forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Forschungsbericht

SMART-TV UND PRIVATHEIT

BEDROHUNGSPOTENZIALE UND HANDLUNGSMÖGLICHKEITEN

Forschungsbericht

SMART-TV UND PRIVATHEIT

BEDROHUNGSPOTENZIALE UND HANDLUNGSMÖGLICHKEITEN

Autorinnen und Autoren:
Marco Ghiglieri[1], Marit Hansen[2], Maxi Nebel[3], Julia Victoria Pörschke[2], Hervais Simo Fhom[1(*)]

(1) Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt
(2) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(3) Universität Kassel, Institut für Wirtschaftsrecht, Fachgebiet Öffentliches Recht, insb. Umwelt- und Technik-recht

(*) Korrespondierender Autor: hervais.simo@sit.fraunhofer.de

Herausgeber:
Peter Zoche, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner

Inhalt

Kurzfassung

Moderne Fernsehgeräte, so genannte Smart-TVs, können eine Vielzahl von Funktionen bieten, die bisher nur von herkömmlichen Computersystemen bekannt waren. Dies sind zum Beispiel die Nutzung von IP-Telefonie, das Abspielen von Videos oder auch das Surfen im Internet. Diese neuartigen Vernetzungsmöglichkeiten versprechen den Nutzenden zahlreiche Vorteile, bergen zugleich jedoch auch neue Gefahren für den Datenschutz und die Privatheit. Neue, innovative Konzepte und Technologien sind unumgänglich, um Nutzende, Unternehmen, aber auch Dritte, vor Missbrauch, Schadprogrammen und anderen Gefahren im Umgang mit Smart-TV zu schützen.

Der vorliegende Beitrag richtet sich vor allem an juristische Berater und technische Entwickler. Hierbei wird ein Überblick über die Chancen und wachsenden Möglichkeiten im Bereich Smart-TV gegeben; die damit verbundenen Risiken für die Persönlichkeitsrechte der Nutzenden werden herausgearbeitet. Nach einer Übersicht über den technischen Hintergrund von Smart-TV werden die beteiligten Akteure und Komponenten erläutert. Anschließend werden verschiedene Angreifermodelle und mögliche Angriffsvektoren erörtert. Im Rahmen der grund- und datenschutzrechtlichen Rahmenbedingungen werden Bedrohungsszenarien abgeleitet, die sich für die informationelle Selbstbestimmung der Nutzenden ergeben; außerdem wird die datenschutzrechtliche Zulässigkeit der Datenverarbeitungsvorgänge im Rahmen der Smart-TV-Nutzung geprüft. Anhand des herausgearbeiteten Befundes zeigen die Autorinnen und Autoren schließlich exemplarisch Methoden und Schutzmaßnahmen auf, wie bestehende Smart-TV-Systeme sowohl technisch optimiert als auch rechtlich zulässig gestaltet werden können. Dies erfolgt anhand des „Privacy by Design"-Ansatzes und im Lichte der ausgewählten Datenschutz-Gewährleistungsziele der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit.

1 Einleitung

Die Vernetzung verschiedener Geräte im Haushalt nimmt von Tag zu Tag zu.[1] Eine stetig wachsende Anzahl derartiger Geräte hat die Möglichkeit, Daten über ihre Umgebung zu erheben und zu verarbeiten, miteinander zu kommunizieren, sowie über das Internet oder das lokale Netzwerk ferngesteuert oder kontrolliert zu werden. Im Bereich von Entertainment-Geräten wie internetfähigen Set-Top-Boxen, Spielekonsolen und Blu-Ray-Playern ist diese Entwicklung bei modernen Fernsehgeräten besonders deutlich zu sehen. Jüngste Fortschritte in der digitalen Rundfunktechnik, schnelle Internetzugänge und Web-Technologien ermöglichen den nächsten logischen Schritt der Fernsehtechnik: die Konvergenz zwischen Internet und Fernsehen. Herzstück eines solchen Schrittes ist das Smart-TV. Als *Smart-TV* werden Fernsehgeräte bezeichnet, die über zusätzliche Funktionen und Schnittstellen für Internet- und Netzwerkanschluss, USB sowie Speicherkarten verfügen. Neben dem Empfang von Rundfunksignalen können auch interaktive (sender- bzw. programmbezogene) Inhalte und Dienste aus dem Internet empfangen und abgebildet werden. Zusätzlich zum herkömmlichen Fernsehen werden durch die Funktion *Hybrid Broadcast Broadband TV* (HbbTV) Medieninhalte aus dem Internet zur laufenden Sendung oder damit zusammenhängende Inhalte aus einer Mediathek zur Verfügung gestellt. Ein Smart-TV-Gerät bietet neben der klassischen Nutzung als Fernsehgerät auch die Möglichkeit, im Internet zu surfen, E-Mails zu lesen, Bilder anzuschauen, Musik zu hören, Videoinhalte aus dem Internet abzurufen oder über Video-Telefonie zu kommunizieren.[2] Durch die Netzwerkanbindung können Smart-TV-Geräte häufig über Smartphones oder Tablets gesteuert werden. In Deutschland wird bis Ende 2016 die Anzahl aktiv vernetzter TV-Geräte auf voraussichtlich 20 Millionen Geräte ansteigen[3], davon über 13 Millionen HbbTV-fähige Geräte[4]. Ein ähnlich deutlicher Trend ist in den USA zu beobachten.[5]

Moderne Smart-TV-Geräte gelten dementsprechend zunehmend als Multimedia-Center, die externe Kommunikations- und Fernsehdienste mit anderen „intelligenten" elektronischen Haushaltgeräten verbinden können. Neben den sich ergebenden wirtschaftlichen Potentialen – dank neuer interaktiver TV-Geschäftsmodelle für Geräteherstellter, TV-Sender bzw. TV-Anstalten, Content-Anbieter sowie Infrastrukturbetreiber und Werbetreibende – zielt eine derartige Konvergenz zwischen Internet und TV auf hohen Nutzerkomfort und einfache Bedienbarkeit ab. Durch die erweiterte Funktionalität von Smart-TV und den unterschiedlichen bei der Bereitstellung und dem Betrieb von Smart-TV-Angeboten beteiligten Akteuren entstehen jedoch auch Risiken für die Selbstbestimmung der Nutzenden. Dieses wird durch die aus Nutzersicht unübersichtliche Dienstleistungsstruktur der beteiligten Akteure und die fehlende Transparenz über eine mögliche Verbindung mit dem Internet und des daraus resultierenden Datenverkehrs verschärft. So wissen mehr als ein Fünftel der Smart-TV-Nutzenden nicht, ob ihr Smart-TV-Gerät mit dem Internet verbunden ist, und fast die Hälfte der Nutzenden ist nicht über die Möglichkeiten von HbbTV informiert.[6]

Dieser Beitrag gibt einen Überblick über die mit Smart-TV verbundenen Techniken und Akteure und zeigt die daraus resultierenden Risiken und Implikationen für die Persönlichkeitsrechte der Nutzenden und mögliche Handlungsoptionen für datenschutzkon-

1 *Bitkom (2014).*
2 *PricewaterhouseCoopers (2013).*
3 *Statista (2011a); Sattler (2011).*
4 *Statista (2011b).*
5 *Emarketer (2013); StrategyAnalytics (2014).*
6 *PricewaterhouseCoopers (2013).*

forme Smart-TV-Systeme auf. Der Beitrag gliedert sich wie folgt: Zunächst wird ein Überblick über die technischen Möglichkeiten von Smart-TV und die bei der Nutzung von an Smart-TV-Systemen beteiligten Akteure und in das System integrierte Komponenten (Abschnitt 2) gegeben.[7] Auf dieser Grundlage werden verschiedene Angriffsvektoren dargestellt (Abschnitt 3) und das Bedrohungspotential für die informationelle Selbstbestimmung (Abschnitt 4) diskutiert. Daran schließen sich die rechtlichen Rahmenbedingungen für die verschiedenen Akteure sowohl auf grundrechtlicher als auch datenschutzrechtlicher Sicht an (Abschnitt 5). Auf dieser Basis werden in einem Ausblick einige Maßnahmen erläutert, die notwendig sind, um Smart-TV-Systeme technisch optimiert und datenschutzkonform zu gestalten (Abschnitt 6).

[7] Eine frühere Version von Abschnitt 2-4 ist erschienen als: *Ghiglieri/Lange/Simo/Waidner (2015).*

2
Technischer Hintergrund des Smart-TV

Dieses Kapitel legt die Grundlage für die in diesem Forschungsbericht angestrebte Diskussion um geltende rechtliche Rahmenbedingungen und mögliche Bedrohungspotentiale vor. Im ersten Abschnitt des Kapitels werden typische Merkmale des Smart-TVs vorgestellt. Die im Smart-TV-System angebundenen Akteure und Komponenten werden im Abschnitt 2.2 vorgestellt. Abschnitt 2.3 fasst alle im Smart-TV-Kontext anfallenden Datentypen zusammen.

2.1 Smart-TV: Ein vernetzter „Fernsehcomputer“[8]

Technische Ausstattung: Anders als bei konventionellen TV-Geräten können moderne „intelligente“ Fernsehgeräte (Smart-TV) direkt mit dem Internet über LAN oder WLAN verbunden werden, ohne dass ein Anschluss an einen externen Rechner oder an eine Set-Top-Box notwendig ist. Ähnlich wie mobile Endgeräte sind Smart-TV-Geräte vernetzte Plattformen, die mit leistungsstarken Prozessoren sowie unterschiedlichen, zum Teil eingebauten Steuerungs- und Bewegungssensoren bestückt sind. Die Internetfunktionalitäten eines Smart-TV-Geräts können in herstellerabhängige und -unabhängige Merkmale unterteilt werden. Der HbbTV-Standard ist beispielsweise eine herstellerunabhängige Funktion, die von immer mehr Fernsehgeräteherstellern implementiert wird. Moderne Smart-TV-Geräte werden außerdem mit einer Vielzahl von Sensoren ausgestattet. Dazu gehören neben Mikrofonen und Kameras auch Bewegungs-, Temperatur- und Luftfeuchtigkeitssensoren. Diese stellen Rückkanäle zur Verfügung, die dem Nutzenden die Interaktion und Partizipation am TV-Programm sowie die Nutzung von Web-Anwendungen wie Sprach-Chat-Diensten oder sozialen Netzwerken ermöglichen.

HbbTV-Standard: Die Verknüpfung von Rundfunk mit interaktiven Online-Diensten auf Smart-TV-Geräten ist mit gängigen Web-Technologien möglich. Prominentes Beispiel ist der offene internationale Standard Hybrid Broadcast Broadband TV (HbbTV).[9] HbbTV war ursprünglich eine pan-europäische Initiative zur Harmonisierung der Rundfunk- und Breitband-Bereitstellung von Multimediainhalten durch internetfähige Fernseher. Die HbbTV-Spezifikation[10] basiert auf der Erweiterung bestehender Web-Technologien und Standards wie JavaScript, HTML und CSS. Mittlerweile wird der HbbTV-Standard über Europa hinaus als ernsthafte Alternative und Ergänzung bestehender Rundfunkstandards betrachtet.[11] Der HbbTV-Standard eröffnet die Möglichkeit, neben linearem Fernsehen (herkömmliches Programmfernsehen) den Zuschauer sowohl zusätzliche webbasierte Medienangebote (zum Beispiel Werbung, Wetterberichte oder Teletext) zum laufenden und zukünftigen Programm als auch On-Demand-Dienste zur Verfügung zu stellen. HbbTV-Dienste werden in der Regel über die rote Taste auf der Fernbedienung aufgerufen, weshalb sie auch als „Red Button“-Dienste bezeichnet werden. Anbieter von HbbTV-Diensten und die über HbbTV angebotenen Inhalte sind entweder die jeweiligen Programmveranstalter oder die Entertainment-Provider. Für die Werbetreibenden und TV-Sender bestehen die Vorteile des „Red Button“ mit HbbTV beispielsweise in der Möglichkeit, völlig neue interaktive TV-Geschäftsmodelle zu etab-

8 Zum definitorischen Hintergrund des Begriffs “Fernsehcomputer” vgl. *Karaboga/Matzner/Morlok/Nebel/Ochs/von Pape/Pittroff/Pörschke/Schütz/Simo (2015).*
9 *ETSI (2012).*
10 *ETSI (2012).*
11 *Deutsche TV Plattform (2014).*

lieren.[12] Zudem haben die Eigenschaften von HbbTV das Potenzial, personalisierte Empfehlungen für Shows und webbasierte Inhalte sowie die Realisierung des Nachfolgesystems für den heutigen Teletext zu ermöglichen.[13]

Erweiterbare Plattform: Die Integration von Web-Technologien in Fernsehgeräte ermöglicht einen Zugriff auf Inhalte des World Wide Web typischerweise sowohl durch einen (zum Teil rudimentären) Web-Browser als auch durch unterschiedliche Kommunikationsdienste wie Musik-Player, E-Mail, Spiele, Social Media, VoIP-Dienste und Bezahlungsdienste einschließlich Online-Banking. Web-Browser und Kommunikationsdienste werden den Nutzenden in Form von Apps, das heißt kleinen herunterladbaren Softwareprogrammen, die direkt auf dem Fernseher ausführbar sind und Zugang zu unterschiedlichen Diensten wie Spielen, Videos, News usw. ermöglichen, zur Verfügung gestellt. Ähnlich wie auf Smartphones bieten Apps die Möglichkeit zur Erweiterung der Funktionalität eines Smart-TV-Geräts. Smart-TV-Apps werden überwiegend vorinstalliert, können aber auch von Online-App-Stores heruntergeladen oder von externen Speichermedien installiert werden. Die meisten Fernsehgerätehersteller betreiben einen eigenen App-Store und bieten in aller Regel Apps für iOS- oder Android-Geräte an. Diese ermöglichen unter anderem eine Echtzeit-Synchronisierung zwischen den Smart-TV-Geräten und einer mobilen App auf dem Smartphone oder Tablet des Zuschauers. Das Konzept ist unter dem Begriff „Second-Screen-Ansatz“[14] bekannt und gilt als wichtiges Instrument, um eine erweiterte Nutzung von neuen Diensten und zusätzlichen senderbezogenen Multimedia-Inhalten zu realisieren. Auch mit HbbTV ist Second-Screen möglich.[15]

2.2 Beteiligte Akteure und Komponenten

Im Folgenden werden die Akteure und Architekturkomponenten im Smart-TV-System konkretisiert und ausgearbeitet. fasst das allgemeine Systemmodell und die Interaktionen zwischen den einzelnen Komponenten zusammen.

Smart-TV-Geräte stellen die Kernkomponente der Architektur dar. Heutige Smart-TV-Geräte bestehen aus einer Vielzahl von integrierten Sensoren, die im Zusammenspiel mit einer in der Regel proprietären Firmware (oder einem Betriebssystem) sowohl interaktives Fernsehen als auch verschiedene Funktionalitäten realisieren, unter anderem Sprach- und Gestensteuerung. Dank zahlreicher Schnittstellen wird die Konnektivität mit anderen im Heimnetzwerk angeschlossenen Geräten wie Smartphones oder Tablets unterstützt. Die Unterstützung des HbbTV-Protokolls in Smart-TV-Geräten ermöglicht es den TV-Sendern, hybride Zusatzangebote in das laufende TV-Programm einzubetten. Zudem bietet ein Smart-TV-Gerät die Möglichkeit, im Internet zu surfen, Bilder anzuschauen, Musik zu hören oder Videotelefonie zu betreiben. Smart-TV-Geräte als IT-Plattformen werden in der Regel von den Geräteherstellern, zum Beispiel Samsung, Sony oder LG, aus der Ferne und in regelmäßigen Zeitabständen oder bei Bedarf aktualisiert.

TV-Sender bieten Fernsehprogramme in Form von Sendungen sowie zusätzliche Online-Inhalte als Zusatzmaterial für einzelne Sendungen an. Sie sind für das HbbTV-Angebot verantwortlich. Um im Zusammenhang mit HbbTV-Angeboten personalisierte Inhalte oder Empfehlungen einblenden zu können, sammelt und bewertet der TV-Sender Details über das Nutzungsverhalten der Zuschauer.

12 *BLM (2012).*
13 *hbbtv-infos.de (2014).*
14 *Kuri*, CE Week: Der Kampf um den „Second Screen“, heise online vom 28.6.2013, http://www.heise.de/-1902324.
15 *IRT GmbH (2014).*

Smart-TV-Nutzende umfassen alle die ein Smart-TV-Gerät verwenden, um neben traditionellen Rundfunkdiensten auch zusätzliche, über das World Wide Web erreichbare interaktive Medieninhalte zu konsumieren. Einbezogen werden können auch juristische Personen, die ihre Räumlichkeiten mit Smart-TV ausstatten, zum Beispiel Arbeitgeber, Gastronomie- und Veranstaltungsbetriebe (Hotels oder Cafés).

Gerätehersteller und Servicetechniker kooperieren mit führenden Soft- und Hardwareherstellern und Anbietern interaktiver Inhalte, um Fernsehgeräte anzubieten, die den besonderen Anforderungen der Smart-TV-Angebote genügen. Sie machen sich die Hard- und Firmware-Merkmale der Geräte sowie einen heute bundesweit relativ weit verbreiteten breitbandigen Internetzugang zunutze, um eine Fernwartung (inklusive Update der Firmware auf dem Gerät) durchzuführen. Ähnliche Wartungstätigkeiten werden bei Bedarf durch einen (Vertrags-)Servicetechniker erledigt, für den der Hersteller spezielle Schnittstellen und Wartungsoptionen auf dem Smart-TV vorgesehen hat. Konfigurationsdetails des Smart-TV-Geräts, Statistiken über ihre Nutzung und die bei der (Fern-)Wartungsarbeit anfallenden Daten werden gegebenenfalls – vertraglich festgelegt – mit weiteren Hardwareherstellern und Inhaltsanbietern geteilt.

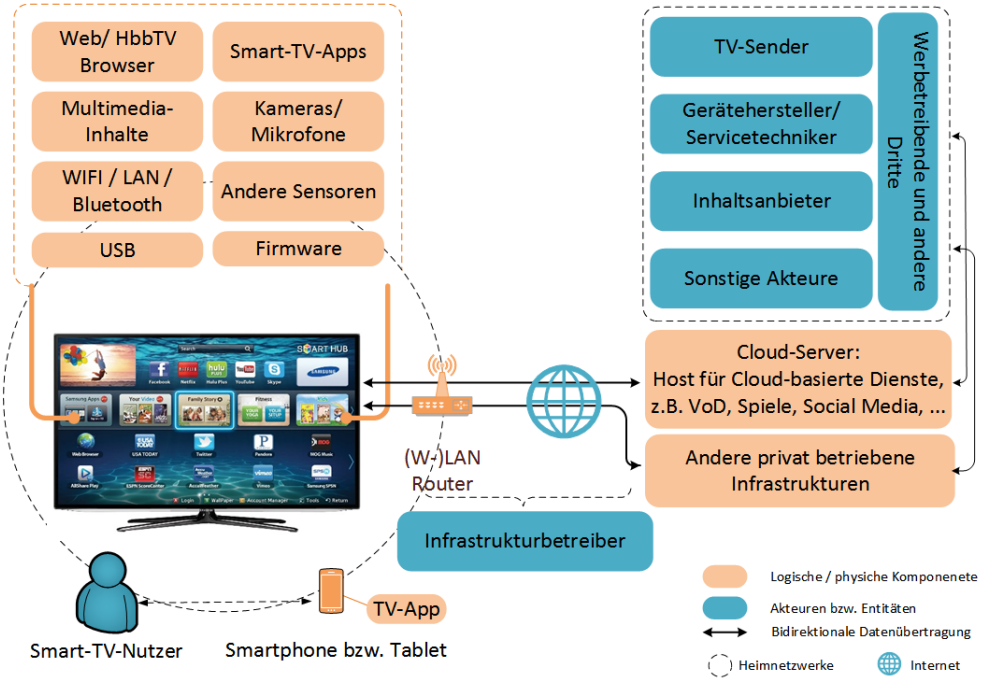

Abb. 01 Akteure und Architekturkomponenten im Smart-TV-System

Inhaltsanbieter stellen Apps mit redaktionellen und sonstigen Inhalten zur Verfügung. In der Regel tragen sie sowohl die redaktionelle als auch rechtliche Verantwortung für die Inhalte der Applikationen und Programme, die den Nutzenden angeboten werden. Inhaltsanbieter können den Zugang zu interaktiven Online-Inhalten entweder durch einen Zugangsanbieter (wie Kabelnetzbetreiber, Telekommunikationsunternehmen oder App-Store) ermöglichen oder selbst die notwendige Zugangsinfrastruktur betreiben. TV-Sender, Gerätehersteller und Anbieter von „Fremd-Anwendungen" wie zum Beispiel Online-Spiele oder Streamingdienste können dementsprechend unter Umständen auch als mögliche Inhaltsanbieter betrachtet werden. Darüber hinaus integrieren Plattformen der Inhaltsanbieter zunehmend Empfehlungsdienste mit dem Ziel personalisierter Inhaltsempfehlungen optimal anbieten zu können.[16]

16 *Lee/Kaoli/Huang (2014).*

Infrastrukturbetreiber sind Betreiber von Kabelnetzen und Telekommunikationsunternehmen. Sie stellen oftmals gegen einen pauschalen monatlichen Tarif die technische Infrastruktur zur Verfügung, die notwendig ist, um Kommunikation zwischen sämtlichen Akteuren zu ermöglichen. In der Regel wird ein Zugriff auf die Infrastruktur durch eine Registrierung des Smart-TV-Nutzers vorausgesetzt. Bei jeder Nutzung der Infrastruktur müssen sich Nutzer mit einem personalisierten Benutzerkonto anmelden.

