängige Testzyklen unter CE bisher vorsehen.

Ähnlich zu freiwilligen Siegeln bleibt die Problematik, dass jeglicher Konformitätstest eine Momentaufnahme ist. Im Rahmen eines Konformitätstests müssten daher auch Aspekte, wie verbindlicher Softwaresupport-Zeitraum und Reaktionszeit bei Auftreten einer Sicherheitslücke überprüft werden.

Die neunte Handlungsempfehlung, die hieraus folgt, ist:

Handlungsempfehlung 9: Da Safety (Produktsicherheit) und Security (IT-Sicherheit) voneinander abhängen, sollten europaweite Mindestanforderungen für beide Aspekte definiert werden. Dies könnte als Ko-Regulierungsansatz zusammen mit der Industrie geschehen, indem sektorspezifische Mindestanforderungen definiert werden und dadurch IT-Sicherheit Teil der CE-Konformitätstests wird. Für eine effektive und effiziente Überwachung der Einhaltung durch Marktteilnehmer, benötigt es jedoch eine umfassende Modernisierung des derzeitigen CE-Ökosystems aus Testlaboren, Standardisierung und Marktüberwachung.

### 7.3.4 HERSTELLER STÄRKER ZUR VERANTWORTUNG ZIEHEN

Die Einführung von „Software-Haftung“ wird seit längerem diskutiert (Spindler, 2007). In einer Welt, in der zunehmend Funktionalitäten eines Gerätes über Software definiert werden, ist es dringend notwendig, etablierte Konzepte der Verteilung von Verantwortung auf den digitalen Raum zu übertragen. Für viele Verbraucherinnen und Verbraucher ist es schwer verständlich, warum ein Smart TV mit einem defekten Netzteil reklamiert werden kann, eine Reklamation aufgrund defekter Software jedoch ausgeschlossen ist. So finden sich auch im Koalitionsvertrag zwischen CDU/CSU und SPD (2018) Aussagen zur Ausweitung der Produkthaftung und der Einführung einer durchgehenden Haftungskette.

**Wirksamkeit**

Eine Ausweitung der Produkthaftung auf Softwarebestandteile hätte die Chance, Rechte und Pflichten zwischen Hersteller, Betreiber und Verbraucherinnen und Verbraucher gerechter zu verteilen. Gerade bei Smart Home-Geräten sind derzeit vor allem Verbraucherinnen und Verbraucher im Schadensfall die Leidtragenden. Gleichzeitig sind damit einige Herausforderungen verbunden, die zunächst durch den Gesetzgeber geklärt werden müssten. Dazu gehören unter anderem:

a. Ab wann stellt eine Sicherheitslücke einen Mangel dar?

b. Gehört es zu den Pflichten der Verbraucherinnen und Verbraucher zeitnah Software-Updates (soweit vorhanden) durchzuführen?

c. Was ist eine angemessene Reaktionszeit seitens des Herstellers auf eine neu bekannt gewordene Sicherheitslücke?

d. Kann sich der Hersteller der Haftung entziehen, falls ausschließlich Open Source Software auf dem Gerät eingesetzt wird?

e. Wie stehen Haftung und gesetzliche Mindestanforderungen zueinander in Beziehung? Wie kann der Hersteller belegen, dass er ein ausreichend vertrauenswürdiges Gerät hergestellt und gepflegt hat?

Aus den Ergebnissen folgt Handlungsempfehlung 10.

Handlungsempfehlung 10: Die Ausweitung der Produkthaftung auf Softwarebestandteile ist eine notwendige aber keine hinreichende Bedingung zur Stärkung der IT-Sicherheit in Smart Home-Anwendungen. Der Fokus sollte auf einer gerechteren Verteilung von Rechten und Pflichten zwischen Hersteller, Betreiber und Nutzerin und Nutzer liegen.

## 7.4 WEITERE PROBLEMFELDER

Über Problemfelder und Lösungsansätze, die den Schwerpunktthemen informationelle Selbstbestimmung, Umgang mit Daten und IT-Sicherheit zugeordnet werden können, gibt es für das Smart Home zwei übergeordnete Empfehlungen. Die erste leitet sich daraus ab, dass Geräte technisch immer einfacher zu vernetzen sind. Die zweite resultiert aus den Forschungslücken, die im Gutachten identifiziert wurden.

### 7.4.1 DATENSPARSAME ANWENDUNGEN FÖRDERN UND RECHT AUF „ANALOGE WELT“ STÄRKEN

Wie in der Anwendungs- und Marktanalyse beschrieben, schreitet die Vernetzung der Heimgeräte immer weiter voran. Zum einen konnte diese Entwicklung darauf zurückgeführt werden, dass Anwendungen komfortabler und somit attraktiver für Verbraucherinnen und Verbraucher werden. Zum anderen sind vor allem datengetrieben Geschäftsmodelle im Bereich des eCommerce erfolgreich. Dieser Entwicklung steht gegenüber, dass manche Verbraucherinnen und Verbraucher kein Bedürfnis haben, vernetzte Anwendungen zu besitzen und nutzen.

Beim Safer Internet Day 2017, der vom BJMV und dem Branchenverband Bitkom zum Smart Home ausgerichtet wurde, wurde denn auch seitens der Politik gefordert, dass Verbraucherinnen und Verbraucher die Möglichkeit behalten sollten, auf die Vernetzung ihrer Wohnung zu verzichten und somit ein „Recht auf analoge Welt“ auszuüben (BMJV, 2017).

Hieraus folgt Handlungsempfehlung 11:

Handlungsempfehlung 11: Trotz der großen Chancen, die sich aus der Vernetzung von Hausgeräten ergeben, sollten Anwendungen nicht um jeden Preis und vollständig vernetzt werden. So müssen Verbraucherinnen und Verbraucher die Möglichkeit behalten, auch nicht-vernetzte Produkte zu nutzen.

### 7.4.2 FORSCHUNGSBEDARFE IDENTIFIZIEREN UND ANGEHEN

Im mehreren Bereichen dieses Gutachtens wurden Forschungsbedarfe identifiziert. Hierzu zählen beispielsweise der Umgang mit psychologischen Hürden bei der Ausübung informationeller Selbstbestimmung oder Bildungsmaßnahmen. Auch der Bereich des User-Profilings ist, bis auf die identifizierten Fallbeispiele, weitestgehend unerforscht und so sind beispielsweise die langfristigen Auswirkungen manipulierender Smart Living-Anwendungen unklar.

Ein zentraler Unterschied zwischen Online-Diensten und Smart Home-Anwendungen ist, dass Online-Dienste einen klaren Fokus auf einzelne Nutzerinnen und Nutzer haben, während viele Smart Home-Anwendungen durch Sensorik ihre gesamte Umgebung wahrnehmen. Dadurch sind von der Datenerfassung auch Dritte und Schutzbedürftige, wie Kinder oder Menschen mit einer Behinderung betroffen (Future of Privacy Forum, 2016). Smart Home ist noch ein junger Markt und es wird sich in den kommenden Jahren zeigen, wie gut die DSGVO unerwünschtes Verhalten von Unternehmen sanktionieren kann. Gleichzeitig benötigt es jedoch verstärkt Forschung, um genauer die Auswirkungen auf Schutzbedürftige und Dritte durch Smart Home-Anwendungen zu identifizieren.

Auch im Bereich der genannten Auswirkungen der Gatekeeper-Problematik ist begleitende Forschung notwendig. Smart Living Anwendungen, die das Einkaufsverhalten beeinflussen oder die Sichtweisen von Kindern (Smart Toys) lenken, sollten somit genauer beleuchtet werden – und dies nicht nur juristisch oder verbraucherpolitisch, sondern auch aus psychologischer Sicht.

Die letzte Handlungsempfehlung lautet deshalb:

Handlungsempfehlung 12: Die Forschung zu den Auswirkungen des Smart Homes auf Verbraucherinnen und Verbraucher sollte ausgeweitet und gefördert werden.

# 8 LITERATUR


Ahmed, E., Yaqoob, I., Hashem, I. A. T., Khan, I., Ahmed, A. I. A., Imran, M., & Vasilakos, A. V. (2017). The role of big data analytics in Internet of Things. Computer Networks, 129, 459-471.

Aksu, H., Babun, L., Conti, M., Tolomei, G., & Uluagac, A. S. (2018). Advertising in the IoT Era: Vision and Challenges. Abgerufen von: http://arxiv.org/abs/1802.04102 (26.02.2018)

Aldrich, F. K. (2003). Smart homes: past, present and future. In Inside the smart home (pp. 17-39). Springer London.

Android. (2018). Dashboards. Abgerufen von: https://developer.android.com/about/dashboards/index.html (26.02.2018)

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Kumar, D. (2017). Understanding the mirai botnet. In USENIX Security Symposium.