Kommunikationsnetze umfassen alle öffentlichen und privaten Kommunikationsnetze. Sie sind Voraussetzungen für den Informationsaustausch sowohl zwischen den Smart-TV-Gerät und weiteren „intelligenten" elektronischen Geräten innerhalb von Heimnetzwerken als auch für die Kommunikation mit externen Parteien, etwa dem Gerätehersteller, dem Infrastrukturbetreiber, den Fernsehanstalten oder Werbetreibenden.

Werbetreibende erhalten durch Smart-TV und die damit verbundenen Second-Screen-Technologien die Möglichkeit, bestimmte Zuschauergruppen gezielt zu adressieren und mit ihnen über die Dauer des im Fernsehen ausgestrahlten Werbespots hinaus zu interagieren. Aus Sicht der Werbetreibenden birgt dieser Trend das Potenzial, die Interaktion der Zuschauer mit den Werbeinhalten besser zu erfassen und auszuwerten. Die dabei anfallenden Daten werden unter Umständen mit den Inhaltsanbietern und/oder den TV-Sendern geteilt.

Sonstige Akteure werden einbezogen, um Geschäftsmodelle in HbbTV-Anwendungen mit elektronischen Bezahlverfahren zu unterstützen und zusätzliche, gegebenenfalls kostenpflichtige Smart-TV-Inhalte anzubieten. Beispiele sind etwa Online-Bezahldienste wie Paypal (www.paypal.com/) und Kreditkartenunternehmen wie Visa (www.visa.de/).

2.3 Bei Smart-TV-Nutzung erhebbare und ableitbare Daten

Bei der Verwendung eines Smart-TV-Geräts fallen vielfältige Daten an. Diese können entweder direkt vom Nutzenden eingegeben werden oder durch die Nutzung des Geräts anfallen. Aus diesen Daten lassen sich darüber hinaus weitere Daten ableiten, die neue persönliche Informationen über den jeweiligen Nutzenden zulassen. Diese werden im Folgenden vorgestellt.

Konto- und Registrierungsdaten: Einige Dienste auf Smart-TV-Systemen erfordern eine Registrierung des Geräts online sowie gültige Nutzerkonten (plus Anmeldedaten und Profildaten) bei den infrage kommenden Diensten. Beim Verknüpfen des Smart-TV-Geräts mit einem Account können die jeweiligen Diensteanbieter[17] verschiedene Daten, zum Beispiel Name, Geburtsdatum, Geschlecht, Adresse und gegebenenfalls Zahlungsinformationen des Benutzers, erheben. Darüber hinaus werden oft Benutzername und Kennwort für den wiederholten Zugriff auf personalisierte Online-Dienste für den komfortablen Umgang mit der Seite im Speicher des Smart-TV-Geräts gespeichert. Eine Nutzung des Smart-TV-Geräts ohne Konto- und Registrierungsdaten ist in der Regel möglich, aber sobald echte „Smart"-Dienste, wie zum Beispiel personalisierte Apps, genutzt werden sollen, muss häufig eine Anmeldung bei einem Dienst erfolgen.

Fernsehverhaltensdaten: Gemeint sind Daten über die Interaktion zwischen dem Smart-TV-Gerät und dem Nutzenden, Details über die für bzw. vom Nutzenden auf dem Fernseher aktivierten Inhalte, Apps oder Dienste sowie Informationen über ihm zur

17 Diensteanbieter sind gemäß § 2 Satz 1 TMG all diejenigen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang dazu vermitteln. Typische Diensteanbieter sind TV-Sender, Streamingdienste oder Spiele-Anbieter; aber auch Geräte-Hersteller bieten Telemedien an, wenn sie etwa Updates für das Smart-TV-Gerät zur Verfügung stellen.

Verfügung stehende TV-Kanäle. Fernsehverhaltensdaten beziehen sich ebenfalls auf Informationen über die Interaktion des Nutzenden mit verfügbaren moderierten Inhalten und sonstigen interaktiven Online-Diensten wie Video-on-Demand. Diese Informationen umfassen unter anderem, welche TV-Programme angesehen werden, Anfragen und Suchbegriffe nach Inhalten (zum Beispiel in der Mediathek), das angeklickte Werbematerial, die Zeiten der Nutzung oder wie lange und welche Steuerungsaktionen (etwa Play, Stop, Pause, Fast Forward etc.) der Zuschauer beim Konsumieren bestimmter audiovisueller Inhalte oder non-linearen Online-Medien betätigt hat. Zwei weitere Typen von Fernsehverhaltensdaten sind Daten über das Browsing-Verhalten bzw. die Browsing-Historie des Nutzenden und die durch Smart-TV-Sensoren erfassten Video-, Bilder-, und Stimmaufnahmen von Hausbewohnern und Besuchern. Aus den Sensordaten können unter Umständen biometrische Daten, wie Gesichtsgeometrie, abgeleitet werden. Sensordaten werden zunehmend genutzt, um ein noch mehr auf die Personen zugeschnittenes TV-Erlebnis zu schaffen, zum Beispiel durch Gesichts- und Stimmerkennung.[18] Fernsehverhaltensdaten werden durch den Fernseher und relevante Apps kontinuierlich erfasst und an externe Entitäten, zum Beispiel Diensteanbieter oder Werbetreibende, übertragen, sobald sich das Fernsehgerät mit dem Internet verbinden. Auch bei HbbTV werden Fernsehverhaltensdaten erfasst und typischerweise schon in dem Moment, in dem die Verfügbarkeit von HbbTV eingeblendet wird, an den Sender übertragen. Google Analytics und andere Trackingdienstleister werden teilweise ebenfalls genutzt.[19]

Gerätespezifische Daten: Zudem können (Hardware-)Merkmale des Smart-TV-Geräts erfasst werden. Dazu gehören unter anderem der Name des Geräteherstellers, die Modellbezeichnung und gegebenenfalls die Version des Geräts sowie der Typ, die Version des Betriebssystems oder der Firmware. Hinzu kommen Details über die Art der Netzwerkschnittstelle bzw. Netzwerkverbindung (WLAN, LAN, Bluetooth), die Netzwerkadresse (MAC- oder IP-Adresse) des Fernsehgeräts, Informationen über eingebaute Sensorgeräte und gegebenenfalls der eindeutige Fernsehgeräte-Identifier (auch „Unique Device ID"). Einbezogen werden können Eingaben über die HbbTV-Einstellungen bei HbbTV-fähigen Geräten, zum Beispiel die Version des HbbTV-Standards, die das Fernsehgerät unterstützt, oder den HbbTV-Status in den Geräteeinstellung (aktiviert/deaktiviert). Weitere gerätespezifische Daten sind Angaben über alle im Heimnetzwerk vorhandenen und an das Smart-TV-Gerät angeschlossenen elektronischen Geräte sowie die notwendigen Zugangsdaten, um sich gegenüber netzwerkfähigen Heimgeräten oder externen Servern, zum Beispiel über die Hersteller-Infrastruktur, zu authentifizieren.

Ableitbare Daten: Eine Auswertung des Nutzungs- und Fernsehverhaltens kann unter anderem Rückschlüsse auf die politische Einstellung, Hobbys, Bildungsgrad oder die ethnischen Hintergründe des Zuschauers zu erlauben. Darüber hinaus lassen sich anhand der Smart-TV-Sensordaten und gerätespezifischer Daten Rückschlüsse auf Familienstatus sowie Gewohnheiten und Objekte in der unmittelbaren Umgebung des Fernsehgeräts ziehen. Die Aggregation von Browsing-Historie und gegebenenfalls Korrelationen mit Konto- bzw. Registrierungsdaten können verwendet werden, um weitere Persönlichkeitsmerkmale und private Attribute der Zuschauer – wie etwa sexuelle Orientierung und Vorlieben – zu gewinnen. Aus der Interpretation der gerätespezifischen Daten bzw. der Netzwerkadresse des Fernsehers können Details über den Standort des Geräts und somit die des Zuschauers gewonnen werden. Dritte können auf diese Weise nicht nur die Fernseh- und Nutzungsgewohnheiten der Zuschauer ausforschen, sondern diese auch gezielt überwachen.

18 *Lendino (2014); Yeong Gon et al. (2012).*
19 *Ghiglieri/Oswald/Tews (2013); Ghiglieri (2014).*

Alle diese Daten können in der Theorie beliebig miteinander verknüpft werden um Rückschlüsse auf die gegenwärtige Nutzungskontexte und Bedürfnisse der Nutzenden zu ziehen. Derartige Entwicklung des Fernsehgeräts hinzu eine Plattform zur Bereitsstellung und Verbreitung personalisierten Web- und Multimedia-Angebote stellt allerdings gleichzeitig ein neue Gefahrenpotential dar. Den zunehmend steigenden (ökonomischen) Wert der im Smart-TV anfallenden Daten und die Tatsache, dass Apps und Sensoren fast uneingeschränkt auf diese zugreifen können, machen alle drei Hauptkomponenten des Smart-TV-Systems – Fernsehergeräte, Netzwerk-/Kommunikationsinfrastruktur und Cloud-Server – zu attraktiven Angriffszielen für unterschiedliche Gegner.[20]

[20] Vgl. Kap. 3

3
Angreifermodelle und mögliche Angriffsvektoren

Um die Gefährdungslagen im Smart-TV-System genauer zu erfassen, ist eine Charakterisierung relevanter Angreifermodelle notwendig. Dabei soll jeweils zwischen unterschiedlichen Angreifertypen differenziert werden, basierend unter anderem auf ihren Zielen, finanziellen und technischen Möglichkeiten und Fähigkeiten, und ihren Kenntnissen des gesamten oder eines Teils des IT-Systems. Das im Rahmen dieses Forschungsberichts verwendete Angreifermodell sieht folgende Angreifertypen vor:

Passiver Angreifer: Dieser ist in der Lage, alle Kommunikationskanäle im Haushalt abzuhören. Dazu zählen sowohl die Kanäle, die zwischen den Fernsehgeräten der Nutzenden und den unterschiedlichen Back-End- bzw. Cloud-Infrastrukturen verlaufen, als auch die Kommunikationskanäle zwischen Gerätehersteller und Servicetechniker, Infrastrukturbetreiber, Werbetreibenden und TV-Sendern.

Aktiver Angreifer: Dieser ist im Gegensatz zum passiven Angreifer zusätzlich zum Abhören in der Lage, kritische Komponenten des Smart-TV-Systems zu kompromittieren um Zugriff auf die dort gespeicherten Daten zu erlangen. Zudem kann ein aktiver Angreifer die über diese Kommunikationskanäle übertragenen Daten nicht nur lesen, sondern auch blockieren und manipulieren.

Interne vs. externe Angreifer: Passive und aktive Angreifer können entweder außenstehende Dritte sein, zum Beispiel professionelle Hacker, die Fernsehgeräte mit Schadsoftware infizieren, um unbemerkt Zuschauerdaten zu entwenden, oder als Insider in einer legitimen Rolle agieren, etwa Mitarbeiter eines Smart-TV-Herstellers.

Angreifer können daher einzelne Personen in der physischen Nähe des Smart-TV-Gerätes sein, zum Beispiel technikaffine „Nachbarn", die die Kommunikation zwischen den Smart-TV-Geräten und Cloud-Diensten abhören[21]; Mitglieder einer koordinierten Gruppe von professionellen Hackern aus dem Internet; oder unachtsamer / neugieriger / krimineller Mitarbeiter eines Inhaltsanbieters bzw. Geräteherstellers. Während einzelne Angreifer aus dem eigenen WLAN möglicherweise durch Neugier getrieben sind und oftmals über limitierte Ressourcen und Wissen verfügen, legen Erfahrungen aus anderen digitalen Anwendungsszenarien, zum Beispiel bei mobiler Kommunikation oder klassischen Internetdiensten, nahe, dass koordinierte Gruppen von professionellen Angreifern aus dem Internet in der Regel finanziell motiviert sind (zum Beispiel die organisierte Kriminalität) oder im Auftrag von staatlichen Organen wie Strafverfolgungsbehörden oder Geheimdiensten handeln. Durch das Infizieren einer großen Zahl von Smart-TV-Geräten kann der Angreifer einen so genannten Botnet einrichten mit dessen Hilfe weitere Angriffe durchgeführt werden können. Beispiele für derartige Angriffe sind „Denial of Service"-Angriffe auf Komponenten im Heimnetzwerk und Rechner im Firmennetzwerk die häufiger an das Internet angebunden sind; Massen-Datendiebstahl; und automatisierte Massenüberwachung.[22]

Neben den oben aufgeführten Angreifertypen, von denen in erster Linie eine Bedrohung für die Daten- und Systemsicherheit ausgeht, müssen im Kontext von Smart-TVs auch Inhaltsanbieter, Gerätehersteller und weitere Akteure aufgrund ihre zum Teil unseriösen / unfairen / obskuren Geschäftspraktiken (vgl. Kap. 4) als mögliche Bedro-

21 *McSorley (2015).*
22 *Sutherland/Huw/Konstantinos (2014).*

hungsquelle für die Privatheit der Smart-TV-Nutzenden betrachtet werden. In der Tat sind alle im Smart-TV-Kontext relevanten Akteure zunehmend an einer Anhäufung und systematischen Auswertung der im Smart-TV-Gerät anfallenden sensiblen Daten für kommerzielle Zwecke und marktpolitische Gründe interessiert.

Eine weitere Grundlage für eine adäquate Betrachtung der Gefährdungslagen im Smart-TV-System ist die Identifizierung der relevanten Angriffsvektoren.[23] Dabei betrachten wir im Folgenden Angriffsvektoren in den jeweiligen Architekturabschnitten wie in Abbildung 1[24] geschildert. Diese sind: 1) Angriffsvektoren in Smart-TV-Geräten, 2) Angriffsvektoren in den Kommunikationsnetzen und 3) Angriffsvektoren in der Cloud und anderen Back-End-Infrastrukturen der Diensteanbieter. In der Praxis können diese Möglichkeiten auch kombiniert auftreten und sind in der Regel mit Social-Engineering-Ansätzen verbunden. Letztere umfassen Methoden, die Angreifer verwenden können, um den Zuschauer so zu beeinflussen, dass er präparierte Schadsoftware in das Smart-TV-System einschleust[25] und vertrauliche Informationen (unbeabsichtigt) preisgibt. Nicht alle diese Angriffsvektoren und Angriffsflächen sind spezifisch für das Smart-TV-System, müssen aber bei einer ganzheitlichen Gefährdungsanalyse in Betracht gezogen werden.

3.1 Angriffsvektoren im Smart-TV-Gerät

Angriffsvektoren in den mit immer mehr Sensoren ausgestatteten Smart-TV-Geräten umfassen potenzielle Schwachstellen in verschiedener, auf dem Gerät vorhandener Soft- und Hardware.[26] Solche umfassen i) Schwachstellen aus der Erweiterung der Smart-TV-Plattform durch Apps[27], ii) Angriffsflächen im Smart-TV- und HbbTV-Browser[28], iii) Ausführungen verschiedener Multimedia-Inhalte[29], und iv) integrierte Sensoren und Hardware-Schnittstellen:

Smart-TV-Apps: Apps haben in der Regel umfassenden Zugriff auf unterschiedliche geräte- und nutzerspezifische Daten. Nutzende haben oft nur ein geringes Bewusstsein darüber, welche Daten bei der Nutzung einer App anfallen, auf welche Daten verschiedene Apps zugreifen und für welchen Zweck sie benötigt werden. Die Apps werden verwendet, um auf eine Vielzahl von externen (Multimedia-)Inhalten zuzugreifen. Dabei setzen sie das Fernsehgerät zusätzlichen Risiken aus. Forscher der koreanischen Forschungseinrichtung „GrayHash – Offensive Security Research Center“ zeigten 2013, wie die fehlende Transparenz über die Erhebung und Verarbeitung sensibler Daten durch Apps vom Angreifer ausgenutzt werden kann, um Schadsoftware in Fernsehgeräte einzuschleusen.[30] Selbstinstallierte oder mitgelieferte datenschutzunfreundliche Smart-TV-Apps können so vom Angreifer benutzt werden, um auf im Smart-TV-Gerät anfallende sensible Daten zuzugreifen. Darüber hinaus ist die Datenübertragung zwischen Smart-TV-Apps und Cloud-Servern oft im Klartext bzw. unverschlüsselt.[31] Als Konsequenz können nicht nur Details zur aktuellen Fernsehnutzung, sondern auch Passwörter der Benutzer von unbefugten Dritten mitgelesen werden.

23 Ein Angriffsvektor beschreibt einen möglichen Weg, mit dessen Hilfe ein Angreifer Schwachstellen und Sicherheitslücken in einem fremden IT-System ausnutzen kann um sein Ziel zu erreichen.
24 Vgl. Kap. 2.2.
25 *Michéle/Karpow (2013).*
26 *Auriemma (2012); SeungJin/Seungjoo (2013).*
27 *Niemietz/Somorovsky/Mainka/Schwenk (2015).*
28 *Ghiglieri/Oswald/Tews (2013).*
29 *Michéle/Karpow (2013); Mulliner/Michéle (2012).*
30 *SeungJin/Seungjoo (2013).*
31 *Niemietz/Somorovsky/Mainka/Schwenk (2015).*

Smart-TV- und HbbTV-Browser: Browser in Smart-TV-Geräten und ihre Unterstützung von Web-Technologien wie Cookies, Javascript oder HTML eröffnen Angreifern neue Wege, um unbemerkt den ungefähren Standort des Smart-TV-Geräts sowie Informationen zum Gerätetyp genauer und kontinuierlich zu erfassen. Ferner dienen sie Angreifern dazu, den Fernseher mit Schadsoftware zu infizieren sowie den Datenaustausch zwischen Browser und Webserver abzuhören, zu manipulieren oder zu unterbinden. Diese Gefahr wird dadurch verschärft, dass die implementierten Sicherheitsfunktionen häufig unzureichend sind und zusätzliche Sicherheitsmängel im Smart-TV-Browser, zum Beispiel durch inkorrekte Überprüfung der digitalen Zertifikate bei der Unterstützung des HTTPS-Standards,[32] ein Einfalltor für Spähsoftware und andere bösartige Inhalte wie Phishing-Websites sein können.[33] Ein HbbTV-Browser ist gewöhnlich nicht sichtbar und vom Smart-TV-Browser auf dem Fernsehgerät getrennt. Es gelten allerdings die gleichen Gefahren wie auch für einen Smart-TV-Browser. Der Unterschied besteht darin, dass der Nutzer den HbbTV-Browser häufig nicht vom eigentlichen TV-Programm unterscheiden kann, da er bei eingeschalteter HbbTV-Funktionalität nicht gesondert dargestellt wird, sondern innerhalb des übertragenen TV-Programms wirkt. Bei vielen Smart-TV-Geräten ist die HbbTV-Funktionalität standardmäßig aktiviert. Nutzende wissen nicht, ob bestimmte Elemente auf dem angezeigten Bildschirm tatsächlich aus dem Internet oder über das Rundfunksignal kommen.