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. Abgerufen von: http://arxiv.org/abs/1708.05044 (26.02.18)

Armis. (2018). BlueBorne Cyber Threat Impacts Amazon Echo and Google Home. Abgerufen von: https://www.armis.com/blueborne-cyber-threat-impacts-amazon-echo-google-home/ (26.02.2018)

Article 29 Data Protection Working Party. (2017a). Guidelines on transparency under Regulation 2016/679, wp260. Abgerufen von: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 (23.02.2018)

Article 29 Data Protection Working Party. (2017b). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, wp251. Abgerufen von: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 (23.02.2018)

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.. (2016). BDEW-Energiemonitor 2016. Abgerufen von: https://www.bdew.de/internet.nsf/id/20160503-pi-energiewende-weiterhin-top-thema-fuer-die-bevoelkerung-de (26.02.2018)

Berkman Center for Internet & Society at Harvard University. (2016). Don't Panic - Making Progress on the "Going Dark" Debate. Abgerufen von: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (26.02.2018)

Billboard. (2017). Smart Speaker Sales More Than Tripled in 2017. Abgerufen von: https://www.billboard.com/articles/business/8085524/smart-speaker-sales-tripled-25-million-year-2017 (26.02.2018)

Bitkom. (2012). Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte (Leitfaden). Abgerufen von: https://www.bitkom.org/noindex/Publikationen/2012/Leitfaden/Leitfaden-Big-Data-im-Praxiseinsatz-Szenarien-Beispiele-Effekte/BITKOM-LF-big-data-2012-online1.pdf (26.02.2018)

Bitkom (2015a): Datenschutz in der digitalen Welt. Präsentation. Abgerufen von: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/09-September/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf (26.02.2018)

Bitkom. (2015b). Big Data und Geschäftsmodell-Innovationen in der Praxis: 40+ Beispiele. Abgerufen von: https://www.bitkom.org/noindex/Publikationen/2015/Leitfaden/Big-Data-und-Geschaeftsmodell-Innovationen/151229-Big-Data-und-GM-Innovationen.pdf (26.02.2018)

Bitkom. (2015c). Zukunft der Consumer Electronics – 2015. Marktentwicklung, Schlüsseltrends, Mediennutzung Konsumentenverhalten, Neue Technologien. Abgerufen von: https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/CE-Studie-Update/160226-CE-Studie-2015-online.pdf (26.02.2018)

Bitkom. (2017). Jeder vierte Deutsche möchte digitale Sprachassistenten nutzen. Pressemitteilung. Abgerufen von: https://www.bitkom.org/Presse/Presseinformation/Jeder-vierte-Deutsche-moechte-digitale-Sprachassistenten-nutzen.html (26.02.2018)

Bitkom und Deutsches CleanTech Institut (DCTI) (2015). DCTI GreenGuide Smart Home 2015 - Die optimale Lösung für Ihr Zuhause. Abgerufen von: http://www.dcti.de/fileadmin/user_upload/GreenGuide_SmartHome_2015_Webversion.pdf (26.02.2018)

boinboing. (2015). If you want a picture of the future, imagine a Roomba leaking pix of your home, forever. Abgerufen von: https://boingboing.net/2015/05/25/if-you-want-a-picture-of-a-fut.html (26.02.2018)

Bosch. (2018). Datenschutzhinweis Bosch Smart Home App. Abgerufen von: https://www.bosch-smarthome.com/de/de/datenschutz (26.02.2018)

Bouchard, K., Gaboury, S., Bouchard, B., Bouzouane, A., & Giroux, S. (2016). Smart Homes in the Era of Big Data. In Trends in Ambient Intelligent Systems (pp. 117-137). Springer, Cham.

Bundesamt für Sicherheit in der Informationstechik (BSI). (2016). Testkonzept für Breitband-Router. Abgerufen von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Testkonzept-Breitbandrouter.html (26.02.2018)

Bundesministerium des Inneren (BMI). (2016). Cyber-Sicherheitsstrategie 2016. Abgerufen von: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (26.02.2018)

Bundesministerium des Inneren (BMI). (2017). Pressemitteilung: Das Vertrauen der Verbraucher in die Digitalisierung stärken. Abgerufen von: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2017/07/it-guetesiegel.html (26.02.2018)

Bundesministerium der Justiz und für Verbraucherschutz (BMJV). (2017). „Smart Home – Wie digital wollen wir wohnen?“ Rede des Bundesministers der Justiz und für Verbraucherschutz Heiko Maas auf der gemeinsamen Konferenz von BMJV und Bitkom zum Safer Internet Day 2017 am 14. Februar 2017 in Berlin. Abgerufen von: https://www.bmjv.de/SharedDocs/Reden/DE/2017/02142017_SID2017.html (26.02.2018)

Bundesministerium der Justiz und für Verbraucherschutz (BMJV). (2018). Wissen wappnet. Das Verbraucherportal. Abgerufen von: http://www.bmjv.de/DE/Verbraucherportal/Verbraucherportal_node.html (26.02.2018)

Bundesministerium für Wirtschaft und Energie (BMWi). (2016). SmartHome2Market. Marktperspektiven für die intelligente Heimvernetzung – 2016. Abgerufen von: https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smarthome-broschuere.pdf?__blob=publicationFile&v=9 (26.02.2018)

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ). (2018). Siegelklarheit. Abgerufen von: https://www.siegelklarheit.de/home (26.02.2018)

CDU, CSU & SPD (2018). Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. Abgerufen von: http://www.handelsblatt.com/downloads/20936422/4/koalitionsvertrag_final.pdf (26.02.2018)

Connected Living. (2017). Smart Home Index 2017. In Kooperation mit Mücke, Sturm & Company. Abgerufen von: http://www.connected-living.org/content/4-information/1-news/20171011-smart-home-index-2017-ist-smart-home-in-deutschen-haushalten-angekommen/20171004_sh_index_connected-living.pdf (26.02.2018)

Consumers International. (2017). Testing our trust: Consumers and the Internet of Things 2017 Review. Abgerufen von: http://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf (26.02.2018)

Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016). Is Anybody Home? Inferring Activity from Smart Home Network Traffic. Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016, 245–251.