Multimedia-Inhalte: Spähsoftware und andere Schädlinge können zusätzlich zu Multimediainhalten eingeschleust werden und unentdeckt bleiben.[34] Dabei machen sich die Angreifer Schwächen der auf fast allen Smart-TV-Modellen integrierten Media-Player zunutze. Der Player und die damit verbundenen Codecs[35] ermöglichen das Öffnen und Ausführen von unterschiedlichen Dateitypen inklusive Videos und Bildern. Diese Dateien werden typischerweise entweder von einem Datenträger (USB, Speicherkarte) oder von einem externen Server auf das Smart-TV-Gerät gespielt. Sie sind potenziell Träger von Trojanern, deren Ausführung dem Angreifer erlauben, i) unbemerkt die Kontrolle über kritische Hardware-Module wie Kameras und Mikrofon zu erlangen, ii) auf sensitive Daten (etwa Kontakte, Passwörter, Kreditkartennummern, Standort des Geräts) zuzugreifen oder iii) das Gerät zum Absturz zu bringen.[36] Ähnlich können Angreifer (oder auch datenhungrige Gerätehersteller, TV-Sender oder Servicetechniker) Schwachstellen im Design der Fernwartungsstrategie für Smart-TV-Geräte ausnutzen, um Nutzende dazu zu bewegen, präparierte Firmware-Updates mit integrierter Spähsoftware auf dem Fernseher zur Ausführung zu bringen. Es ist daher wichtig, dass Sicherheitsaktualisierungen in allen Teilsystemen auf dem Smart-TV-Gerät schnell und zügig auch beim Nutzer ankommen. Veraltete Systeme erhöhen das Risiko von Sicherheitsvorfällen signifikant.

Integrierte Sensoren und Hardware-Schnittstellen: Moderne Smart-TV-Geräte[37] werden mit einer Vielzahl von Sensoren ausgestattet, zum Beispiel Mikrofone, Kameras, Bewegungs-, Temperatur- und Luftfeuchtigkeitssensoren. Diese stellen einerseits Rückkanäle zur Verfügung, die wiederum die Interaktion mit und Partizipation am TV-Programm oder die Nutzung von Web-Anwendungen wie Skype oder Facebook ermöglichen. Anderseits steigt mit dem Trend zu Ausstattung des Geräts mit HD-Kameras, Mikrofon und Bewegungssensoren auch das Risiko für Schwachstellen in den verwendeten Apps und in der Software für die Sensorsteuerung. Angreifer können Kenntnis über die Architektur der eingebauten Hardware und Sensoren und über das

32 HTTPS ist der Standard für die verschlüsselte Übertragung von Daten zwischen Browser und Webserver.
33 *Ghiglieri (2014).*
34 *Michéle/Karpow (2014).*
35 Verfahren, um bestimmte Videoformate abzuspielen.
36 *Auriemma (2012); SeungJin/Seungjoo (2013).*
37 Häufig bieten Hersteller verschiedene Produktreihen mit verschieden ausgestatteten Smart-TV-Geräten an.

Zusammenspiel zwischen diesen und weiterer Software auf dem Smart-TV-Gerät erlangen. Sie können dieses Wissen nutzen, um das System zu kompromittieren. Geräte mit größerer Ausstattung besitzen bereits Kameras oder Bewegungssensoren sowie Mikrofone. Sie können durch schadhafte Firmware so manipuliert werden, dass sie als Wanze nutzbar sind.[38] Eine Untersuchung unterschiedlicher Smart-TV-Modelle der Firma Samsung hat 2013 gezeigt, wie vorinstallierte Web-Anwendungen von Angreifern manipuliert werden können, um aus der Ferne Zuschauer oder deren Wohn- und Schlafzimmer über in Smart-TV-Geräten eingebaute Webcams und Mikrofone auszuspionieren.[39] Dabei ist das Fernsehgerät nicht mehr in der Lage, den üblichen Hinweis (je nach Ausstattung rotes oder grünes Licht oder keine Information an den Nutzenden) auf den Status der Kamera oder des Mikrofons zu geben; der Betrieb von Webcam und Mikrofon ist somit durch den Nutzenden nicht mehr kontrollierbar.

3.2 Angriffsvektoren in Kommunikationsnetzen

Weitere Angriffsvektoren bestehen darin, Design und Implementierungsschwächen in Protokollen zur Übertragung von Daten zwischen Smart-TV-Gerät und externen Parteien auszunutzen, um den Datenverkehr abzuhören oder manipulierte Datenpakete einzuschleusen oder den Datenverkehr zu filtern bzw. zu blockieren.[40] Gelingt es einem passiven Angreifer, den Verkehr zwischen Smart-TV-Gerät und externem Webserver, zum Beispiel den des Geräteherstellers oder des Online-Bezahldienstes, auszuspähen, kann dieser unbemerkt und unautorisiert Zugriff auf sensible Zuschauer- und Fernseherdaten erlangen. Ghiglieri et al.[41] zeigten 2013, wie Dritte Schwächen des HbbTV-Protokolls ausnutzen können, um das Nutzungsverhalten der Zuschauer eines HbbTV-tauglichen Fernsehers mit WLAN-Nutzung ohne deren Wissen oder das der TV-Sender aufzuzeichnen. Der Angriff ist selbst dann möglich, wenn das WLAN mit Hilfe von WPA2 abgesichert ist und der Angreifer nicht Teil des Netzwerkes ist.[42] Das ist möglich, da TV-Sender unterschiedliche und jeweils charakteristische Paketgrößen für die übertragenen Daten verwenden. Durch einen Abgleich mit einem eigenen Smart-TV-Gerät kann ein Angreifer auf diese Weise sogar bei verschlüsselten Datenpaketen leicht Übereinstimmungen in der Größe der Pakete feststellen und bei Erkennung einer bestimmten Paketreihenfolge die Bestimmung des eingeschalteten Senders durchführen. Zudem dokumentierten die Autoren, wie HbbTV-Features die Sendeanstalten befähigen, sensible Daten, etwa zum Nutzungsverhalten, detaillierter über ihre Zuschauer zu erfassen. Dieselbe Schwachstelle könnte auch von aktiven Angreifern und bösartigen Infrastrukturbetreibern ausgenutzt werden, um zusätzlich bestimmte Inhalte zu blockieren bzw. zu zensieren oder präparierte Datenpakete in Fernsehgeräte als Vorstufe eines großflächigen „Denial of Service"-Angriffs einzuschleusen.

Ein weiterer Angriff bezieht sich auf das Rundfunksignal, welches die Internet-Adresse für die HbbTV-Anwendung beinhaltet. Durch Manipulation der HbbTV-Adresse im Rundfunksignal kann eine großflächige Manipulation von Inhalten auf HbbTV-fähigen Geräten stattfinden. Zudem sind existierende Schutzmaßnahmen im Rundfunksignal oft äußerst ineffektiv.[43]

38 *Michéle/Karpow (2014).*
39 *Grattafiori/Yavor (2013).*
40 *Bachy/Basse/Nicomette/Alata/Kaâniche/Courrege/Lukjanenko (2015).*
41 *Ghiglieri/Oswald/Tews (2013).*
42 *Ghiglieri/Oswald/Tews (2013); Ghiglieri/Tews (2014).*
43 *Oren/Keromytis (2014); Michéle (2015).*

3.3 Angriffsvektoren in der Cloud und anderen Back-End-Infrastrukturen

Bei cloudbasierten Webdiensten bestehen zahlreiche Angriffsvektoren, die unabhängig vom Anwendungsszenario der Smart-TV-Geräte bestehen. Die typischen drei relevanten Angriffsvektoren werden im Folgenden zusammengefasst:

Böswilliger Insider beim Cloud-Betreiber: Es handelt sich dabei um Angreifer (häufig auch Angestellte der Cloud-Betreiber mit privilegiertem Zugang zu Kundendaten) mit Kenntnissen über die interne grundlegende Architektur der aktuellen Cloud-Computing basierten Smart-TV-Angebote.[44] Je nach Berechtigungen kann der böswillige Insider Kundendaten löschen, ändern oder kopieren und im schlimmsten Falle sogar an kriminelle Organisationen verkaufen.[45]

Schwachstellen in der „Shared Architecture": Dazu gehören Isolationsbrüche, unsichere virtuelle Maschinen und unvollständige Löschung sensibler Daten:

- **Isolationsbrüche:** Die Tatsache, dass in der Cloud mehrere virtuelle Maschinen auf einem Rechner laufen und dementsprechend verschiedene Cloud-Anwender (Anbieter von Webdiensten) sich Ressourcen wie CPU, Speicher, Netzwerk usw. teilen müssen, kann gemeinsam mit Schwachstellen im Design oder der Implementierung des Hypervisors[46] ausgenutzt werden, um auf fremde Daten, Ressourcen und Anwendungen zuzugreifen[47].
- **Unsichere virtuelle Maschinen:** Es kommt häufig vor, dass unachtsame Entwickler Images (Details zur Konfiguration von virtuellen Maschinen) veröffentlichen, die noch private kryptographische Schlüssel, Zertifikate und Passwörter enthalten.[48] Für einen Angreifer mit Wissen über diese sensiblen Informationen wäre dann eine Kompromittierung der virtuellen Maschine mitsamt der Kundendaten und der Anwendungen keine große Herausforderung.
- **Unvollständige Löschung sensibler Daten:** Im Rahmen vieler cloudbasierter Angebote kann es aus unterschiedlichen Gründen dazu kommen, dass ein neuer Kunde eine virtuelle Maschine erhält, auf der die Datenbestände vorheriger Anwender nicht vollständig gelöscht wurden. Dies erhöht das Risiko, dass sensible Kundendaten in falsche Hände geraten könnten.

Unsichere Managementschnittstellen und APIs: Cloud-basierten Smart TV-Dienste werden in der Regel über Schnittstellen und Interfaces verwaltet, welche wiederum über das Internet erreichbar sind. Diese können in Kombination mit einer schwachen Authentifizierung oder gefälschten Identitäten unbefugt verwendet werden, um auf Kundendaten und Anwendungen zuzugreifen.[49]

Zusätzlich zu den Folgen der oben beschriebenen Schwachstellen und Angriffsvektoren für die Daten- und Systemsicherheit, birgt die Nutzung von Smart TVs auch bisher für viele Nutzenden schwer abschätzbare Implikationen für die informationelle Selbstbe-

44 *Kandias/Virvilis/Gritzalis* (2013).
45 *Zeit Online (2013),* Daten von zwei Millionen Vodafone-Kunden kopiert, 12.9.2013, http://www.zeit.de/digital/2013-09/vodafone-daten-diebstahl.
46 Komponenten/Mechanismen zur effektiven Trennung der Daten und Anwendungen verschiedener VMs.
47 *Wojtczuk/Beulich (2012); Kortchinsky (2009); Elhage (2011).*
48 *Bugiel/Nürnberger/Pöppelmann/Sadeghi/Schneider (2011).*
49 Für einen aktuellen Überblick über Angriffsvektoren und Bedrohungen in der Cloud vgl. *CSA (2013); Zeit Online (2013),* Daten von zwei Millionen Vodafone-Kunden kopiert, 12.9.2013, http://www.zeit.de/digital/2013-09/vodafone-daten-diebstahl; *Buchmann (2012),* 189 ff.

Angreifermodelle und mögliche Angriffsvektoren

stimmung, da unterschiedliche Akteure und Architekturkomponenten im Smart-TV-System personenbezogene bzw. personenbeziehbare Daten sammeln und auswerten.

Im nächsten Kapitel werden mögliche Bedrohungen von Smart-TVs für die informationelle Selbstbestimmung angeführt.

4
Bedrohungspotenzial für die informationelle Selbstbestimmung

Die finanziellen oder politischen Anreize, Smart-TV-Daten[50] systematisch zu erfassen und auszuwerten, beinhalten vor allem in der entstehenden „Big Data"-Ära schwerwiegende Folgen für die informationelle Selbstbestimmung des Nutzenden. Mögliche Implikationen und Einschränkungen für die informationelle Selbstbestimmung können sich durch die Nutzung von Smart-TV-Systemen etwa in folgender Hinsicht ergeben:

Intransparenz der Datenverarbeitung: Die Nutzenden sind sich nicht immer dessen bewusst, dass ihre Fernsehgeräte Daten häufig auch ohne konkreten Bedarf erfassen und weiterleiten können. Besonders problematisch dabei ist, dass die Nutzenden eine Übertragung von Inhalten gar nicht erwarten und daher auch nicht darauf kommen, dies zu hinterfragen. Viele Nutzende von Smart-TV-Geräten sind sich nicht einmal der Tatsache bewusst, dass ihr Gerät über eine Verbindung ins Internet verfügt.[51] Zudem ermöglicht die Systemgestaltung heutiger Smart-TVs eine Erhebung und Verarbeitung vielfältiger sensitiver Daten ohne Mitwirkung und Einwilligung der Betroffenen.[52] Beispielsweise werden zum Zweck der Datensammlung verstärkt Töne im Ultraschallbereich (kaum wahrnehmbar durch die Nutzenden) in Kombination mit Cookies eingesetzt.[53] Dementsprechend gefährdet die Übertragung der so gesammelten Daten an externe Akteure das Einhalten des Transparenzprinzips gegenüber den Nutzenden.

Zweckentfremdete Datennutzung: Anders als beim herkömmlichen Fernsehen können bei dem Einsatz von Smart-TV-Technologien unterschiedliche personenbeziehbare Daten durch Dritte unbemerkt gesammelt, mit anderen persönlichen Daten des Zuschauer verknüpft und zweckentfremdet weiterverarbeitet werden, etwa durch Verknüpfung von Kreditkartendaten mit Details über die Nutzung des HbbTV-Angebots oder über die Nutzung des Smart-TV-Geräts. Eine derartige Datennutzung ermöglicht die Zusammenstellung von umfassenden und detaillierten Zuschauerprofilen und stellt somit ein Gefährdungspotenzial für die informationelle Selbstbestimmung dar.[54]

Tracking und Profilbildung: Smart-TV-Geräte verbinden sich zu den Servern der Sender des jeweils auf dem Gerät laufenden Programms, sofern diese eine HbbTV-Anwendung bereitstellen. Beim Einschalten[55] eines Senders wird vom Gerät mindestens eine Anfrage an einen Server des Senders gestellt, um den so genannten „Red Button", der die Verfügbarkeit von weiteren Online-Inhalten zum gewählten Programm anzeigt, auf dem Bildschirm einzublenden. Viele Sender belassen es jedoch nicht bei einer einmaligen Anfrage, sondern senden periodische Anfragen mit einem Zeitintervall zwischen einer Sekunde und mehreren Minuten.[56] Auf diese Weise ist der Sender in regelmäßigen Abständen (in der Vergangenheit sogar teilweise sekundengenau) darüber informiert, wann genau der Nutzende einen Sender eingeschaltet hat. Dies verletzt das Prinzip der Datensparsamkeit und Datenvermeidung. Bei einigen Sendern werden über periodische Anfragen auf den Server des Senders zugleich Trackingskripte von

50 Vgl. Kap. 2.3.
51 Nach *PricewaterhouseCoopers (2013)*, S. 12 wissen 22% der Smart-TV-Benutzer nicht, ob ihr Smart-TV mit dem Web verbunden ist; 10% der TV-Haushalte wissen nicht, ob ihr TV-Gerät ein Smart-TV ist.
52 DoctorBeet's Blog (2013).
53 Goodin (2015).
54 Angwin (2015).
55 Datenschutzfreundlichere Varianten von HbbTV ermöglichen sogar das Laden über das Rundfunksignal. So würden Nutzertracking und Profilbildung verhindert.
56 *Ghiglieri/Oswald/Tews (2013).*

Bedrohungspotenzial für die informationelle Selbstbestimmung

Drittanbietern wie Google Analytics oder eTracker geladen oder Cookies gesetzt. Beides sind Maßnahmen, um das Nutzerverhalten nachzuverfolgen und zu analysieren. Die Ergebnisse des Trackings mit Google Analytics erhält der Sender selbst nur in anonymisierter Form. So dürfen keine ganzen, sondern nur Teile der IP-Adressen an den Sender übertragen werden. Dagegen ermöglicht die Verwendung von Cookies dem Sender wesentlich detailliertere Informationen zum Nutzerverhalten. Dem Setzen von Cookies kann in vielen Smart-TV-Geräten nicht widersprochen werden. Ferner können diese oft gar nicht oder nur umständlich angesehen oder gelöscht werden.[57] Beides hat zur Folge, dass gesetzte Cookies für immer auf dem Gerät gespeichert bleiben und damit eine eindeutige Nutzerkennung darstellen. Da häufig eine Sendeanstalt mehrere Sender verantwortet, können dadurch auch ein senderübergreifendes Tracking der Nutzenden und die Erstellung von detaillierten Nutzerprofilen möglich sein. Dass die Sender tatsächlich Nutzerprofile erstellen, zeigt die bei manchen Sendern in festen Zeitabständen eingeblendete personalisierte Werbung.[58] Besonders problematisch ist das Tracking des Nutzerverhaltens, weil dies technisch sogar dann möglich ist, wenn der Nutzende die HbbTV-Funktionalität nicht wissentlich anfordert, weil er den „Red Button" auf der Fernbedienung noch nicht gedrückt hat. Unabhängig von Cookies oder Skripten wird in jedem Fall durch eine Verbindung des Smart-TV-Geräts zum Sender die IP-Adresse des Nutzenden übertragen, die eine grobe Lokalisierung des Nutzenden erlaubt. Da IP-Adressen bei vielen Internetprovidern für 24 Stunden oder länger gleich bleiben, liefert die IP-Adresse damit zugleich die Möglichkeit, den Nutzenden in diesem Zeitraum wiederzuerkennen. Darüber hinaus machen sich Werbetreibende und andere Datensammler zunehmend die Möglichkeit zunutze, zusätzliche und für die Nutzenden kaum wahrnehmbare (Ton-)Signale im ausgestrahlten TV-Programm und besuchten Webseiten einzubetten, um Nutzerverhalten über mehreren Geräte (Fernseher, Smartphone, PC) hinaus tracken zu können.[59] So können Nutzerprofile, dank der Korrelation zwischen Details zu TV-Werbespots / -Sendungen und Websuche-Metadata bereichert werden.

Massenüberwachung und gezielte Überwachung der Zuschauer: Aus Daten von kompromittierten Smart-TV-Sensoren, zum Beispiel Video-, Bilder-, und Stimmaufnahmen, lassen sich ohne Wissen und Einverständnis der Nutzenden Informationen über Aktivitäten und Verhaltensweisen der Nutzenden sowie über die Ausstattung in sensiblen Bereichen des Haushalts ableiten. Dies stellt nicht nur ein Sicherheitsrisiko dar, weil Einbrecher oder aufdringliche Diensteanbieter und Werbetreibende den Zuschauer on- und offline (gezielt) überwachen können. Auch global agierende Organe wie Geheimdienste können sich unberechtigt und unbemerkt Zugriff auf die im Smart-TV-System anfallenden Daten, gegebenenfalls durch Umwege über Server der Diensteanbieter, verschaffen und diese zweckentfremden, um Massenüberwachungsprogramme durchzuführen. Zudem können Dritte vorhandene Schwächen der Soft- und Hardware ausnutzen,[60] um Zuschauer aus der Ferne über die in Smart-TV-Geräten eingebauten Kameras und Mikrofone gezielt zu überwachen.[61] Über ähnliche Fähigkeiten verfügen Hersteller modernerer Smart-TV-Geräte. Sie können ihre Geräte ohne Wissen und vor allem ohne informierte Einwilligung der Smart-TV-Nutzenden als Lauschinstrument heimlich in Wohn- oder Schlafzimmern verwenden. So ist etwa die Spracherkennungsfunktion in neuen Smart-TV-Geräten der Marke Samsung *per default* aktiviert, und das Gerät kann dementsprechend Gespräche in seiner Umgebung kontinuierlich aufzeichnen und zur Weiterverarbeitung an externe Server schicken.[62]

57 Ghiglieri/Oswald/Tews (2013).
58 Ghiglieri/Oswald/Tews (2013).
59 Goodin (2015).
60 Vgl. Kap. 3.1.
61 Grattafiori/Yavor (2013); Derene (2015).
62 *ACLU (2015); Harris (2015).*

Bedrohungspotenzial für die informationelle Selbstbestimmung

Verlust / Einschränkung der Entscheidungsautonomie: Heutige Smart-TV-Dienste können schwerwiegende Folgen für die individuelle Entscheidungsautonomie haben. Insbesondere gibt es Bedenken, dass aufgrund der Gestaltung der Plattform und Methoden zur Erhebung und Verarbeitung der Daten im Smart-TV-System den Nutzenden keine echten Entscheidungsoptionen gegeben werden. Dies lässt die Verbraucher mit einer nicht akzeptablen Wahl zurück, da ein Widerspruch der Datenerhebung meist mit einem völligen Verlust des Dienstes verbunden ist.[63] Alleine die Möglichkeit, Smart-TV-Systeme und die dabei anfallenden Daten zur gezielten Überwachung einzusetzen, kann die Entscheidungsautonomie der Nutzenden stark einschränken. Sie könnten ihr Nutzungsverhalten als Reaktion auf ein Gefühl des Beobachtetwerdens zu ihren Ungunsten einschränken oder gar auf die Nutzung eines Smart-TV-Geräts gänzlich verzichten. Es besteht zudem die Gefahr, dass der Einzelne in Folge der allgegenwärtigen „Überwachung" sein persönliches Verhalten ändert, sich sozialen Erwartungen anpasst und vermeintlich inadäquates Verhalten meidet. Das Risiko des sozial erwünschten, angepassten Verhaltens kann sich auf alle Lebenslagen ausdehnen, nicht nur auf die Bereiche der Informationsbeschaffung und Meinungsäußerung, sondern auch auf das alltägliche Verhalten in der eigenen Wohnung.[64]

Weitere Bedenken: Darunter fällt unter anderem das Risiko einer Offenlegung vertraulicher Daten, etwa Konto- und Registrierungsdaten des Zuschauers, als Folge von technischem oder menschlichem Versagen oder Cyber-Angriffen. Damit eng verbunden ist das Risiko für millionenfachen Identitätsdiebstahl mit potenziell schwerwiegenden Auswirkungen für die Nutzenden, etwa in Form von materiellem oder finanziellem Schaden nach Identitätsmissbrauch. Zudem ist in Anbetracht des zunehmenden Einsatzes von Big-Data-Technologien als wichtiges Element entstehender Smart-TV-Anwendungen festzustellen, dass hier neue Möglichkeiten zur Segmentierung der Zuschauer entstehen, mit Konsequenzen weit über den Datenschutz und die informationelle Selbstbestimmung hinaus.[65] Beispielweise wird durch die fehlende Unterstützung von Anonymität bei der Nutzung derzeitiger Smart-TV-Systeme das Recht des Einzelnen auf freie Meinungsbildung, ein nicht wegzudenkender Bestandteil einer freiheitlich-demokratischen Ordnung, gefährdet.[66]

63 *DoctorBeet's Blog (2014).*
64 Vgl. *Schaar* 2007, 65; *Bergt*, Überwacht bis in die Kaffeeküche, die tageszeitung vom 23.4.2010, http://www.taz.de/!51502/; *Gaycken*, "Man passt sich an und merkt es nicht", die tageszeitung vom 31.10.2007, http://www.taz.de/!6887/.
65 *Roßnagel*, ZD 2013, 562; *Ochs*, in: Richter 2015, 169 ff.; *Simo*, in: Richter 2015, 13 ff.
66 Vgl. Kap. 5.1.1 zum Recht auf freie Meinungsäußerung.

5
Rechtliche Rahmenbedingungen

Wie gezeigt, ist die Zahl der an der Datenerhebung und -verarbeitung beteiligten Akteure und potenziellen Angreifer auf Smart-TV-Systeme groß. Dennoch ist das Smart-TV-System kein rechtsfreier Raum; es gilt sowohl grundrechtliche als auch datenschutzrechtliche Rahmenbedingungen zu beachten. Um Akzeptanz und Vertrauen der Nutzenden in die Technologie zu steigern und zu erhalten, ist eine verfassungskonforme Gestaltung dieser Technologie unabdingbar. Der folgende Abschnitt untersucht, welche Vorschriften für die jeweils am System beteiligten Akteure (Smart-TV-Nutzende, TV-Sender und Smart-TV-Hersteller) Beachtung finden müssen.

5.1 Grundrechtliche Rahmenbedingungen

Die grundrechtlichen Rahmenbedingungen, die im Zusammenhang mit Smart-TV-Systemen eine Rolle spielen, sind vielfältig und aufgrund der Vielzahl der am System Beteiligten häufig gegenläufig.

Für Smart-TV-Nutzer, das heißt die Inhaber der jeweiligen Geräte, ergeben sich Risiken für das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG in seinen verschiedenen Ausprägungen der informationellen Selbstbestimmung, des Rechts am eigenen Wort und Bild sowie dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Aber es sind auch Auswirkungen auf die Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 GG, die Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG sowie das Fernmeldegeheimnis aus Art. 10 GG denkbar. Für TV-Sender als Zugangsanbieter kommt in erster Linie die Rundfunk- und Pressefreiheit aus Art. 5 Abs. 2 GG in Frage; für Smart-TV-Hersteller sind die Berufsfreiheit aus Art. 12 GG sowie die Eigentumsfreiheit aus Art. 14 GG näher zu betrachten.[67]

5.1.1 Smart-TV-Nutzende

Potenziell am stärksten in ihren Grundrechten beeinträchtigt sind diejenigen Smart-TV-Nutzenden, die ein solches Gerät in ihrer häuslichen Umgebung täglich gebrauchen. Durch die mit der Nutzung verbundene (potenzielle) Datenerhebung sind vielerlei Grundrechte betroffen, die geeignet sind, das allgemeine Persönlichkeitsrecht des Einzelnen zu beeinträchtigen. Darüber hinaus bedürfen aber auch die Informationsfreiheit, das Fernmeldegeheimnis und die Unverletzlichkeit der Wohnung einer näheren Betrachtung.

Allgemeines Persönlichkeitsrecht

Das allgemeine Persönlichkeitsrecht schützt den sozialen Geltungsanspruchs des Menschen sowie die „konstituierenden Elemente der Persönlichkeit", die nicht durch spezielle Grundrechte geschützt sind.[68] Das umfasst die Integrität der Persönlichkeit in geistig-seelischer Beziehung, also das Handeln und das Sein einer Person.[69] Das allgemeine Persönlichkeitsrecht beruht auf der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 GG in Verbindung mit der Menschenwürde des Art. 1 Abs. 1 GG. Mit der Menschenwürde

67 *Weichert*, DuD 2014, 528 (529 f.).
68 BVerfGE 54, 148, 153; ausführlich zum Beispiel *Murswiek*, in: Sachs 2011, Art. 2 GG, Rn. 59 f., 66; *Starck*, in v. Mangoldt/Klein/Starck 2010, Art. 2 Abs. 1 GG, Rn. 17.
69 *Murswiek*, in: Sachs 2011, Art. 2 GG, Rn. 59.

ist es unvereinbar, den Menschen zum bloßen Objekt zu machen, ihn „zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, und einer Bestandsaufnahme in jeder Beziehung zugänglich zu machen".[70] Das allgemeine Persönlichkeitsrecht schützt vor Beeinträchtigungen sowohl durch staatliches Handeln als auch durch Dritte.[71] Auf Grund der Gemeinschaftsgebundenheit des Einzelnen ist der Schutz des allgemeinen Persönlichkeitsrechts jedoch nicht absolut und kann mit Rücksicht auf andere Rechtsgüter, zum Beispiel dem durch Art. 5 Abs. 1 GG geschützten legitimen Informationsinteresse der Allgemeinheit, – unter strikter Wahrung des Verhältnismäßigkeitsgebots – Einschränkungen unterliegen.[72]

Bei dem Grundrecht handelt es sich um ein entwicklungsoffenes und durch die Rechtsprechung noch weiter auszudifferenzierendes Grundrecht. Dies ermöglicht, auf neue Herausforderungen durch die technisch-gesellschaftliche Entwicklung zu reagieren[73] – nicht nur, aber gerade auch in der digitalen Welt. Dennoch lassen sich Fallgruppen bilden, die für die Persönlichkeitsentfaltung und den sozialen Geltungsanspruch des Einzelnen essenziell sind und im Zusammenhang mit Smart-TV einer genaueren Betrachtung bedürfen, nämlich das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme.

Recht auf informationelle Selbstbestimmung

Durch die Nutzung von Smart-TV-Geräten, durch die Verbindung mit dem Internet sowie durch eingebaute Sensoren und Kameras und Mikrophone werden personenbezogene Daten erhoben. Dadurch ergeben sich persönlichkeitsrelevante Fragestellungen, die die informationelle Selbstbestimmung tangieren.

Als Konkretisierung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG wurde das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht im Volkszählungsurteil[74] im Jahre 1983 entwickelt. Die freie Entfaltung der Persönlichkeit setzt unter den Bedingungen moderner Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung und Nutzung personenbezogener Daten voraus. Neben dem Schutz der individuellen Entfaltungschancen des Einzelnen dient die informationelle Selbstbestimmung auch dem Gemeinwohl, da Selbstbestimmung Grundvoraussetzung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten Gemeinwesens ist.[75] Selbst zu bestimmen, welche Informationen in die Öffentlichkeit gelangen, ist notwendig, um sich frei und ungezwungen zu verhalten. Die Selbstbestimmung ist damit für die Ausübung anderer Grundrechte essenziell. Nur wenn der Einzelne nicht befürchten muss, dass Informationen über ihn ohne oder gegen seinen Willen aus dem jeweiligen Zusammenhang gerissen und zweckentfremdet verwendet werden, kann er sich ohne Angst vor Nachteilen frei entfalten und vor allem seine anderen Grundrechte wahrnehmen, etwa die Meinungs-, Informations- und Kommunikationsfreiheit oder auch die Religionsfreiheit.

Das Recht umfasst daher die Befugnis des Einzelnen, unabhängig von der betroffenen Lebenssphäre selbst zu bestimmen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[76] Damit soll jeder selbst sowohl über die Erhebung und Verwendung seiner personenbezogenen Daten als auch über den jeweiligen

70 BVerfGE 5, 85 (204); 7, 198 (205); 27, 1 (6).
71 *Murswiek*, in: Sachs 2011, Art. 2 GG, Rn. 59.
72 BVerfGE 34, 238 (248 f.); *Starck*, in: v. Mangoldt/Klein/Starck 2010, Art. 2 GG, Rn. 173.
73 *Di Fabio*, in: Maunz/Dürig 2014, Art. 2 GG, Rn. 147.
74 BVerfGE 65, 1.
75 BVerfGE 65, 1 (43).
76 BVerfGE 65, 1 (42).

Empfänger der Information bestimmen können.[77] Auf die Art und Herkunft der Daten kommt es dabei nicht an; entscheidend ist allein die Nutzbarkeit und Verwendungsmöglichkeit, da durch moderne Verarbeitungs- und Verknüpfungstechnologien je nach Kontext jedes Datum einen neuen Stellenwert bekommen kann.[78]

Das Recht auf informationelle Selbstbestimmung gewährt sowohl einen Abwehranspruch gegenüber staatlichen Eingriffen als auch einen Schutzanspruch des Einzelnen gegenüber dem Staat zur Verhinderung des Eingriffs durch private Akteure.[79] Eine Verletzung des Rechts auf informationelle Selbstbestimmung besteht unter anderem in einem unrechtmäßigen Erheben und Verwenden personenbezogener Daten ohne Einwilligung des Betroffenen oder gesetzliche Ermächtigungsgrundlage,[80] in der zweckungebundenen Speicherung personenbezogener Daten auf Vorrat[81] sowie in der Verweigerung des Zugangs des Einzelnen zu ihn betreffenden Informationen.[82]

Das Bedrohungspotenzial für die informationelle Selbstbestimmung wurde bereits in Kapitel 4 ausführlich erläutert; für Beispiele sei auf dieses verwiesen.

Vertraulichkeit und Integrität informationstechnischer Systeme

Smart-TV-Geräte sind zu einem wichtigen Bestandteil des täglichen Medienkonsums geworden, die viele persönliche Informationen verfügbar halten. Nicht nur wird der Einzelne hierdurch abhängig von der Technik, sie wird auch zum Teil der Persönlichkeit, der tiefe Einblicke in die Interessen, Psyche und Neigungen erlaubt und gewissermaßen als „ausgelagerter Teil des Körpers“[83] funktioniert. Daraus resultiert die entsprechend große Bedeutung informationstechnischer Systeme für die individuelle Persönlichkeitsentfaltung des Einzelnen. Das Vertrauen des einzelnen Nutzenden in die Funktionsfähigkeit und den Ausschluss Dritter auf diese Systeme zu schützen, ist Inhalt des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme.[84] Dieses Grundrecht hat das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung 2008 aufgrund der Persönlichkeitsrelevanz der informationstechnischen Systeme aus dem allgemeinen Persönlichkeitsrecht konkretisiert.[85]

Vom Schutzbereich umfasst sind eigengenutzte informationstechnische Systeme von einer gewissen Komplexität.[86] Persönlichkeitsrelevanz besitzen nur solche informationstechnischen Systeme, über die der Einzelne selbstbestimmt verfügen kann und die allein oder durch ihre Vernetzung mit anderen Systemen personenbezogene Daten des Betroffenen in einem Umfang und einer Vielfalt erheben, die zum Beispiel einen wesentlichen Einblick in Aspekte der Lebensgestaltung oder sogar ein aussagekräftiges Persönlichkeitsprofil ermöglichen können. Solche Systeme waren zur Zeit des Urteilsspruchs nach Meinung des Bundesverfassungsgerichts zum Beispiel Personal Computer, Mobiltelefone und elektronische Terminkalender, sofern diese durch einen großen Funktionsumfang und das Erfassen und Speichern personenbezogener Daten einen

77 BVerfGE 65, 1 (41 f.).
78 BVerfGE 65, 1 (45); *Di Fabio*, in: Maunz/Dürig 2014, Art. 2 GG, Rn. 174; *Jarass*, in: Jarass/Pieroth 2012, Art. 2 GG, Rn. 43.
79 *Di Fabio*, in: Maunz/Dürig 2014, Art. 2 GG, Rn. 176, 189.
80 *Di Fabio*, in: Maunz/Dürig 2014, Art. 2 GG, Rn. 178.
81 BVerfGE 65, 1 (46); zur Vorratsdatenspeicherung siehe auch EuGH, Urt. v. 8.4.2014, Rs. C-293/12 und C-594/12 sowie BVerfGE 125, 260.
82 *Murswiek*, in: Sachs 2011, Art. 2 GG, Rn. 73a; *Trute*, in: Roßnagel 2003, Kap. 2.5, Rn. 58.
83 *Hassemer*, Süddeutsche Zeitung vom 11.6.2008, zitiert in *Hoffmann-Riem*, JZ 2008, 1009 (1012) Fußnote 22; ähnlich argumentierte der Supreme Court in den USA in seinem Urteil vom 25.6.2014 (Riley vs. California), vgl. *Richter*, Fast schon ein Körperteil, Süddeutsche.de vom 26.6.2014, http://sz.de/1.2018007.
84 BVerfGE 120, 274.
85 BVerfGE 120, 274; ausführlich zum Beispiel *Hoffmann-Riem*, JZ 2008, 1009 ff.; *Hornung*, CR 2008, 299 ff.; *Roßnagel/Schnabel*, NJW 2008, 3534 ff.; *Kutscha*, DuD 2012, 391 ff.
86 BVerfGE 120, 274 (313).

Einblick in die Lebensgestaltung einer Person und ein aussagekräftiges Bild seiner Persönlichkeit erlauben.[87] Heute zählen dazu ebenso Laptops, Smartphones und Tablets, vernetzte Haushalts- und Betriebstechnik, Informations-, Kommunikations- und Multimedia-Anwendungen und mithin auch Smart-TV-Geräte, sowie telemedizinische Anwendungen, sofern diese durch das Aufzeichnen der Gewohnheiten und Verhaltensweisen eines Bewohners – seien es Aufzeichnungen zum Schlaf- oder Essverhalten, der Empfang von Besuch oder das verfolgte TV-Programm – detaillierte und aussagekräftige Einblicke in oder Rückschlüsse auf die private Lebensgestaltung des Nutzenden ermöglichen.[88]

Schutzrichtung des Grundrechts ist zum einen die Vertraulichkeit, zum anderen die Integrität informationstechnischer Systeme: Die Vertraulichkeit umfasst die durch solche informationstechnischen Systeme erzeugten, verarbeiteten und gespeicherten Daten, also das Interesse des Nutzenden, dass diese Daten vertraulich bleiben.[89] Ein Eingriff in die Vertraulichkeit liegt bei jeder Erhebung von Daten und bei jedem Zugriff auf Daten aus dem System vor, unabhängig von der Qualität der Daten oder der Art des Zugriffs. Eine Wahrnehmung der Daten ist nicht notwendig, vielmehr ist die Vertraulichkeit bereits mit der Speicherung der Daten beeinträchtigt.[90]

Der Schutz der Integrität informationstechnischer Systeme umfasst den Schutz der Leistungen, Funktionen und Speicherinhalte des informationstechnischen Systems vor dem Zugriff Dritter.[91] Darunter fällt der Schutz vor der Überwindung von Hindernissen, die vor dem Eindringen in das System schützen, sowie der Schutz vor Störungen und Manipulation des Systems, etwa durch Verfälschen oder Ergänzen von Daten, durch eine Ausstattung mit Software, die das Ausspähen oder Ausleiten von Daten durch Dritte ermöglicht, oder durch eine Veränderung der Funktionsweise der eingesetzten Software.[92] Ein Eingriff in die Integrität liegt bereits dann vor, wenn ein späterer Informationseingriff vorbereitet wird, auch wenn (noch) keine Daten erhoben werden oder die Erhebung fehlschlägt. Bereits mit der Überwindung eines Hindernisses, das ein Eindringen in ein informationstechnisches System von außen verhindern soll, ist die Integrität des Systems beeinträchtigt.[93]

Das Grundrecht schützt das Vertrauen in die Funktionsfähigkeit des Systems, das Grundlage der Selbstbestimmung ist. Das Vertrauen in das informationstechnische System ist essenziell für eine freie und ungezwungene Kommunikation, mithin Grundvoraussetzung für eine ungehinderte Ausübung der Meinungsfreiheit und Entfaltung der Persönlichkeit. Nur wenn der Mensch darauf vertrauen kann, dass nur solche Informationen an die Öffentlichkeit gelangen, die er freiwillig offenbart, und nicht zusätzlich auch solche Informationen, die durch eine Infiltrierung des Systems in die Hände eines unbefugten Dritten geraten, kann der Einzelne sich bei der Nutzung informationstechnischer Systeme frei verhalten.