Crain, M. (2018). The limits of transparency: Data brokers and commodification. New Media & Society, 20(1), 88-104.

DATENSCHUTZscanner. (2018). DATENSCHUTZscanner by PrivacyGuard - ein Forschungsprojekt gefördert vom Bundesministerium für Bildung und Forschung. Abgerufen von https://datenschutz-scanner.de/das-projekt/ (26.02.2018)

Deloitte & TU München. (2015). Ready for Take-off? – Smart Home aus Konsumentensicht. Abgerufen von: http://www.connected-living.org/content/4-information/4-downloads/4-studien/8-ready-for-takeoff/deloitte-smart-home-consumer-survey-20150701.pdf (26.02.2018)

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI). (2015). Allgemeine Geschäftsbedingungen (AGB) von Kommunikationsdienstleistern (Ergebnisbericht). Abgerufen von: https://www.divsi.de/wp-content/uploads/2015/10/2015-10-22_DIVSI_AGB-Umfrage_Charts.pdf (26.02.2018)

Deutsche Telekom AG. (2015). Marktanalyse: Wachstumschancen für Unternehmen im Smart Home-Markt. Abgerufen von: https://www.qivicon.com/assets/PDF/Deutsche-Telekom-QIVICON-Marktanalyse-Smart-Home.pdf (20.02.2018)

Deutsche Telekom AG (2016). Datenschutz - ganz einfach!. Abgerufen von: https://www.telekom.de/datenschutz-ganz-einfach (26.02.2018)

Deutschland sicher im Netz e.V. (DsiN). (2017). DsiN SicherheitsIndex 2017 - Digitale Sicherheitslage der Verbraucher in Deutschland. Abgerufen von: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsindex_2017_web_0.pdf (26.02.2018)

Deutschland sicher im Netz e.V. (DsiN). (2018). Deutschland sicher im Netz. Webseite. Abgerufen von: https://www.sicher-im-netz.de (26.02.2018)

Dywer, C. (2017). Arkansas Prosecutors Drop Murder Case That Hinged On Evidence From Amazon Echo. NPR. Abgerufen von: https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo (26.02.2018)

Elshout, M., Elsen, M., Leenheer, J., Loos, M., & Luzak, J. (2016). Study on consumers' attitudes towards Terms and Conditions (T&Cs) - Final Report. Report for the European Commission, Consumers, Health, Agriculture and Food Executive Agency (Chafea) on behalf of Directorate-General for Justice and Consumers.

ENISA. (2017). Baseline Security - Recommendations for IoT. Abgerufen von: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (26.02.2018)

Europäische Kommission. (2017) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). COM(2017)477. Directorate-General for Communications Networks, Content and Technology. Abgerufen von: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en (26.02.2018)

Federal Trade Commission. (2017a). VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent. Abgerufen von: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it (26.02.18)

Federal Trade Commission. (2017b). What Vizio was doing behind the TV screen. Abgerufen von: https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen (26.02.18)

Future of Privacy Forum. (2016). Kids & the connected home: privacy in the age of connected dolls, talking dinosaurs, and battling robots. Abgerufen von: https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf (26.02.2018)

Gartner. (2014). Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022. Pressemitteilung. Abgerufen von: https://www.gartner.com/newsroom/id/2839717 (26.02.2018)

Gazis, V. (2017). A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Communications Surveys and Tutorials, 19(1), 482–511.

Gesellschaft für transparenten Datenschutz mbH (GftD). (2017). Gesellschaft für transparenten Datenschutz. Abgerufen von: https://www.datenschutz-mit-siegel.de (26.02.2018)

Gewirtz, D. (2017). Roomba is no spy: CEO says iRobot will never sell your data. ZDNet. Abgerufen von: http://www.zdnet.com/article/exclusive-roomba-ceo-responds-to-spying-story/ (26.02.2018)

GfK (2016a). Smart Home Lösungen bei deutschen Verbrauchern immer beliebter. Pressemitteilung vom 22.12.2016. Abgerufen von: http://www.gfk.com/de/insights/press-release/smart-home-loesungen-bei-deutschen-verbrauchern-immer-beliebter/ (26.02.2018)