Als Schutz- und Abwehrrecht muss das Grundrecht nicht nur vor staatlicher Ausspähung, sondern auch vor den Interessen der Privatwirtschaft schützen.[94] Gerade durch die Verbreitung smarter Technologien erhöht sich das Potenzial zum unbefugten Eindringen in informationstechnische Systeme, die große Mengen teils sehr sensitiver Da-

87 BVerfGE 120, 274 (314).
88 Ausführlich zur Frage der Komplexität einzelner informationstechnischer Systeme *Skistims*, Smart Home, Dissertation Uni Kassel 2015 i. E., 102-107.
89 BVerfGE 120, 274 (314); *Murswiek*, in: Sachs 2011, Art. 2 GG, Rn. 73b.
90 *Skistims*, Smart Home, Dissertation Uni Kassel 2015 i. E., 126.
91 BVerfGE 120, 274 (314).
92 *Hoffmann-Riem*, JZ 2008, 1009 (1010).
93 *Murswiek*, in: Sachs 2011, Art. 2 GG, Rn. 73c; *Hornung*, CR 2008, 299 (303); *Roßnagel/Schnabel*, NJW 2008, 3534 (3536).
94 *Kutscha*, DuD 2012, 391 (392).

ten aus allen Lebensbereichen vorhalten und so durch den etwaigen Zugriff Dritter zur Ausspähung der Betroffenen beitragen.

Recht am eigenen Wort und Bild

Das Schutzbedürfnis für das Recht am eigenen Wort und Bild erfährt durch moderne Kommunikations- und Informationstechnologien eine neue Relevanz, die der Möglichkeit geschuldet ist, „das Erscheinungsbild eines Menschen in einer bestimmten Situation von diesem abzulösen, datenmäßig zu fixieren und jederzeit vor einem unüberschaubaren Personenkreis zu reproduzieren".[95] Risiken für das Recht am eigenen Wort und Bild ergeben sich zunächst durch die rasante Verbreitung leistungsfähiger Kameras und Sprachsensoren, wie sie auch in Smart-TV-Geräten zu finden sind. Insbesondere durch die Anbindung der Geräte an das Internet können die angefertigten Bilder und Tonaufnahmen grundsätzlich schnell hochgeladen und veröffentlicht werden. Gerade diese Möglichkeiten beeinträchtigen durch ihre geringe Auffälligkeit die Selbstbestimmung des Einzelnen, die die Durchsetzung dieses Rechts um ein Vielfaches erschwert.

Das Recht am eigenen Bild ist in den §§ 22 ff. Kunsturhebergesetz (KunstUrhG) gesetzlich geregelt. Die Verbreitung und öffentliche Zurschaustellung eines Bildnisses ist gemäß § 22 Abs. 1 KunstUrhG nur mit Einwilligung des Abgebildeten zulässig. Es obliegt dem Einzelnen, selbst zu entscheiden, wann ein Abbild von ihm veröffentlicht werden darf. Unter welchen Umständen und in welchen Situationen das Bild entstanden ist, ist im Rahmen des § 22 Abs. 1 KunstUrhG nicht entscheidend. Daher bedarf es auch keiner Unterscheidung, aus welchem Lebensbereich das Bild stammt. Nur unter den Voraussetzungen des § 23 KunstUrhG kann die Selbstbestimmung eingeschränkt werden. Gemäß § 23 KunstUrhG ist eine Einwilligung nicht erforderlich, wenn es sich zum Beispiel um ein Bildnis aus dem Bereich der Zeitgeschichte handelt (Nr. 1), die abgebildete Person nur Beiwerk ist (Nr. 2), das Bildnis im Rahmen von Versammlungen und Aufzügen entstanden ist (Nr. 3) oder ein nicht auf Bestellung angefertigtes Bild einem höheren Interesse der Kunst dient (Nr. 4). Gemäß § 23 Abs. 2 KunstUrhG darf kein entgegenstehendes berechtigtes Interesse des Abgebildeten vorliegen.

Die Bedrohung des Rechts am eigenen Wort und Bild im Rahmen von Smart-TV ist weitestgehend von der konkreten Gestaltung der Technik abhängig. Da die Geräte mit Mikrofonen und Kameras ausgestattet sind, ist theoretisch also eine unbegrenzte und unbemerkte Speicherung und Übertragung von Bild- und Tonaufnahmen möglich. Solange die technische Ausgestaltung jedoch vorsieht, dass Aufnahmen erst auf eindeutigen Sprachbefehl oder Tastendruck hin beginnen, findet diese im Bewusstsein und mit Einwilligung des Betroffenen statt. Wird die Sprachnachricht außerdem nur lokal auf dem Gerät verarbeitet und nicht an externe Server übertragen, erhalten unbefugte Dritte keinen Zugang zu den personenbezogenen Daten des Betroffenen.[96]

Problematisch ist darüber hinaus, wenn sich unbeteiligte Dritte in Räumlichkeiten aufhalten in denen sich Smart-TV-Geräte befinden. Kameras und Mikrophone können grundsätzlich deren Wort und Bild aufzeichnen, möglicherweise ohne dass den betroffenen Dritten dies bewusst ist. Solange jedoch eine Aufnahme nur nach vorherigem eindeutigen Sprachbefehl möglich ist, ist eine Verletzung des Rechts am eigene Wort und Bild nicht gegeben.

Informationsfreiheit

Fernsehen bildet seit jeher einen wichtigen Pfeiler zur Informationsbeschaffung und Meinungsbildung. Die Verbreitung des Internets hat die Möglichkeiten der Informati-

95 BVerfGE 101, 361 (381).

96 Zu den technischen Ausgestaltungen Stiftung Warentest 5/2014, 40, 41, zitiert in *Schmidtmann/Schwiering*, ZD 2014, 448, Fn. 18; *Spehr/Tunze*, Horchposten im Wohnzimmer, Frankfurter Allgemeine Sonntagszeitung vom 15.2.2015, V9.

onsbeschaffung erweitert, ohne die Bedeutung des Fernsehens wesentlich geschmälert zu haben. Smart-TV-Systeme verbinden nun beide Quellen miteinander und geben den Nutzenden die Möglichkeit, sich beliebig mit Hilfe eines Geräts aus verschiedenen Quellen zu unterrichten. Art. 5 Abs. 1 Satz 1 GG gewährleistet diese Informationsfreiheit, sich selbst ungehindert aus allgemein zugänglichen Quellen zu unterrichten. Neben dem Fernsehen gilt auch das Internet gilt als solch eine allgemein zugängliche Quelle, sofern die Inhalte frei verfügbar sind.[97] Die Informationsfreiheit ist unabdingbare Voraussetzung für die Meinungsfreiheit,[98] also das aktive Bilden, Äußern und Verbreiten von Meinungen. Geschützt ist ebenso der damit zusammenhängende Prozess der Informationsübertragung, also der Abruf der Information oder der Kommunikationsvorgang.[99]

Die Informationsfreiheit findet ihre Grenze dort, wo ein Eingriff gemäß Art. 5 Abs. 2 GG zur Wahrung eines Rechtsguts[100] sowie zum Jugend- oder Ehrschutz gerechtfertigt ist. Im Rahmen des Smart-TV sind Eingriffe in die Informationsfreiheit der Nutzenden denkbar, etwa indem der Zugang zu allgemein zugänglichen Informationen erschwert oder verhindert oder die Äußerung einer Meinung verboten wird. Das gilt zunächst nur im Verhältnis des Staates zum Bürger. Darüber hinaus besteht aber auch eine Schutzpflicht des Staates, den Einzelnen vor Beeinträchtigung der Meinungs- und Informationsfreiheit durch Dritte zu schützen,[101] etwa weil eine einseitige Informationsmacht sich in der Hand weniger Anbieter konzentriert. Darüber hinaus liegt eine Einschränkung auch dann vor, wenn der Betroffene daran gehindert wird, Informationen anonym einzuholen.[102]

Fernmeldegeheimnis

Das Fernmeldegeheimnis aus Art. 10 GG schützt die Freiheit und Unverletzlichkeit der auf Fernmeldetechnik angewiesenen Informationsübertragung und Kommunikation.[103] Fernmeldeverkehr ist dabei jede fernmeldetechnische Übertragung von Informationen an individuelle Empfänger. Als technikoffenes Grundrecht sind alle Möglichkeiten der Fernkommunikation umfasst, unabhängig von der konkreten Übertragungstechnik, solange diese Individualkommunikation ermöglicht, zum Beispiel Telefon, SMS, E-Mail, Instant Messaging-Dienste, Internet-Telefonie (VoIP) etc.[104] Da Smart-TV-Geräte mit einem Rückkanal ausgestattet sind, der die Datenübertragung vom Einzelnen zum Zugangsanbieter ermöglicht, fällt auch Datenübertragung im Rahmen von Smart-TV unter das Fernmeldegeheimnis. Ein Eingriff in das Fernmeldegeheimnis liegt vor, wenn sich unbefugte Dritte Kenntnis vom Inhalt der Datenübertragung zwischen dem TV-Gerät und dem Zugangsanbieter verschaffen. Das Fernmeldegeheimnis entfaltet seinen Schutz nur auf dem Übertragungsweg;[105] nach Abschluss des Kommunikationsvorgangs gewährleisten andere Grundrechte den Schutz des Einzelnen, insbesondere das allgemeine Persönlichkeitsrecht in den Ausprägungen der informationellen Selbstbestimmung und Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

97 *Jarass*, in: Jarass/Pieroth 2012, Art. 5 GG, Rn. 16; *Schemmer*, in: Epping/Hillgruber 2014, Art. 5 GG, Rn. 26; *Holznagel*, AfP 2011, 532 (533 f.).
98 BVerfGE 27, 71 (81).
99 *Jarass*, in: Jarass/Pieroth 2012, Art. 5 GG, Rn. 6; *Grabenwarter*, in: Maunz/Dürig 2013, Art. 5 GG, Rn. 46 m.w.N.; *Bethge*, in: Sachs 2011, Art. 5 GG, Rn. 38a.
100 Zum Beispiel BVerfGE 113, 63 (79); 117, 244 (260).
101 BVerfGE 73, 118 (201); 97, 125 (146); 99, 185 (194 f.).
102 *Weichert*, DuD 2014, 528 (530).
103 *Albers* 2005, 244.
104 *Jarass*, in: Jarass/Pieroth 2012, Art. 10 GG, Rn. 5; *Gusy*, in: v. Mangoldt/Klein/Starck 2010, Art. 10 GG, Rn. 19; *Pagenkopf*, in: Sachs 2011, Art. 10 GG, Rn. 14.
105 BVerfGE 115, 166 (184 f.); *Jarass*, in: Jarass/Pieroth 2012, Art. 10 GG, Rn. 2; *Gusy*, in: v. Mangoldt/Klein/Starck 2010, Art. 10 Rn. 24.

Unverletzlichkeit der Wohnung

Die Wohnung als elementarer Lebensraum und Mittelpunkt menschlicher Existenz[106] dient der selbstbestimmten Abschirmung des Privatbereichs, denn zur freien Entfaltung der Persönlichkeit bedarf es eines absolut geschützten Eigenbereichs.[107] Art. 13 Abs. 1 GG gewährleistet daher die Unverletzlichkeit der Wohnung. Vom Schutzbereich umfasst ist die räumliche Sphäre der Wohnung, die der allgemeinen Zugänglichkeit durch eine räumliche Abschirmung entzogen und zur Stätte privaten Lebens und Wirkens gemacht ist.[108] Ein Eingriff in das Grundrecht liegt auch in der Öffnung der räumlich geschützten Sphäre mittels moderner Technik ohne Wissen des Betroffenen, zum Beispiel durch das Aufstellen technischer Vorrichtungen zur Ausspähung des Einzelnen in seiner Wohnung.[109]

Im Bereich des Smart-TV-Geräts ergibt sich ein erhöhtes Risiko für die Unverletzlichkeit der Wohnung. Art. 13 GG bindet jedoch nur den die staatliche Gewalt und entfaltet keine unmittelbare Drittwirkung hinsichtlich privater Akteure.[110] Bei Ausnutzung oder Infiltration des Smart-TV-Geräts durch die in Kap. 2.2 dargestellten Akteure mit dem Ziel der Erhebung personenbezogener Daten und zur Ausspähung der Kommunikation sind ausschließlich das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG sowie die Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG einschlägig.[111]

5.1.2 TV-Sender

TV-Sender können sich auf die Rundfunkfreiheit aus Art. 5 Abs. 1 Satz 2 GG berufen. Rundfunk ist ein linearer Informations- und Kommunikationsdienst, für die Allgemeinheit und zum zeitgleichen Empfang bestimmte Veranstaltung und Verbreitung von Angeboten in Bewegtbild und Ton entlang eines Sendeplans unter Einsatz elektromagnetischer Schwingungen. Dem entspricht auch die Regelung in § 2 Abs. 1 Satz 1 Rundfunkstaatsvertrag (RStV). Nur die linear ausgestrahlten Programme über Smart-TV gelten als Rundfunk, etwa das Fernsehprogramm und Videotext; sonstige Angebote, die über das TV-Gerät zur Verfügung gestellt werden, insbesondere individualisierte Angebote, die personenbezogene Daten des Nutzenden erheben und verwenden, fallen nicht unter den Rundfunkbegriff, sondern unterliegen als Telemedium im Sinne von § 2 Abs. 1 Satz 3 RStV nicht dem besonderen verfassungsrechtlichen Schutz der Rundfunkfreiheit;[112] die TV-Sender können sich in diesem Fall aber auf die Berufsausübungsfreiheit berufen. Für die Rundfunkfreiheit gelten die gleichen Grenzen wie für die Meinungs- und Informationsfreiheit: Ein Eingriff ist gerechtfertigt auf Grund allgemeiner Gesetze, zum Schutz der Jugend und der persönlichen Ehre.

5.1.3 Smart-TV-Hersteller

Smart-TV-Hersteller können sich sowohl auf ihre Berufs- als auch Eigentumsfreiheit berufen.[113] Art 12 Abs. 1 GG schützt die berufliche Tätigkeit der Herstellung und des Vertriebs von Smart-TV-Geräten. Eingriffe bedürfen einer gesetzlichen Grundlage. Als

106 BVerfGE 18, 121 (131 f.).
107 BVerfGE 42, 212 (219); 89, 1 (12); *Gornig*, in: v. Mangoldt/Klein/Starck 2010, Art. 13 GG, Rn. 1; *Kühne*, in: Sachs 2011, Art. 13 GG, Rn. 9.
108 BGHSt 44, 138 (140); *Jarass*, in: Jarass/Pieroth 2012, Art. 10 GG, Rn. 4; *Gornig*, in: v. Mangoldt/Klein/Starck 2010, Art. 13 GG, Rn. 15.
109 *Jarass*, in: Jarass/Pieroth 2012, Art. 10 GG, Rn. 7; *Gornig*, in: v. Mangoldt/Klein/Starck 2010, Art. 13 GG, Rn. 43.
110 *Gornig*, in: v. Mangoldt/Klein/Starck 2010, Art. 13 GG, Rn. 12, 41.
111 *Jarass*, in: Jarass/Pieroth 2012, Art. 10 GG, Rn. 2 und Art. 13 GG, Rn. 2; *Gornig*, in: v. Mangoldt/Klein/Starck 2010, Art. 13 GG, Rn. 49; *Hoffmann-Riem*, JZ 2008, 1009 (1021).
112 *Schmidtmann/Schwiering*, ZD 2014, 448 (449); wohl auch *Weichert*, DuD 2014, 528 (530).
113 *Weichert*, DuD 2014, 528 (530).

Rechtfertigung für einen Eingriff in die Berufsfreiheit kommt im Rahmen von Smart-TV vor allem kollidierendes Verfassungsrecht, insbesondere die informationelle Selbstbestimmung und Informationsfreiheit der Nutzenden, in Betracht. Die Eigentumsfreiheit aus Art. 14 GG schützt das geistige[114] und materielle Eigentum; Schranken der Eigentumsfreiheit und Rechte und Pflichten des Eigentümers ergeben sich aus Allgemeinwohlbelangen und sind in allgemeinen Gesetzen niedergelegt.[115]

5.2 Datenschutzrechtliche Rahmenbedingungen

Smart-TV-Geräte ermöglichen den Nutzenden nicht nur den herkömmlichen Fernsehgenuss, sondern bieten durch den in dem Fernsehgerät eingebauten Web-Browser die Möglichkeit, interaktive Web-Angebote und Zusatzdienste in Anspruch zu nehmen. Das herkömmliche Fernsehgerät mutiert hierdurch zu einem Hybriden, der die Grenzen zwischen Fernsehen und Internet für den Nutzenden teilweise verschmelzen lässt. Während die klassische, lineare Fernsehtechnik den rundfunkrechtlichen Regelungen unterworfen ist, führt die neu entstandene Konvergenz mit Internetdiensten dazu, dass aufgrund der digitalen Übertragungsart eine Anwendbarkeit des Telemediengesetzes (TMG) in Betracht zu ziehen ist. Der folgende Abschnitt untersucht zunächst Fragen zu personenbezogenen Daten bei Smart-TV-Geräten, um anschließend die akteurspezifischen Erlaubnisnormen zur Verarbeitung dieser Daten zu erläutern.

5.2.1 Personenbezogene Daten bei Smart-TV-Geräten

Bei der Nutzung von Smart-TV-Geräten fällt eine erhebliche Menge Daten an. Der folgende Abschnitt wird beleuchten, welche Daten konkret erhoben werden und welche Bedrohungen sich hieraus für die Nutzenden ableiten. Voraussetzung für die Anwendung der Datenschutzgesetze ist zunächst, dass es sich bei den relevanten Daten auch um solche mit Personenbezug handelt. Ob und in welchem Umfang ein Personenbezug besteht, wird im Anschluss erläutert.

Bestands-, Nutzungs- und Inhaltsdaten

Personenbezogene Daten werden in drei Kategorien unterteilt: Bestandsdaten, Nutzungsdaten und Inhaltsdaten. Bestandsdaten sind gemäß § 14 Abs. 1 TMG personenbezogene Daten eines Nutzenden, die zur Begründung und Durchführung eines Vertragsverhältnisses zwischen dem Diensteanbieter und Nutzenden eines Telemediums erforderlich sind. Je nach Art des Dienstes fallen darunter Account-Daten, also Name, E-Mail-Adresse, Benutzername, Kennwort, gegebenenfalls Geburtsdatum und bei zahlungspflichtigen Diensten auch die Zahlungsinformationen.[116] Bestandsdaten stehen gemäß § 14 Abs. 1 TMG grundsätzlich nur dem Diensteanbieter zur Verfügung und dürfen von diesem nur für die in § 14 TMG genannten Zwecke verwendet werden.