GfK (2016b). Wie smart sind deutsche TV-Nutzer?. Pressemitteilung vom 31.05.2016. Abgerufen von http://www.gfk.com/de/insights/press-release/wie-smart-sind-deutsche-tv-nutzer/ (26.02.2018)

Google-Play Hilfe (2018) Erläuterungen zu den einzelnen Berechtigungsgruppen. Abgerufen von: https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1 (26.02.2018)

Google. (2018). Datensicherheit & Datenschutz bei Google Home. Abgerufen von: https://support.google.com/googlehome/answer/7072285?hl=de (26.02.2018)

Greis, F. (2017). Der streng geheime Streit über die Routersicherheit. Golem. Abgerufen von: https://www.golem.de/news/bsi-richtlinie-der-streng-geheime-streit-ueber-die-routersicherheit-1801-132363.html (26.02.2018)

GSMA. (2018). GSMA IoT-Security Guidelines. Abgerufen von: https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ (26.02.2018)

Hallman, R., Bryan, J., Palavicini, G., Divita, J., & Romero-Mariona, J. (2017). IoDDoS The Internet of Distributed Denial of Service Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: IoTBDS, (IoTBDS), 47–58.

Harper, R. (Ed.). (2003). Inside the smart home. Springer Science & Business Media.

Hill, K. & Mattu, S. (2018). The House that spied on me. Gizmodo. Abgerufen von: https://gizmodo.com/the-house-that-spied-on-me-1822429852 (26.02.2018)

Hirsch, L. und Castillo, M. (2018). Amazon has big plans for Alexa ads in 2018; it's discussing options with P&G, Clorox and others. CNBC. Abgerufen von: https://www.cnbc.com/2018/01/02/amazon-alexa-is-opening-up-to-more-sponsored-product-ads.html (26.02.2018)

Hirsch, L. (2018). Amazon has big plans for Alexa ads in 2018; it's discussing options with P&G, Clorox and others. Abgerufen von: https://www.cnbc.com/2018/01/02/amazon-alexa-is-opening-up-to-more-sponsored-product-ads.html (26.02.2018)

IBM Big Data Hub. (2013). The FOUR V's of Big Data. Abgerufen von: http://www.ibmbigdatahub.com/sites/default/files/infographic_file/4-Vs-of-big-data.jpg (26.02.2018)

Ingenrieth, F., & Kettner, S.E. (2017). Datenschutz bei Apps - eine Bestandsaufnahme. Vortrag auf dem V. Interdisziplinären Workshop „Privacy, Datenschutz & Surveillance“ / Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), Berlin.

Initiative D21. (2017). D21 Digital Index 2016. Jährliches Lagebild zur digitalen Gesellschaft. Abgerufen von: https://initiatived21.de/app/uploads/2017/01/studie-d21-digital-index-2016.pdf (26.02.2018)

Initiative D21. (2018). D21 Digital Index 2017/2018. Jährliches Lagebild zur digitalen Gesellschaft. Abgerufen von: https://initiatived21.de/app/uploads/2018/01/d21-digital-index_2017_2018.pdf (26.02.2018)

IOTA. (2018). IOTA Webseite. Abgerufen von: https://data.iota.org/ (26.02.2018)

#iotmark. (2017). Open Internet of things Certification Mark. Abgerufen von: https://iotmark.wordpress.com/principles/mozfest17/ (26.02.2018)

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. Future Generation Computer, 56, 719–733.

IoT Security Foundation. (2018). Best Practice User Mark FAQ and Terms of Use. Abgerufen von: https://www.iotsecurityfoundation.org/best-practice-user-mark/ (26.02.2018)

Kerner, R. (2016). Remote Code Execution in CCTV-DVR affecting over 70 different vendors. Abgerufen von: http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.htm (26.02.2018)

KerneronSecurity (2016). Remote Code Execution in CCTV-DVR affecting over 70 different vendors. Abgerufen von: http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html

Kettner, S.E., Thorun, C. & Vetter, M. (2018). Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz. ConPolicy – Institut für Verbraucherpolitik. Abgerufen von: https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (28.02.2018)

Kleinhans, J.-P. (2017). Internet of Insecure Things. Abgerufen von: https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf (26.02.2018)

Kühl, E. (2018). Alexa ist nicht mehr deine Schlampe. Zeit Online. Abgerufen von: http://www.zeit.de/digital/internet/2018-01/sprachassistenten-alexa-sexismus-feminismus-sprachsteuerung-ki/komplettansicht (26.02.2018).