Nutzungsdaten sind gemäß § 15 Abs. 1 Satz 1 TMG personenbezogene Daten, die zur Inanspruchnahme und Abrechnung von Telemedien erforderlich sind. Zu Nutzungsdaten zählen zum Beispiel Merkmale zur Identifikation des Nutzenden wie Nutzername, Passwort oder unter Umständen die IP-Adresse;[117] Angaben zu Beginn, Ende und Umfang der jeweiligen Nutzung, Systeminformationen wie das verwendete Gerät, Be-

114 *Depenheuer*, in: v. Mangoldt/Klein/Starck 2010, Art. 14 GG, Rn. 369.
115 *Depenheuer*, in: v. Mangoldt/Klein/Starck 2010, Art. 14 GG, Rn. 220, 225.
116 *Dix*, in: Roßnagel 2013, § 14 TMG, Rn. 22-26; *Zscherpe*, in: Taeger/Gabel 2013, § 14 TMG, Rn. 12-18.
117 Zum Personenbezug von statischen und dynamischen IP-Adressen ausführlich zum Beispiel *Dammann*, in: Simitis 2014, § 3 BDSG, Rn. 63; *Moos*, in: Taeger/Gabel 2013, § 11 TMG, Rn. 24 ff.; *Zscherpe*, in: Taeger/Gabel 2013, § 14 TMG, Rn. 19 ff.; *Krüger/Maucher*, MMR 2011, 433; *Schmidtmann/Schwiering*, ZD 2014, 448 (450).

triebssystem oder Browser;[118] aber auch die eingegebenen Suchbegriffe und Zielseiten der spezifischen Anfragen.[119] Solche Daten können dem Diensteanbieter zum Beispiel Aufschluss über Surfverhalten oder Interessen des Nutzenden geben. Im Gegensatz zu Bestandsdaten sind Nutzungsdaten auf das konkrete Nutzungsverhältnis beschränkt und sind nach Ende des konkreten Nutzungsvorgangs zu löschen, sofern sie nicht zu Zwecken der Abrechnung nach § 15 Abs. 4, 6 und 7 TMG verwendet werden dürfen. In ihrem Anwendungsbereich überschneiden sich also Bestands- und Nutzungsdaten und sind je nach Verwendungszusammenhang entweder als Bestands- oder Nutzungsdatum einzuordnen.[120]

Alle übrigen Daten, die sich bei der Nutzung des Smart-TV-Geräts durch den Nutzenden ergeben und nicht für die Erbringung des Dienstes oder dessen Abrechnung essenziell sind, sind Inhaltsdaten. Deren Zulässigkeit der Verarbeitung richtet sich für den Diensteanbieter nach § 28 BDSG[121], sofern die Daten personenbezogen sind. Inhaltsdaten sind zum Beispiel Profildaten, mit denen der Nutzende sein persönliches Profil personalisiert. Auch ableitbare Daten, die sich aus der Korrelation und Kombination vorhandener Daten ergeben und zum Beispiel Aufschluss über Interessen, Bildungsgrad, politische oder religiöse Einstellung oder den ethnischen Hintergrund zulassen,[122] gehören zu den Inhaltsdaten.

Personenbezug von Smart-TV-Daten

In allen dargestellten Bedrohungsszenarien ist Voraussetzung für die Anwendbarkeit der Datenschutzgesetze der Personenbezug elektronischer Daten. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, dem Betroffenen. Personenbezogen sind Daten, wenn sie Angaben enthalten, die direkt auf die Person des Betroffenen schließen lassen. Personenbeziehbarkeit ist gegeben, wenn die betroffene Person durch eigenes oder verfügbares Zusatzwissen identifiziert werden kann. Da dieses Zusatzwissen unter Beachtung vorhandener Ressourcen für jede verantwortliche Stelle unterschiedlich ist, muss der Personenbezug relativ zu den Möglichkeiten der jeweiligen verantwortlichen Stelle bestimmt werden.[123] Die Bestimmbarkeit einer Person ist dann praktisch ausgeschlossen, wenn der Aufwand an Zeit, Kosten und Arbeitskraft die Identifizierung des Betroffenen praktisch unmöglich machen.[124] In § 3 Abs. 9 BDSG sind besondere Arten personenbezogener Daten genannt, deren Erhebung, Verarbeitung und Nutzung besonders strengen Voraussetzungen unterliegen: Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.

Wie bereits dargestellt, werden durch die Nutzung eines Smart-TV-Systems zahlreiche Daten erhoben. Neben Konto-, Registrierungsdaten und gerätespezifischen Daten werden Daten bezüglich der Interaktionen der Nutzenden, die Rückschlüsse auf die Nutzung und das Fernsehverhalten (individueller TV-Konsum, Lieblingsprogramme, Internetdienste, Dauer des Konsums oder auch verwendete Suchbegriffe) zulassen, erfasst und übertragen. Unter diesen Voraussetzungen können grundsätzlich sämtliche Daten, die bei der Nutzung des Smart-TV-Systems anfallen, personenbezogen sein oder durch

118 *Zscherpe*, in: Taeger/Gabel 2013, § 15 TMG, Rn. 17; *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 43f.
119 *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 43; *Lerch u. a.*, MMR 2010, 454 (456).
120 *Zscherpe*, in: Taeger/Gabel 2013, § 15 TMG, Rn. 16.
121 Im Falle der öffentlich-rechtlichen Sendeanstalten treten an diese Stelle gegebenenfalls die jeweiligen Landesdatenschutzgesetze.
122 Ausführlich Kap. 5.2.1.
123 *Bergmann/Möhrle/Herb* 2015, § 3 BDSG, Rn. 16.
124 *Dammann*, in: Simitis 2014, § 3 BDSG, Rn. 23, 25.

Kombination mit weiteren Daten personenbezogen werden. Personenbezug entsteht nicht erst bei Preisgabe des Namens, etwa durch Registrierung mit einer E-Mail-Adresse oder Eingabe von Zahlungsinformationen. Zur Identifizierung einer Person als ein spezifischer Nutzender, zum Beispiel in einem Mehrpersonenhaushalt, sind bereits Fernsehverhaltensdaten ausreichend, um eindeutige Merkmale zu liefern und ihn so zum Beispiel zum Objekt personenbezogener Werbeeinblendungen machen.[125]

5.2.2 Akteur-spezifische Erlaubnisnormen

Datenerhebung, -verarbeitung und -nutzung ist nur zulässig, sofern eine wirksame, informierte Einwilligung des Betroffenen vorliegt oder eine gesetzliche Ermächtigungsgrundlage diese zulässt. Im Folgenden werden die gesetzlichen Ermächtigungsgrundlagen für die bei der Datenerhebung, -verarbeitung und -nutzung beteiligten Akteure untersucht.

Beim Einsatz von Smart-TV-Systemen kommen alle in Kap. 2 identifizierten Akteure als verantwortliche Stelle in Betracht: TV-Sender, Inhaltsanbieter, Gerätehersteller, Servicetechniker und sonstige Akteure, soweit diese im konkreten Fall personenbezogene Daten verarbeiten. Als verantwortliche Stelle wird gemäß § 3 Abs. 7 BDSG jede Person oder Stelle bezeichnet, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.[126] Die verantwortliche Stelle ist der Adressat der datenschutzrechtlichen Erlaubnisnormen und unterliegt der Kontrolle durch die Aufsichtsbehörden, sofern die nationalen Datenschutzregeln Anwendung finden.

Anwendbarkeit nationalen Datenschutzrechts

Deutsches Recht im Allgemeinen und datenschutzrechtliche Regelungen im Besonderen können ihren Schutz nur entfalten, wenn diese nach den Kollisionsnormen anwendbar sind. Art. 4 Abs. 1 lit. a) DSRL erklärt das Recht des jeweiligen Mitgliedstaats für anwendbar, in welchem der Gerätehersteller die Datenverarbeitung im Rahmen einer Niederlassung ausführt. Art. 4 Abs. 1 lit. c) DSRL setzt unter anderem voraus, dass das jeweilige mitgliedstaatliche Recht anwendbar ist, wenn personenbezogene Daten von dem für die Verarbeitung Verantwortlichen verarbeitet werden, der nicht im Gemeinschaftsgebiet niedergelassen ist und zum Zweck der Verarbeitung auf automatisierte oder nicht automatisierte Mittel im Inland zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaates gelegen sind. § 1 Abs. 5 BDSG setzt die Inhalte der Richtlinie um.[127] Damit ist § 1 Abs. 5 BDSG die universelle Kollisionsnorm zur Bestimmung der Anwendbarkeit deutschen Datenschutzrechts. Sie gilt auch, soweit das Telemediengesetz vorrangig einschlägig ist, da gemäß § 3 Abs. 3 Nr. 4 TMG die Anwendbarkeit des deutschen Rechts in Bezug auf den Schutz personenbezogener Daten nicht durch das Herkunftslandprinzip bestimmt wird, sondern die allgemeinen Regeln des Bundesdatenschutzgesetzes gelten.

Aus § 1 Abs. 5 BDSG ergeben sich zwei Hauptkonstellationen bei der Bestimmung des anwendbaren Rechts. Zu unterscheiden ist danach, ob der Gerätehersteller als die verantwortliche Stelle in einem Mitgliedstaat der Europäischen Union beziehungsweise in einem Vertragsstaat des Europäischen Wirtschaftsraums gelegen ist oder aber in einem Drittstaat.

125 *Weichert*, DuD 2014, 528 (530); ähnlich *Kannenberg*, Google Fiber: Maßgeschneiderte TV-Werbung für Glasfaserkunden, heise online vom 23.3.2015, http://heise.de/-2583103.
126 *Buchner*, in: Taeger/Gabel 2013, § 3 BDSG, Rn. 52 ff.
127 *Dammann*, in: Simitis 2014, § 1 BDSG, Rn. 198; *Gabel*, in: Taeger/Gabel 2013, § 1 BDSG, Rn. 49.

Ist die verantwortliche Stelle in einem anderen Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens des Europäischen Wirtschaftsraums[128] gelegen und erhebt, verarbeitet oder nutzt diese von dort aus Daten im Inland, also Deutschland (so genanntes Sitzlandprinzip),[129] ist in diesem Fall das Bundesdatenschutzgesetz gemäß § 1 Abs. 5 Satz 1 BDSG nicht anwendbar, es sei denn, die verantwortliche Stelle erhebt diese Daten durch eine Niederlassung im Inland. Eine solche Niederlassung ist eine feste Einrichtung, innerhalb deren Tätigkeit personenbezogene Daten verarbeitet werden.[130] Ausreichend für eine solche Tätigkeit sind unterstützende Arbeiten wie Marketingmaßnahmen.[131]

Das Bundesdatenschutzgesetz findet hingegen gemäß § 1 Abs. 5 Satz 2-4 BDSG dann Anwendung, wenn die verantwortliche Stelle nicht in einem Mitgliedstaat der Europäischen Union oder einem Vertragsstaat des Europäischen Wirtschaftsraums gelegen ist, sondern in einem Drittstaat, und Daten im Inland erhebt, verarbeitet oder nutzt (so genanntes Territorialprinzip).[132] Dafür ist ein Rückgriff auf technische Mittel notwendig. „Mittel" im Sinne der Datenschutzrichtlinie sind körperliche Einrichtungen, die der Verarbeitung personenbezogener Daten dienen,[133] also die Hardware der Nutzenden. „Zurückgreifen" auf diese Mittel umfasst die Notwendigkeit, dass die verantwortliche Stelle aktiv auf diese Mittel einwirkt, zumindest über die Mittel der Erhebung, Verarbeitung und Nutzung entscheiden können oder steuernd Einfluss auf diese haben, etwa durch Cookies oder Software.[134] Nicht darunter fällt jedoch die bloße selbstbestimmte Eingabe von Daten durch den Nutzenden.[135] Ist die Software auf dem Smart-TV-Gerät geeignet, über Formulardaten hinausgehend personenbezogene Daten des Nutzenden zu erheben und zu analysieren, beispielsweise wenn Daten zum Fernsehverhalten des Nutzenden gewonnen werden, dann liegt ein Rückgriff auf im Inland gelegene Mittel vor mit der Folge, dass das deutsche Datenschutzrecht Anwendung findet.

HbbTV als Telemediendienst

Die Anwendbarkeit des Telemediengesetzes setzt zunächst voraus, dass es sich bei den HbbTV-Anwendungen um so genannte Telemedien handelt. Telemedien sind in § 1 Abs. 1 Satz 1 TMG sowie in § 2 Abs. 1 Satz 3 RStV als elektronische Informations- und Kommunikationsdienste definiert, soweit sie nicht Telekommunikation oder Rundfunk sind. Telekommunikation sind gemäß § 3 Nr. 24 TKG Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Das Rundfunkprogramm als solches und gleichgestellte Dienste wie Web-Casting und Live-Streaming sind als Rundfunk zu qualifizieren und damit keine Telemediendienste.[136] Hingegen gehören Radio- und Fernsehtext, Teleshopping und Video-on-Demand zu den klassischen Telemedien.[137]

128 Island, Liechtenstein und Norwegen.
129 BT-Drs. 14/4329, 31; *Dammann*, RDV 2002, 70 (71); *Wagner* 2006, 202; *Gabel*, in: Taeger/Gabel 2013, § 1 BDSG, Rn. 54.
130 Erwägungsgrund 19 der Richtlinie 95/46/EG;
131 EuGH, Urteil vom 13.5.2014, Rs. C‑131/12, Rn. 55; *Piltz*, K&R 2014, 566 (567).
132 BT-Drs. 14/4329, 31; *Gola/Klug/Körffer*, in: Gola/Schomerus 2015, § 1 BDSG, Rn. 28; *Gabel*, in: Taeger/Gabel 2013, § 1 BDSG, Rn. 54; *Dammann*, in: Simitis 2014, § 1 BDSG, Rn. 199 f.
133 Mit Hinweis auf die englische Sprachfassung „equipment" *Dammann*, in: Simitis 2014, § 1 BDSG, Rn. 220; *Dammann*, RDV 2002, 70 (74); *Piltz*, K&R 2013, 292 (294 f.).
134 Herrschende Meinung *Dammann*, RDV 2002, 70 (74); *Wagner* 2006, 204; *Jandt*, DuD 2008, 664 (669); *Alich/Nolte*, CR 2011, 741 (742); *Piltz*, K&R 2013, 292 (295) – mit Hinweis auf die englische Sprachfassung „make use of"; *Gabel*, in: Taeger/Gabel 2013, § 1 BDSG, Rn. 59; *Dammann*, in: Simitis 2014, § 1 BDSG, Rn. 220; für ein Zwischenmaß plädierend *Art. 29-Gruppe*, WP179, 25; nicht nach Beherrschbarkeit des Mittels differenzierend *Nolte*, ZRP 2011, 236 (239).
135 *Dammann*, in: Simitis 2014, § 1 BDSG, Rn. 223; *Gabel*, in: Taeger/Gabel 2013, BDSG § 1 Rdnr. 59.
136 BT-Drs. 16/3078, 13.
137 BT-Drs. 16/3078, 13; *Roßnagel*, NVwZ 2007, 743.

Die Abgrenzung des Telemediums vom Rundfunk ist Voraussetzung für die Anwendung der datenschutzrechtlichen Regelungen. Für die öffentlich-rechtlichen TV-Sender gelten die jeweiligen Landesstaatsverträge; für Privatsender gilt der Rundfunkstaatsvertrag. Liegt keine journalistisch-redaktionelle Privilegierung vor, sondern eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu sonstigen Zwecken, gelten gemäß § 16 ZDF-Staatsvertrag bzw. § 47 Abs. 1 RStV die datenschutzrechtlichen Regelungen des Telemediengesetzes, also §§ 11 ff. TMG.[138]

Mittels HbbTV lassen sich sowohl spezielle rundfunkbezogene als auch vom Rundfunksignal unabhängige Anwendungen aufrufen, die gleichwohl als Telemedien eingeordnet werden. Rundfunkbezogene Anwendungen lassen sich mit Hilfe des „Red Buttons" auf der Fernbedienung aus dem laufenden, linearen Fernsehprogramm heraus starten. Dem Nutzenden werden auf diesem Wege Zusatzinformationen zum laufenden Fernsehprogramm, die in senderspezifischen Mediatheken enthalten sind, zum Abruf verfügbar gemacht. Dass ein solches Zusatzangebot verfügbar ist, wird auf dem Fernsehbildschirm durch Einblendung des „Red Button"-Emblems angezeigt.[139] Anbieter jener so genannten rundfunkbezogenen Anwendungen[140] sind die Fernsehsender.[141] Neben den rundfunkbezogenen Anwendungen ermöglicht HbbTV auch zusätzlich den Zugriff auf von der Übertragung des Rundfunksignals unabhängige Anwendungen (so genannte *broadcast independent applications*)[142], welche von unterschiedlichen Anbietern stammen und wie bei nicht HbbTV-fähigen Smart-TV-Geräten als Apps auf dem Herstellerportal abrufbar sind (TV-Apps).[143]

Sowohl bei rundfunkbezogenen als auch bei vom Rundfunksignal unabhängigen Anwendungen erschöpft sich der Großteil der HbbTV-Anwendungen nicht in der bloßen telekommunikationsrechtlichen Signalübertragung.[144] Alle Zusatzdienste des Smart-TV-Systems sind mithin als Telemedium einzuordnen, auch sofern während des Rundfunkprogramms personenbezogene Daten des Nutzenden erhoben, verarbeitet und genutzt werden.[145] Werden Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt, unterliegen diese daher als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Dessen Vorschriften (§§ 11 ff. TMG) bilden den rechtlichen Maßstab, an welchem die Zulässigkeit der Datenverarbeitung zu messen ist.

TV-Sender

Die Direktverbindung zwischen Sender und Empfänger über das Internet ermöglicht den TV-Sendern regelmäßige Rückmeldungen von den Empfangsgeräten. Anhand der IP-Adressen wäre es den TV-Sendern grundsätzlich möglich, eine Standortbestimmung (Geolokalisierung) der verwendeten Geräte vorzunehmen sowie individuelle, gerätebezogene Nutzungsprofile zu erstellen.[146] § 12 Abs. 1 TMG schreibt für den Bereich der Telemedien allerdings vor, dass die Erhebung und Verwendung personenbezogener Daten zur Bereitstellung von Telemedien durch den Diensteanbieter nur zulässig ist, wenn eine gesetzliche Regelung, die sich ausdrücklich auf Telemedien bezieht, diese Maßnahmen erlaubt oder wenn der Nutzende in diese Maßnahmen eingewilligt hat.

138 *Weichert*, DuD 2014, 528 (534).
139 *Schwartmann* 2014, 3016.
140 Der ETSI Standard spricht hierbei von so genannten broadcast-related autostart applications, vgl. *ETSI* (2012), Nr. 5.3.1., S. 21; *Keber*, RDV 2013, 236 (237).
141 *Schwartmann* 2014, 3016.
142 *ETSI* (2012), Nr. 5.3.1., S. 21; *Keber*, RDV 2013, 236 (237).
143 *Schwartmann* 2014, 3016.
144 *Keber*, RDV 2013, 236 (238); *Schmidtmann/Schwiering*, ZD 2014, 448 (449).
145 *Schmidtmann/Schwiering*, ZD 2014, 448 (449); *Weichert*, DuD 2014, 528 (532, 534).
146 *Weichert*, https://www.datenschutzzentrum.de/vortraege/20140516-weichert-internet-tv.html.

Gesetzliche Erlaubnis aus § 15 Abs. 1 Satz 1 TMG

Das Telemediengesetz unterscheidet – abweichend von den Begriffen des BDSG – zwischen Erhebung und Verwendung personenbezogener Daten und gilt grundsätzlich nur im Anbieter-Nutzer-Verhältnis. Das Telemediengesetz orientiert sich dabei an der gleichlautenden Terminologie der §§ 91 ff. TKG. Das Erheben von Daten ist gemäß § 12 Abs. 3 TMG, § 3 Abs. 3 BDSG das finale, zielgerichtete Beschaffen von Daten als Vorstadium für das Speichern.[147] Das Verwenden personenbezogener Daten ist weit zu verstehen und umfasst alle Vorgänge des Umgangs mit personenbezogenen Daten, also sowohl die Verarbeitung als auch die Nutzung personenbezogener Daten.[148]

Als möglicher Erlaubnistatbestand zur Erhebung von Nutzungsdaten kommt zunächst § 15 Abs. 1 Satz 1 TMG in Betracht. Die Erhebung und Verwertung personenbezogener Daten ist hiernach zulässig, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Bei der Erforderlichkeitsprüfung kommt es immer auf die konkrete Nutzung des Smart-TV an. So ist die Erforderlichkeit dann zu bejahen, wenn die aus dem Rechtsverhältnis folgenden Rechte und Pflichten nur bei der Verwendung der jeweiligen Daten geltend gemacht bzw. erfüllt werden können.[149] Wird zum Beispiel ein zahlungspflichtiges Online-Angebot per Smart-TV gebucht, kann die Erhebung der Nutzungsdaten zu Abrechnungszwecken im Einzelfall erforderlich sein.