Lenhard, W. & Lenhard, A. (2017). Berechnung des Lesbarkeitsindex LIX nach Björnson. Bibergau: Psychometrica. Abgerufen von: http://www.psychometrica.de/lix.html (10.12.2018)

Lübbeke, T. (2016). Akzeptanz von Smart Homes – von der Theorie zur Vermarktung. In Begleitforschung Mittelstand-Digital. (2016). Wissenschaft trifft Praxis – Neue Formen des Home Experience Design. Abgerufen von: http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/wissenschaft-trifft-praxis-ausgabe4,property=pdf,bereich=md,sprache=de,rwb=true.pdf (12.01.2018)

Markoff, J. (2016). Why light bulbs may be the next hacker target. New York Times. Abgerufen von: https://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=0 (26.02.2018)

Marktwächter Digitale Welt. (2017). E-Payment – Wie sicher sind unsere Daten beim Bezahlen im Netz? Eine Untersuchung der Verbraucherzentralen. Abgerufen von https://ssl.marktwaechter.de/sites/default/files/downloads/17-11-14_untersuchungsbericht_e-payment.pdf (26.02.2018)

Marr, B. (2015). Why only one of the 5 Vs of big data really matters. Abgerufen von: http://www.ibmbigdatahub.com/blog/why-only-one-5-vs-big-data-really-matters (26.02.2018)

mobilsicher. (2018). Das Infoportal für mehr Sicherheit auf Smartphone und Tablet. Webseite. Abgerufen von: https://mobilsicher.de (26.02.2018)

Morgner, P. & Zinaida Benenson, Z. (im Erscheinen). Exploring Security Economics in IoT Standardization Efforts.

Moynihan, T. (2015). This Toy Dinosaur uses IBM's Watson as a brain. Abgerufen von: https://www.wired.com/2015/08/toy-dinosaur-uses-ibms-watson-brain/ (26.02.2018)

Mozilla Foundation. (2017). *priacy not included. A Guide to Make Shopping for Connected Gifts Safer, Easier, and Way More Fun. Abgerufen von: https://advocacy.mozilla.org/en-US/privacynotincluded (26.02.2018)

Mücke, Sturm & Company. (2015). Attack of the Future Smart Home Giants - The fight of Apple, Google, Amazon, and others for the most customer centric ecosystem. Abgerufen von: http://www.muecke-sturm.de/wp-content/uploads/Smart-Home-Giganten.pdf (26.02.2018)

Nickel, O. (2018). Viele Android-Apps kollidieren mit kommendem EU-Datenschutz. Golem. Abgerufen von: https://www.golem.de/news/marktforschung-viele-android-apps-kollidieren-mit-kommendem-eu-datenschutz-1801-132302.html (20.02.2018).

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.

Philips. (2017). Datenschutzhinweis für Kunden, Verbraucher und Geschäftspartner. Abgerufen von: https://www2.meethue.com/de-de/support/datenschutzhinweis (26.02.2018)

Porup, J.M. (2016). "Internet of Things" security is hilariously broken and getting worse. Abgerufen von: https://arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/ (26.02.2018)

PwC. (2017). Digitale Assistenten Bevölkerungsbefragung 2017. Abgerufen von: https://www.pwc.de/de/consulting/management-consulting/pwc-befragung-digitale-assistenten-2017.pdf (20.02.2018)

OECD. (2017). OECD Science, Technology and Industry Scoreboard 2017: The digital transformation, OECD Publishing, Paris.

O'Toole, J. (2014). Cops can access your connected home data. CNN. Abgerufen von: http://money.cnn.com/2014/06/16/technology/smart-home-footage/index.html (26.02.2018)

Otto GmbH & Co KG. (2017). DATENSCHUTZ KOMPAKT. Abgerufen von: https://www.otto.de/shoppages/service/about/datenschutzinformation/aboutprivacyneedtoknow (26.02.2018)

Rapid7. (2016). Comments to "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things". Docket No. 160331306–6306–01. Abgerufen von: https://www.ntia.doc.gov/files/ntia/publications/rapid7_comments_to_ntia_iot_rfc_-_jun_2_2016.pdf (26.02.2018)

Raspin, J. (2016). Smart & Connected Homes: Key Trends and Opportunities.

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. Journal of Consumer Affairs, 39(2), 339-362.

Ronen, E., & Shamir, A. (2016). Extended functionality attacks on IoT devices: The case of smart lights. In Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016 (pp. 3–12).

Ronen, E., O'Flynn, C., Shamir, A. & Weingarten, A.-O. (2017). IoT Goes Nuclear: Creating a ZigBee Chain Reaction. Abgerufen von: http://iotworm.eyalro.net (26.02.2018)

Sachverständigenrat für Verbraucherfragen (SVRV). (2017). Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Abgerufen von: http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souveränität_.pdf (26.02.2018)

Saizmaa, T., & Kim, H. C. (2008). Smart home design: Home or house? Proceedings - 3rd International Conference on Convergence and Hybrid Information Technology, ICCIT 2008, 1, 143–148.