Die Erfassung des Medienverhaltens des Nutzenden, zum Beispiel die Nutzungsdauer bestimmter Sendungen oder die Umschaltfrequenz hinsichtlich einzelner Programme, ist jedoch weder zur Inanspruchnahme des Smart-TV-Systems oder zur Vertragsdurchführung noch zur Wahrung berechtigter Interessen des Diensteanbieters erforderlich. Ziel solcher Analysen ist es, Nutzungsstatistiken zu erstellen. Zudem sollen durch die Korrelation mit (pseudonymisierten) Daten anderer Nutzender (Big-Data-Analysen) mittels einer Zweitverwertung Erkenntnisse gewonnen werden, die verborgene, wirtschaftlich nutzbare Aussagepotenziale erschließen sollen.[150] Auf diesem Wege soll die Auslieferung individualisierter Werbeangebote ermöglicht werden.

Bei Daten über das Nutzungsverhalten handelt es sich regelmäßig um Inhaltsdaten. Hierbei sind Inhaltsdaten solche Daten, die nicht zur Inanspruchnahme des Dienstes erforderlich sind, sondern erst im Rahmen der Inanspruchnahme anfallen.[151]

Wie bereits dargestellt, erfolgt eine Auswertung des Nutzerverhaltens nicht erst dann, wenn der „Red Button" ausgelöst wird, sondern bereits schon zu einem früheren Zeitpunkt, in dem der Nutzende den „Red Button" noch nicht ausgelöst hat.[152] Bei HbbTV ist die Auswertung des den Broadcast-Kanal betreffenden Sehverhaltens (TV-Reichweitenmessung) der Nutzenden durch die Rundfunkveranstalter technisch nicht nur dann möglich, wenn die Nutzenden den „Red Button" betätigen und somit HbbTV-Anwendungen abfragen, sondern schon zu einem Zeitpunkt, in dem die Nutzenden den „Red Button" noch nicht ausgelöst haben. Dies liegt in der speziellen Funktionsweise von HbbTV begründet: So ermöglicht es die Rückkanalfähigkeit von HbbTV-Sendern, Fernsehgewohnheiten, -zeiten oder das Surfverhalten zur Erstellung von Nutzerprofilen oder zum Zwecke personalisierter Werbung zu erfassen und auszuwerten.[153] Erfolgt eine solche periodische Anfrage des Nutzerverhaltens in der „Red

147 *Müller-Broich* 2012, § 12 TMG, Rn. 1; *Dammann*, in: Simitis 2014, § 3 BDSG, Rn. 102.
148 *Schulz*, in: Roßnagel 2013, § 12 TMG, Rn. 9; *Müller-Broich* 2012, § 12 TMG, Rn. 1.
149 *Schmidtmann/Schwiering*, ZD 2014, 448 (450).
150 *Arning/Moos*, ZD 2014, 242; *Schmidtmann/Schwierig*, ZD 2014, 448 (450).
151 *Roßnagel*, in: Roßnagel (Hrsg.) 2003, Kap. 7.9, Rn. 37.
152 *Ghiglieri/Oswald/Tews* (2013).
153 *Ghiglieri/Oswald/Tews* (2013); *Schmidtmann/Schwiering*, ZD 2014, 448 (448 f.); *Weber*, ZUM 2011, 455f.

Button"-Ladephase, so ist dies für die Inanspruchnahme des HbbTV-Angebots gerade nicht erforderlich.[154]

Anders hingegen ist die Erhebung der IP-Adresse zu bewerten: Um die angefragten Datenpakete (HbbTV oder TV-App-Inhalt) an die richtige Adresse, also das konkret anfragende Smart-TV-Gerät, zustellen zu können, ist die Erhebung der IP-Adresse erforderlich im Sinne des § 15 Abs. 1 TMG.[155] Gleichwohl ist der Nutzungsvorgang nach Zustellung des Datenpaketes abgeschlossen und die IP-Adresse grundsätzlich zu löschen; eine dauerhafte Speicherung der IP-Adresse ist unzulässig.

Smart-TV-Geräte verfügen zumeist nur über vereinfachte Browser, welche über keinen Cookie-Manager verfügen, der die vorhandenen Daten löschen könnte. Das Setzen von Cookies erleichtert es den TV-Sendern somit, die hieraus gewonnenen Daten zur Erstellung von Nutzerprofilen zu verwenden. Werden Cookies zum Zwecke der Erstellung von Nutzungsprofilen gesetzt, ist dies regelmäßig nur unter der Voraussetzung zulässig, dass Pseudonyme erstellt werden und der Nutzende dem nicht widerspricht (§ 15 Abs. 3 Satz 1 TMG, so genanntes Opt-out).

Gesetzliche Erlaubnis aus § 15 Abs. 3 Satz 2 TMG?

Nahezu alle Privatsender lassen zudem die Abrufe der „Red Button"-Seite mit Hilfe des Werkzeugs „Analytics" durch Google nachverfolgen (tracken). Das Tracking von Zuschauern durch die Sender stellt eine Verwendung von Nutzungsdaten dar, die – wenn das Tracking nicht zum Erbringen des Dienstes erforderlich ist – lediglich pseudonymisiert unter den Voraussetzungen des § 15 Abs. 3 Satz 1 TMG erlaubt ist. Hiernach dürfen Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzende dem nicht widerspricht. Gleichwohl hat der Diensteanbieter den Nutzenden „im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG" auf sein Widerspruchsrecht hinzuweisen (§ 15 Abs. 3 Satz 1 TMG). Die Sender müssen folglich über die Verwendung sowie das Widerspruchsrecht informieren. Möchte ein Nutzender verhindern, dass seine Daten erhoben und verarbeitet werden, so ist den Nutzenden die wirksame Möglichkeit eines Opt-outs einzuräumen, zum Beispiel durch das Löschen lokal gespeicherter Cookies[156]. Dies erfolgt in der Praxis jedoch nicht.

Problematisch ist, dass insbesondere die TV-Apps oftmals die Datenschutzerklärungen des korrespondierenden Web-Angebots übernehmen. So wird der Hinweis gegeben, dass die Annahme von Cookies über den Webbrowser abgewählt werden könne. Ein solcher Hinweis geht gerade bei Smart-TV-Geräten fehl, welche anders als sonstige Internet-Endgeräte wie PCs, Laptops, Tablets oder Smartphones nur über eine reduzierte Browsertechnologie verfügen und die Möglichkeit einer Installation eines Cookie-Managers gerade nicht vorsehen. Zumindest in den Browsereinstellungen muss den Nutzenden die Möglichkeit gegeben werden, technisch die Verwendung von Cookies auszuschalten.[157] Die Nutzenden können die ihnen vorgeschlagenen Handlungsoptionen nicht effektiv nutzen geschweige denn betätigen, da den eingesetzten Geräten die Anzeigemöglichkeiten fehlen, mit denen gegenüber den Nutzenden Transparenz über die Verarbeitungsprozesse hergestellt werden könnte.[158] Die Beeinflussbarkeit durch die Nutzenden kann hierdurch stark eingeschränkt sein.

154 *Schwartmann* 2014, 3018.
155 *Schwartmann* 2014, 3018.
156 Gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, Mai 2014, S. 2, http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/05/Beschluss_Smart_TV.pdf.
157 *Ghiglieri/Oswald/Tews* (2013), S. 11.
158 *Weichert*, https://www.datenschutzzentrum.de/vortraege/20140516-weichert-internet-tv.html.

Die Annahme einer Opt-out-Lösung steht im Widerspruch zur europäischen Gesetzeslage: So fordert die europäische Datenschutzrichtlinie elektronischer Kommunikation (EG-TK-DSRL)[159] eine Opt-in-Lösung, wenn sie innerhalb ihres Art. 5 Abs. 3 statuiert, dass die „Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzer gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer [...] seine Einwilligung gegeben hat". Der Nutzer muss hiernach aktiv in die Verwendung von Cookies einwilligen.

Umstritten ist daher, ob die deutsche Opt-out-Regelung europarechtswidrig ist. Teilweise wird vertreten, dass dieser Widerspruch zwischen europäischer und nationaler Rechtslage dahingehend aufzulösen sei, dass die deutsche Opt-out-Regelung zu kurz greife, so dass nach dem erfolglosen Ablauf der Umsetzungsfrist der europäischen Richtlinie eine unmittelbare Anwendbarkeit des Art. 5 Abs. 3 der EG-TK-DSRL (Opt-in-Regelung) anzunehmen sei.[160]

Werden Richtlinien nicht rechtzeitig umgesetzt, gilt nach dem europarechtlichen Prinzip des „effet utile", dass Richtlinien jedenfalls dann unmittelbare Wirkung zukommt, wenn diese für eine Umsetzung bestimmt genug sind.[161] Ob Art. 5 Abs. 3 n. F. der Richtlinie diesem Standard entspricht, ist umstritten. Nach Auffassung des früheren Bundesbeauftragten für den Datenschutz ist eine direkte Anwendbarkeit gegeben, da die Vorschrift Umstände, unter denen die Vorschrift greift, eindeutig erkennen lässt.[162] Dem ist wegen der verschiedenen denkbaren Umsetzungsvarianten der Richtlinie die nicht ausreichende Bestimmtheit zur direkten Anwendung entgegenzuhalten.[163] Ein weiteres Problem besteht darin, dass die unmittelbare Wirkung nicht umgesetzter Richtlinien nur vertikal, d. h. zwischen Bürger und Staat, gelten kann. Hauptanwendungsgebiet der Cookie-Richtlinie dürften allerdings Unterlassungsklagen und Wettbewerbsstreitigkeiten zwischen Privatrechtssubjekten darstellen.[164] Im Ergebnis ist, trotz der oben zitierten kryptischen Aussage der Europäischen Kommission, derzeit nicht von einer Einwilligungspflicht für pseudonymes Tracking durch Cookies in Deutschland auszugehen.

Unterstellt man die unmittelbare Anwendbarkeit des Art. 5 Abs. 3 der EG-TK-DSRL, so folgt hieraus, dass das Setzen von Cookies zum Zwecke der Reichweitenanalyse, unter anderem durch die Verwendung von Google Analytics, ohne vorherige Zustimmung der Nutzenden grundsätzlich unzulässig ist.[165] Erfolgt, wie bei der Nutzung von Google Analytics, zusätzlich eine Übermittlung ins EU-Drittausland ohne hinreichenden Datenschutzstandard[166], so stellt diese Auslandsübermittlung einen eigenständigen Verarbei-

159 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG L 201, 37.

160 *Keber*, RDV 2013, 236 (243); *EU-Parlament*, Connected TV, 7.

161 *Gärditz*, in: Rengeling/Middeke/Gellermann 2014, Teil 2, § 34, Rn. 37; ausführlich *Seidel*, NJW 1985, 517.

162 *Viefhues*, ZD-Aktuell 2012, 02996.

163 I.E. *Ehmann*, Lexikon für das IT-Recht (2014/2015), 96.

164 *Martinek*, in: Grabitz/Hilf/Nettesheim (2009), Art. 13 RL 94/47/EG, Rn. 257 f.

165 *Schwartmann* 2014, 3018.

166 Eine Übermittlung personenbezogener Daten in ein Drittland ist grundsätzlich nur zulässig, wenn dieses ein angemessenes Schutzniveau gewährleistet. Die Angemessenheit des Schutzniveaus kann durch Entscheidung der Europäischen Kommission festgestellt werden, aber lässt sich auch durch Standardvertragsklauseln sicherstellen. Für die Übermittlung in die USA galt bis Oktober 2015 die Entscheidung der Kommission 2000/520/EG, nach der sich US-amerikanische Unternehmen zur Einhaltung bestimmter Grundsätze verpflichten konnten („Safe Harbor"); diese wurde durch den EuGH mit Urteil vom 6. Oktober 2015, Rs. C-362/14 für nichtig erklärt. Da in diesem Bereich aufgrund der anstehenden Datenschutz-Grundverordnung zukünftig viele Änderungen zu erwarten sind, kann an dieser Stelle nicht genau auf die Problematik der Übermittlung personenbezogener Daten in Drittländer ohne angemessenes Schutzniveau eingegangen werden.

tungszweck dar, welcher für sich allein genommen bereits einer Einwilligung oder aber eines gesonderten Hinweises bedarf.[167]

Informationspflicht nach § 13 TMG

Unabhängig davon, ob man nun ein Opt-out genügen lässt oder aber ein Opt-in der Nutzenden verlangt, stellt die Einholung einer informierten Einwilligung die für Diensteanbieter rechtlich risikoärmste Lösung zum Angebot von Smart-TV-Diensten dar. Diese Lösung vermag es nicht nur Betroffeneninteressen zu schützen, sondern auch Rechtssicherheit herzustellen, bis eine endgültige Klärung der Rechtslage durch die obersten Gerichte erfolgt. Die Nutzenden sind spätestens zu Beginn des Datenverarbeitungsvorganges transparent nach Maßgabe des § 13 TMG zu informieren.

Die Diensteanbieter werden durch § 13 Abs. 1 TMG zur umfassenden und transparenten Information über die Datenverarbeitung verpflichtet. Folglich muss der Nutzende über die Identität des Diensteanbieters, die Art, den Umfang und die Zwecke der Erhebung und Verwendung personenbezogener Daten informiert werden. Ist eine Datenverarbeitung in Staaten außerhalb des Anwendungsbereichs der EU-Datenschutzrichtlinie[168] beabsichtigt – zum Beispiel wenn zur Analyse der Daten Google Analytics genutzt wird –, so erwachsen hieraus zumindest weitere gesonderte Informationspflichten. Die Unterrichtung hat spätestens zu Beginn des Nutzungsvorgangs zu erfolgen[169] und muss sowohl sprachlich als auch ihrer äußeren Gestaltung nach in allgemein verständlicher Form ergehen.

Wie aus § 13 Abs. 1 Satz 2 TMG folgt, gilt die Unterrichtungspflicht auch dann, wenn der Personenbezug erst im Rahmen eines automatisierten Verfahrens, das heißt ohne individuelle Entscheidung des Nutzenden, zu einem späteren Zeitpunkt hergestellt wird, wie dies beispielsweise bei Cookies der Fall ist[170].

Gerätehersteller

Gerätehersteller verarbeiten personenbezogene Daten vor allem dann, wenn sie die Geräte mit Systemupdates versorgen. In dieser Funktion treten Gerätehersteller als Diensteanbieter auf, so dass bei der Verarbeitung von Bestands- und Nutzungsdaten die §§ 11 ff. TMG zu beachten sind.[171] Sollten darüber hinaus Daten verarbeitet werden, die nicht für die Bereitstellung des Systemupdates erforderlich sind, muss die Verarbeitung nach den Vorschriften der §§ 27 ff. BDSG zulässig sein oder die Einwilligung des Betroffenen vorliegen.

Sonstige

Neben den Geräteherstellern und den TV-Sendern verarbeiten auch sonstige Akteure, vor allem Inhaltsanbieter wie Werbetreibende, Streamingdienste, Social-Media-Unternehmen oder Spieleanbieter, bei der Smart-TV-Nutzung personenbezogene Daten. Die datenschutzrechtliche Einordnung jener Vorgänge weicht insoweit nicht von jener des klassischen Internet-Szenarios ab, so dass dies im Rahmen dieses Beitrages nicht weitergehend vertieft wird.

Servicetechniker werden in der Regel personenbezogene Daten verarbeiten, um Probleme des Geräts zu beheben. Da die Verarbeitung hier in der Regel zur Erfüllung eigener Geschäftszwecke erforderlich ist, ist diese nach § 28 BDSG zulässig.

167 *Weichert*, https://www.datenschutzzentrum.de/vortraege/20140516-weichert-internet-tv.html.
168 RL 95/46/EG.
169 BT-Drucks. 14/6098, 28; *Müller-Broich* 2012, § 13 TMG, Rn. 1.
170 *Spindler/Nink*, in: Spindler/Schuster 2015, § 13 TMG, Rn. 5; *Müller-Broich* 2012, § 13 TMG, Rn. 2.
171 *Weichert*, DuD 2014, 528 (532); *Heckmann*, in: jurisPK 2014, Kap. 1, Rn. 35.

5.2.3 Rechtfertigung durch Einwilligungserklärung des Nutzenden

Fehlt eine gesetzliche Ermächtigungsgrundlage zur Erhebung und Verarbeitung personenbezogener Daten des Nutzenden, kann der Datenumgang über eine wirksame Einwilligung des Nutzenden gerechtfertigt werden. Das Telemedienrecht sieht gemäß § 13 Abs. 2 TMG eine Einwilligung in elektronischer Form als ausreichend an, wenn der Nutzende seine Einwilligung bewusst und eindeutig erteilt hat (Nr. 1), die Einwilligung protokolliert wird (Nr. 2), der Inhalt der Einwilligung jederzeit abgerufen werden kann (Nr. 3) und durch den Nutzenden jederzeit mit Wirkung für die Zukunft widerrufen werden kann (Nr. 4).[172] Die Einwilligung des Nutzenden muss spätestens vor der ersten Datenerhebung eingeholt werden, kann aber auch unabhängig von einem konkreten Datenerhebungsvorgang erteilt werden, zum Beispiel bei der ersten Inbetriebnahme des Smart-TV-Geräts.

Die Informationspflicht des Diensteanbieters aus § 13 Abs. 1 TMG[173] besteht unabhängig von dem Erfordernis, eine Einwilligung des Nutzenden einzuholen. Die Informationen des Abs. 1 sind aber mindestens erforderlich für die Erteilung einer wirksamen Einwilligung im Sinne von Abs. 2, andernfalls kann keine informierte Einwilligung vorliegen.[174] Die Vorschrift des § 13 Abs. 2 TMG ist technikneutral formuliert.[175] Wie die Einwilligung im Einzelnen eingeholt wird, wird dem Diensteanbieter als Verpflichtetem überlassen. Üblich sind in diesem Zusammenhang Checkboxen, gleichwohl sind aber auch andere technische Umsetzungen denkbar.

Da Smart-TV-Geräte regelmäßig von mehreren Personen genutzt werden können, muss der Diensteanbieter sicherstellen, dass von jedem Nutzenden gesondert eine wirksame Einwilligung eingeholt wird. In der Folge muss außerdem gewährleistet werden, dass bei Betrieb des Geräts nur Daten derjenigen Nutzenden erhoben werden, die ihre Einwilligung hierzu gegeben haben. Die technische Umsetzung sieht etwa so aus, dass jeder Nutzer einen oder mehrere Accounts hat, über die die Funktionalität der Einwilligung oder ihres Widerrufs realisiert werden.