Schmidt, J. (2016). Großstörung bei der Telekom: Was wirklich geschah. Heise online. Abgerufen von: https://www.heise.de/security/meldung/Grossstoerung-bei-der-Telekom-Was-wirklich-geschah-3520212.html (26.02.2018)

Schneier, B. (2017). Security and Privacy Guidelines for the Internet of Things. Schneier on Security. Abgerufen von: https://www.schneier.com/blog/archives/2017/02/security_and_pr.html (26.02.2018)

Schulze-Sturm, S. (2016). Blickwinkel Smart Home – Studien aus Angebots- und Nachfragesicht. In Begleitforschung Mittelstand-Digital. (2016). Wissenschaft trifft Praxis – Neue Formen des Home Experience Design. Abgerufen von: http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/wissenschaft-trifft-praxis-ausgabe4,property=pdf,bereich=md,sprache=de,rwb=true.pdf (12.01.2018)

Shodan. (2018). Explore tag: webcam. Abgerufen von: https://www.shodan.io/explore/tag/webcam (26.02.2018)

Silverman, C. (2015). 7 Creepy Baby Monitor Stories That Will Terrify All Parents. Abgerufen von: https://www.buzzfeed.com/craigsilverman/creeps-hack-baby-monitors-and-say-terrifying-thing (26.02.2018)

Sist, M. (2017). Amazon's Alexa is our robot Social Justice Warrior and we, the libs, have won. Abgerufen von: https://www.newstatesman.com/science-tech/technology/2017/12/amazon-s-alexa-our-robot-social-justice-warrior-and-we-libs-have-won (26.02.2018)

SmartHome Initiative Deutschland. (2017). Smart Living Kompendium - SmartHome, Smart Building, Smart Grid, Smart City, Smart Living an Beispielen erklärt.

Sønstebø, D. (2017). IOTA Data Marketplace. Abgerufen von: https://blog.iota.org/iota-data-marketplace-cb6be463ac7f (26.02.2018)

Spindler, G. (2007). Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Studie im Auftrag des BSI. Abgerufen von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf (26.02.2018)

Splendid Research. (2017). Smart Home Monitor 2017 - Repräsentative Umfrage zum Status quo und Entwicklung von Smart Home in Deutschland.

Stanislav, M. & Beardsley, T. (2015). HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities. Rapid7. Abgerufen von: https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf (26.02.2018)

Statista. (2016a). Statista –Umfrage „Wie ist Ihre Einstellung zum vernetzten Wohnen/ zu Smart-Home- Anwendungen insgesamt?" Abgerufen von: https://de.statista.com/statistik/daten/studie/164392/umfrage/kenntnis-von-connected-home-und-heimvernetzung-nach-alter/ (26.02.2018)

Statista. (2016b). Statista-Umfrage "Wie gut sind Sie selber über das Thema Smart-Home informiert?". Abgerufen von: https://de.statista.com/statistik/daten/studie/591831/umfrage/grad-der-informiertheit-zum-thema-smart-home-deutschland/ (26.02.2018)

Statista. (2016c). Statista-Umfrage "Wie ist Ihre Einstellung zum vernetzten Wohnen/zu Smart-Home-Anwendungen insgesamt?" Abgerufen von: https://de.statista.com/statistik/daten/studie/317965/umfrage/umfrage-zum-interesse-an-smart-home-technologien-in-deutschland/ (26.02.2018)

Stiftung Datenschutz. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Stiftung Datenschutz. Abgerufen von: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf (26.02.2018)

Stiftung Warentest. (2017). Pokémon Go, Minecraft & Co: So werden Kids mit Apps abgezockt. Abgerufen von: https://www.test.de/Pokemon-Go-Minecraft-Co-So-werden-Kids-mit-Apps-abgezockt-5197290-0/ (23.02.2018)

Stiftung Warentest. (2018). Lovoo, Tinder & Co: Wie schludrig Dating-Apps mit Daten umgehen. Abgerufen von: https://www.test.de/Datensicherheit-bei-Dating-Apps-im-Test-5286506-0/ (23.02.2018)

Swant, M. (2017). Facebook Raked in $9.16 Billion in Ad Revenue in the Second Quarter of 2017. Abgerufen von: http://www.adweek.com/digital/facebook-raked-in-9-16-billion-in-ad-revenue-in-the-second-quarter-of-2017/ (26.02.2018)

Tanczer, L., Parkin, s., Danezis, G., & Patel, T. (2018). Gender and IoT. Abgerufen von: https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/dpl-projects/gender-and-iot (26.02.2018)

Thaler, R. H., & Sunstein, C. R. (2009). Nudge: Wie man kluge Entscheidungen anstößt. Ullstein eBooks.

TÜV Informationstechnik GmbH. (2006). Nachweis der Datenschutzkonformität. Abgerufen von: https://www.tuvit.de/de/leistungen/datenschutz/trusted-site-privacy/ (26.02.18)

Unabhängiges Datenschutzzentrum Saarland. (2017). 26. Tätigkeitsbericht. Abgerufen von: https://datenschutz.saarland.de/fileadmin/tberichte/tb26.pdf (26.02.2018)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). (2014). Datenschutz-Gütesiegel beim ULD. Abgerufen von: https://www.datenschutzzentrum.de/guetesiegel/ (26.02.18)

U.S. Senate. (2018). Internet of Things (IoT) Cybersecurity Improvement Act of 2017. Abgerufen von: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text (26.02.2018)

Verbraucher Initiative e.V. (Bundesverband). (2018). Label-online. Webseite. Abgerufen von: https://label-online.de (26.02.2018)

Wendehorst, C. (2016). Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge. Abgerufen von: http://www.svr-verbraucherfragen.de/wp-content/uploads/Wendehorst-Gutachten.pdf (26.02.2018)

Whittaker, Z. (2017). Sonos says users must accept new privacy policy or devices may "cease to function". ZDNet. Abgerufen von: http://www.zdnet.com/article/sonos-accept-new-privacy-policy-speakers-cease-to-function/ (26.02.2018)

Wissenschaftliche Dienste des Deutschen Bundestages (2013). Aktueller Begriff Big Data. Abgerufen von: https://www.bundestag.de/blob/194790/c44371b1c740987a7f6fa74c06f518c8/big_data-data.pdf (26.02.2018)

Wittes, B., Poplin, C., Jurecic, Q. & Spera, C. (2016). Sextortion: Cybersecurity, teenagers, and remote sexual assault. Center for Technology Innovation at Brookings.

Wolfe, J. (2017) Roomba vacuum maker iRobot betting big on the 'smart' home. Reuters. Abgerufen von: https://www.reuters.com/article/us-irobot-strategy/roomba-vacuum-maker-irobot-betting-big-on-the-smart-home-idUSKBN1A91A5 (26.02.2018)

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, 444-458.

Zalando SE. (2016). Datenschutz-One-Pager. Abgerufen von: https://a1276.ztat.net/lpo/zalando/1_cro/2017/02/BIT-129/zalando-onepager.pdf (26.02.2018)

Zigbee. (2018). Zigbee Light Link. Smart, easy-to-use lighting control designed for consumers. Abgerufen von: http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbee-light-link/ (26.02.2018)

Zukunftsinstitut. (2015). Connected Home. Digitale Vernetzung und das Wohnen von morgen. Eine Trendstudie des Zukunftsinstituts powered by Siemens Hausgeräte. Abgerufen von: https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/Connected_Home_Trendstudie_Zukunftsinstitut.pdf (26.02.2018)

Zwetsloot, G. I. J. M., Zwanikken, S., & Hale, A. (2011). Policy expectations and the use of market mechanisms for regulatory OSH certification and testing regimes. Safety Science, 49(7), 1007–1013.

# 9 APPENDIX

## 9.1 EXPERTENINTERVIEWS

Für die Experteninterviews wurde mit den folgenden Vertretern aus Wirtschaft, Wissenschaft, Zukunftsforschung und Verbänden gesprochen.

Dr. Thomas Keiser
Vorstand, Smart Home Initiative Deutschland e.V.

Prof. Dr.-Ing. Wolfgang Maaß
Wissenschaftlicher Direktor, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)
Lehrstuhlinhaber des Lehrstuhls für Betriebswirtschaftslehre, insbesondere Wirtschaftsinformatik im Dienstleistungsbereich, Universität des Saarlandes

Thomas Rockmann
Vice President, V TI I Product Innovation, Deutsche Telekom AG

Michael Schidlack
Chief Strategy Officer, digitalSTROM AG

Willi Schroll
Geschäftsführer, strategiclabs – Foresight Services

Robert Spanheimer
Referent Smart Grids & Smart Home, Bitkom e.V.

## 9.2 INFORMATIONELLE SELBSTBESTIMMUNG – AUSGEWÄHLTE ANWENDUNGEN

| Produkt |
|---|
| Beleuchtung |
| Philips Hue |
| Osram Lightify |
| Ikea Tradfry |
| Yeelight |
| TP-Link Kasa |
| MiPow Playbulb |
| LIFX |
| Sengled Pulse |
| Videokameras |
| Netgear Arlo |
| Bosch Smart Camera |
| mydlink |
| Nest Cam |
| Ring Always Home |
| SkyBell |
| Philips In.Sight |
| Rogers Smart Home Monitor |
| Zmodo |
| Logitech Alert |
| Sprachassistenten |
| Amazon Alexa |
| Google Assistant |
| Microsoft Cortana |
| Apple Siri |

Tabelle 12: Ausgewählte Anwendungen, die bei der Analyse der Datenschutzerklärungen berücksichtigt wurden