Besondere Schutzanforderungen gelten, wenn der Nutzende des Smart-TV minderjährig ist. Diese ergeben sich nicht aus dem Datenschutzrecht selbst, da weder im Telemediengesetz noch im Bundesdatenschutzgesetz besondere Altersgrenzen vorgesehen sind. Auch Minderjährige können in einen Eingriff in ihre informationelle Selbstbestimmung zustimmen. Die Altersgrenzen des Bürgerlichen Gesetzbuchs (BGB) für rechtsgeschäftliche Handlungen sind nicht pauschal übertragbar. Vielmehr ist auf die Einsichtsfähigkeit des Minderjährigen abzustellen, das heißt auf die Fähigkeit, den Eingriff in sein Rechtsgut zu überschauen und die Konsequenzen abzuschätzen.[176] Sowohl der Inhalt der Informationspflichten nach § 13 Abs. 1 TMG als auch die Einwilligungserklärung nach Abs. 2 richten sich nach dem Empfängerhorizont, also danach, ob die Informationen und die Formulierungen zielgruppenspezifisch ausgestaltet sind. Sie müssen durch einen durchschnittlichen Minderjährigen aus der Zielgruppe aufgenommen und verstanden werden können. Für den Diensteanbieter ist das mit erheblichen Rechtsunsicherheiten behaftet, da kaum pauschale Vorgehensweisen möglich sind. In jedem Fall muss eine Altersverifikation stattfinden, und die Einwilligungserklärung (wie auch die Informationen nach § 13 Abs. 1 TMG) ist nach Altersgruppen getrennt verständlich und eindeutig zu formulieren sowie übersichtlich zu gestalten.[177]

172 Im einzelnen *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 66 ff.
173 Siehe Kapitel 5.2.2.
174 *Schmitz*, in: Hoeren/Sieber/Holznagel 2014, § 13 TMG, Rn. 176.
175 *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 71.
176 *Jandt/Roßnagel*, MMR 2011, 637 (638); *Micklitz/Schirmbacher*, in: Spindler/Schuster 2015, § 7 UWG, Rn. 108 f.
177 *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 44; *Jandt/Roßnagel*, MMR 2011, 637 (642).

5.2.4 Ausblick: Datenschutz-Grundverordnung

Das Datenschutzrecht in Europa steht derzeit vor großen Veränderungen. Mit der von der Europäischen Kommission vorgeschlagenen und nunmehr zwischen Europäischem Rat, Parlament und Kommission ausgehandelten Datenschutz-Grundverordnung[178] werden datenschutzrechtliche Vorschriften mit dem voraussichtlichen Inkrafttreten der Verordnung ab 2018 europaweit harmonisiert. Die europäischen Datenschutzvorschriften werden anwendbar sein auf alle für die Verarbeitung Verantwortlichen, die personenbezogene Daten im Rahmen der Tätigkeit ihrer Niederlassung verarbeiten sowie auf alle nicht in der Europäischen Union niedergelassenen Verantwortlichen, die personenbezogene Daten von in der Union ansässigen Personen verarbeiten, wenn die Datenverarbeitung dazu dient, diesen betroffenen Personen – auch unentgeltliche – Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten. Die Datenschutzgrundverordnung sieht hierfür zum Beispiel eigene Erlaubnistatbestände für die Verarbeitung personenbezogener Daten, für Betroffenenrechte sowie Vorschriften zu Datensicherheit, Aufsicht und Kontrolle vor. Da der Anwendungsvorrang der Datenschutz-Grundverordnung nur dann gilt, wenn und soweit europarechtliche und mitgliedstaatliche Vorschriften kollidieren, werden einige mitgliedstaatliche Vorschriften auch weiterhin bestehen bleiben. Es ist abzusehen, dass zukünftig eine heterogene, komplexe Rechtslage entsteht; wie sich das auf die beteiligten Akteure auswirkt, bleibt zu untersuchen.

178 Datenschutz-Grundverordnung, Fassung vom 15.12.2015, Trilog-Verhandlung, 2012/0011 (COD).

6
Ausblick und Handlungsmöglichkeiten

Immer mehr Lebensbereiche werden mit dem Internet vernetzt: zu Hause, unterwegs oder im Körper.[179] Dies betrifft auch das Fernsehen mit der Entwicklung von Smart-TV-Systemen, die zusätzlich zum TV-Programm für alle auch individuelle Inhalte, die sich auf die jeweiligen Zuschauer zuschneiden lassen, anbieten. Für den Mehrwert, den Smart-TV-Systemen gegenüber den alten Modellen des herkömmlichen Fernsehens bereitstellen, gehen sie online – ähnlich der Nutzung eines Browsers von einem PC aus. Nur dass die Internet-Surfer am Computer Möglichkeiten haben, Selbstdatenschutztools zum Verhindern oder Eindämmen von Tracking oder Datenabflüssen zu installieren, z.B. als Add-on zum Browser. Über Datenspuren beim Surfen im Netz wird vielfach berichtet, doch dass solche Spuren bei der neuen Art des Fernsehens ebenfalls entstehen, ist bisher nur Experten bekannt. Die aus der Internetkonnektivität erwachsende Datenerhebung „versteckt" sich quasi im Fernseher. Personenbezogene Daten werden oftmals ohne Wissen und ohne Zustimmung der Nutzenden erhoben und verarbeitet. Die Standardkonfiguration schützt die Nutzenden nicht vor einem Tracking. Weitere Smart-TV-Funktionalität wie beispielsweise die Sprachsteuerung kann in die Privatsphäre und in die Datenschutzrechte eingreifen, wenn unkontrolliert per Mikrofon oder über andere Sensoren personenbezogene Daten der Zuschauer im Wohnzimmer übertragen werden.

Auch aus Sicherheitssicht sind Änderungen bei den Smart-TV-Systemen nötig, beispielsweise wenn sicherheitskritische Fehler gefunden wurden und eine Aktualisierung (Update) der Systeme nötig werden. Hierfür ist erforderlich, dass die Aktualisierung der Fernsehgeräte schnell, sicher und ohne schwierige Handhabungen für die Nutzenden durchgeführt werden kann.[180] Heutige Smart-TV-Geräte erfordern teilweise die Aktualisierung per USB-Stick mit vorherigem Herunterladen der Software aus dem Internet. Dies ist in vielen Fällen für den Nutzenden mit einem nicht vertretbaren Aufwand verbunden und stellt eine fragwürdige Verantwortungsverlagerung auf den Betroffenen dar. Auch hier gibt es bereits gute Beispiele, wie veraltete Software in aktuellen Browsern durch Aktualisierungsstrategien vermieden werden kann.[181] In jedem Fall wären aber vor jedem Update die Betroffenen darüber zu informieren. Denn jedes Update bedeutet eine Änderung des bisherigen Systems, die vom Nutzenden normalerweise nicht überblickt werden kann. Dies wiederum bedeutet, dass Updates selbst ein Risiko darstellen können und dass sich über einen Update-Mechanismus möglicherweise auch Schadsoftware verbreiten ließe. Weiterhin dürfen Updates nicht dazu führen, dass getätigte Datenschutzkonfigurationen von Smart-TV-System verschwinden. Gleichzeitig wäre ein Verlagern aller gerätebezogenen Konfigurationen in eine Cloud möglicherweise im Sinne der Verfügbarkeit, aber würde wiederum ein Datenschutzrisiko darstellen, weil diese Datenspeicherung der direkten Kontrolle durch den Nutzenden entzogen ist und außerdem jeder Abruf wieder Datenspuren generiert.

Im Folgenden werden die Anforderungen skizziert, die an die beteiligten Akteure zu stellen sind, um Datenschutz bei Smart-TV-Systemen zum Normalfall werden zu lassen. Neben grundlegender Sicherheitsfunktionalität wie beispielsweise einer standardmäßigen Verschlüsselung sämtlicher Internetkommunikation nach dem Stand der Technik

179 *Karaboga*/Matzner/Morlok/Nebel/Ochs/von Pape/Pittroff/Pörschke/Schütz/Simo (2015).
180 *Ghiglieri* (2014a); *Michéle/Karpow* (2014).
181 *Ragan* (2009).

müssen die Gewährleistungsziele des Datenschutzes, Transparenz und Intervenierbarkeit berücksichtigt werden.[182]

6.1 Nichtverkettbarkeit

Das Datenschutz-Gewährleistungsziel[183] der Nichtverkettbarkeit soll gewährleisten, dass personenbezogene Daten nicht für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. Grundvoraussetzung dafür ist die Datensparsamkeit, d.h. es werden überhaupt nur diejenigen Daten erhoben, die für den Zweck erforderlich sind, und nur so lange aufbewahrt, wie es für den Zweck erforderlich ist.[184] Gemäß dem Ziel der Nichtverkettbarkeit sind Datenbestände und Verarbeitungsprozesse zweckbezogen zu trennen: Dies bedeutet, dass Prozesse auf solch eine Weise auszugestalten sind, dass die im System befindlichen personenbezogenen Daten nicht mit beliebigen anderen personenbezogenen Daten, die sich außerhalb der durch den Zweck definierten Domain befinden, verknüpft werden können.

Ziel einer in diesem Sinne verstandenen Nichtverkettbarkeit ist es, nicht nur anfallende personenbeziehbare Daten im Sinne einer Datensparsamkeit zu minimieren, sondern auch eine über den Zweck der Erhebung hinausgehende, durch die Verknüpfung bedingte weitergehende Aussagekraft der Daten zu vermeiden. Grundlegend wäre die Berücksichtigung der Datensparsamkeit in Protokollspezifikationen oder in verbindlichen technischen Standards.

Die Nichtverkettbarkeitsanforderungen sollten sich in den Standardeinstellungen wiederfinden. Gesetzlich zwar noch nicht verpflichtend, ist „Privacy by Default" schon jetzt aus den Datenschutzgrundsätzen der Datensparsamkeit und Datenerforderlichkeit ableitbar.[185] Bereits die Endgerätehersteller müssen angehalten werden, ihre Produkte und Angebote datenschutzkonform auszugestalten und datenschutzfreundliche Grundeinstellungen zu wählen.[186] Im Falle der Smart-TV-Geräte erfordert das beispielsweise, dass eine Aktivierung und Verbindung mit dem Internet oder der Sensoren erst dann erfolgt, wenn die Nutzenden diese Funktionen gesondert und bewusst aktivieren. Ein einfaches Beispiel besteht darin, dass die Internetverbindung anders als heute bei vielen Smart-TV-Systemen erst dann aufgebaut werden sollte, wenn der „Red Button" vom Nutzenden aktiviert wird. Auch sollten keinesfalls Mikrofone oder Kameras eingeschaltet sein, bevor dies nicht bewusst vom Nutzenden veranlasst wird. Zusätzlich sollten die Nutzenden die Möglichkeit haben, durch mechanische Vorrichtungen (zum Beispiel Schalter oder verschiebbare Klappen) Mikrofone und Kameras in ihrer Funktion zu beschränken, zum Beispiel ganz von der Stromversorgung zu nehmen, damit auch keine Gefahr der unerwünschten Fernsteuerung besteht, oder die Kameralinse mechanisch abzudecken. Auch ein dauerhaftes Abschalten muss möglich sein.

182 Weitere Anforderungen können der Orientierungshilfe Smart-TV entnommen werden: *Düsseldorfer Kreis – Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich*, Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste, V1.0, 2015.

183 Zu den Datenschutz-Gewährleistungszielen zum Beispiel *Rost/Pfitzmann*, Datenschutz-Schutzziele – revisited, DuD 2009, 353-358; *Rost/Bock*, Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen, DuD 2011, 30-35; *Hansen/Jensen/Rost,* Protection Goals for Privacy Engineering, in: Proc. 2015 International Workshop on Privacy Engineering – IWPE'15, 2015.

184 In einigen Veröffentlichungen ist Datensparsamkeit ein eigenes, vorgelagertes Gewährleistungsziel (z.B. *AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Das Standard-Datenschutzmodell, V.0.9, 2015); andere Veröffentlichungen subsumieren Datensparsamkeit als Gestaltungsanforderung unter Nichtverkettbarkeit.

185 Zum Begriff *Kipker*, DuD 2015, 410.

186 So auch die Position des *Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten*, Mai 2014, S. 2, http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/05/Beschluss_Smart_TV.pdf.

Alle Akteure – Gerätehersteller, TV-Sender, Inhaltsanbieter, App-Anbieter und Betreiber von App-Stores – sollten datensparsam agieren und nur die erforderlichen Daten erheben. Hier ist insbesondere zu hinterfragen, wann und inwieweit tatsächlich die Verarbeitung von eindeutigen Identifikatoren wie Geräte-IDs und Verkettungen zu nutzerspezifischen Profilen notwendig sind.

Denkbar ist zudem auch, dass sich die Smart-TV-Hersteller gegenüber den Diensteanbietern im Rahmen von Kooperationsverträgen dazu verpflichten, „Privacy by Design" mit der Standardeinstellung des „Privacy by Default" zu gewährleisten.[187]

6.2 Transparenz

Ziel des Gewährleistungsziels der Transparenz ist, dass die Nutzenden wie auch die anderen Beteiligten Datenerhebung und -verarbeitung ausreichend verstehen und nachvollziehen können. Art, Umfang und Zweck der Erhebung und Verwendung der Daten sowie Informationen zu Betroffenenrechten müssen den Nutzenden in allgemein verständlicher Form erläutert werden. Diese Transparenzpflichten gelten für sämtliche verantwortliche Stellen, unter anderem für die Hersteller der mit smarter Technologie ausgerüsteten Produkte.

Die Sensibilisierung der Nutzenden ist ein wichtiges Instrument, um Transparenz und Vertrauen in neue Techniken zu schaffen.[188] Das erscheint auf den ersten Blick einfach, dennoch ergeben sich einige technische Probleme, die gelöst werden müssen, insbesondere die benutzergerechte Visualisierung und dementsprechende Deutung der Daten. Bei beiden Aspekten ist zu beachten, dass die stetige Ersetzung von alten Fernsehgeräten durch neue Smart-TV-Geräte den Nutzerkreis vergrößert. So werden auch weniger technikaffine Personen die Funktionen eines Smart-TV nutzen, ohne einen versteckten Datentransfer zu erwarten.

Die Visualisierung beginnt bei dem Sichtbarmachen der Datenerhebung, zum Beispiel wenn Mikrofon und Kamera aktiviert sind, von Datenströmen zwischen Geräten und Internet sowie der Kommunikation zwischen den Geräten. Häufig ist eine Information zu Datenübertragungen ohne Kenntnis über den Inhalt und die Bedeutung der Daten schlecht für Nutzende bewertbar. Die reine Kommunikation mit einer Fremdpartei kann zwar schon Indiz für eine unberechtigte Verbindungsaufnahme sein. In vielen Fällen ist es jedoch wünschenswert, den Grund und den Inhalt für eine Kommunikation mit in die Bewertung einfließen zu lassen. Heutzutage sind die benutzergerechte Visualisierung der Datenströme und die damit verbundenen Risiken für die Privatheit im Bereich Smart-TV nicht weit fortgeschritten.

Oftmals wird den rechtlichen Hinweispflichten nur ungenügend Rechnung getragen, sodass Betroffenenrechte gefährdet oder sogar ausgeschlossen sind. So finden sich wichtige Informationen meist lediglich versteckt innerhalb der Nutzungsbedingungen, Allgemeinen Geschäftsbedingungen (AGB) oder Privacy Policies (Datenschutzerklärungen), die den Nutzenden zusammen mit dem Produkt ausgehändigt werden. Innerhalb dieser „Wüste des Kleingedruckten" können die auf den Datenschutz bezogenen Regelungen in einem Großteil der Fälle von den Nutzenden nicht kritisch zur Kenntnis genommen werden.[189]

Umso wichtiger ist es daher, dass entsprechende Hinweise auf die Aufnahmefähigkeit und -bereitschaft des Nutzenden abgestimmt werden. Das kann durch die Hersteller auf unterschiedlichem Wege erfolgen: Bereits beim Verkauf des Produktes muss eine

187 So auch *Ghiglieri/Oswald/Tews* (2013), 11; *Schmidtmann/Schwiering*, ZD 2014, 448 (452); *Weber*, ZUM 2011, 452 (455 f.).
188 *Buchmann* 2013, 74 ff.
189 *Gilbert*, http://www.ibtimes.co.uk/ -1487153.

umfassende, allgemeine Information für den späteren Nutzenden bereitgestellt werden. Im Sinne des Verbraucherschutzes ist hierbei zum Beispiel die Einführung eines entsprechenden Piktogramms oder Icons auf der Verpackung des Produktes denkbar, welches bereits beim Kauf des Produktes optisch auf dessen Internetkonnektivität und möglichst darüber hinaus auf die für Zusatzdienste erforderlichen Datenübermittlungen hinweist. Derartige optische Hinweis- und Logopflichten auf Produkten sind auf EU-Ebene bereits für RFID-Produkte für Hersteller verpflichtend.

Darüber hinausgehend böte es sich an, unter vertraglicher Verpflichtung der Gerätehersteller oder des Einzelhandels Informationen zum Beispiel bezüglich der Rückkanalfähigkeit von HbbTV zur Verfügung zu stellen.[190]

Während des Betriebs des Smart-TV ist es zudem sinnvoll, dem Nutzenden situationsbezogen Informationen per visuellem oder akustischem Signal zukommen zu lassen, also nicht nur vorab, sondern aktuell während des Betriebs, sofern das in dem konkreten Fall erforderlich ist. Die Nutzenden sollen durch auf dem Display erscheinende allgemeine Hinweise befähigt werden, selbst zu entscheiden, ob und vor allem in welcher Detailfülle sie weitergehende Erläuterungen wünschen. Dieses Konzept ist als „Layered Policy Design“ bekannt.

6.3 Intervenierbarkeit

Entsprechend dem Datenschutz-Gewährleistungsziel der Intervenierbarkeit müssen den Betroffenen die ihnen zustehenden Rechte (insbesondere auf Benachrichtigung, Auskunft, Sperrung, Löschung und Widerruf einer zuvor erteilten Einwilligung) jederzeit effektiv ausüben können. Daraus folgt, dass die verantwortliche Stelle Maßnahmen zum Gewährleisten der Betroffenenrechte umsetzen und damit auch Einfluss auf die laufenden und geplanten Datenprozesse nehmen können muss.

Darüber hinaus sollten die Nutzenden im Sinne des Selbstdatenschutzes die Möglichkeit haben, selbst einen unerwünschten Datenstrom nach Deutung der Daten zu unterbinden. Es gibt verschiedene Maßnahmen zur Steuerung: Filterung und Blockierung von Datenverbindungen. Der Großteil der gängigen Filterungs- und Blockierungsmaßnahmen bezieht sich häufig nur auf netzwerktechnisch basierte Filterungen und Blockierungen. Bei zunehmender Funktionalität eines Geräts wird es jedoch vermutlich notwendig sein, feingranularer vorzugehen und eine inhaltsbasierte Filterung anzuwenden. Der einfachste Fall ist die Blockierung von ganzen Geräten, so dass diese beispielsweise keine Verbindung ins Internet aufbauen dürfen. Denkbar ist auch die Blockierung verschiedener Dienste auf dem Fernsehgerät.

Zudem sollten die Nutzenden zumindest so gut, wie dies zurzeit beim Verwenden eines Browsers vom PC aus möglich ist, Cookies löschen oder Anonymisierer hinzuschalten können.

In Zukunft sind standardisierte Systeme notwendig. Sie müssen den Datenstrom überwachen und nach gewissen Regeln ungewollte Verbindungen unterbinden und den Nutzenden dadurch schützen. Handelsübliche Router können nach heutigem Stand für solche Zwecke nicht eingesetzt werden, da die verbaute Hardware im Allgemeinen nicht leistungsfähig genug ist. Die Benutzungsfreundlichkeit wird bei diesen Lösungen eine besondere Rolle spielen.

190 *Schmidtmann/Schwiering*, ZD 2014, 452.

6.4 Das Selbstdatenschutztool „Privacy Protector“

In [191] wird gezeigt, wie eine neue Art der Zuschauermessung datenschutzfreundlich durchgeführt werden kann. Anstatt wie bisher durch eine Telefonleitung eine Verbindung zwischen Erfassungsunternehmen und Haushalt herzustellen, kann nun auch eine Internetverbindung genutzt werden, bei der eine Zwischeninstanz dafür genutzt wird, Daten zu aggregieren. Diese Aggregation dient dazu, dass nur die erforderlichen Daten (in diesem Fall beispielsweise die Anzahl der Zuschauer aller Haushalte) und nicht zusätzliche Daten über einen speziellen Haushalt an das Erfassungsunternehmen weitergegeben werden. Dieses Verfahren hat den Vorteil, dass auch andere Geräte (etwa smarte Stereoanlagen) gemessen werden können. Als zusätzliche Besonderheit erhält der Nutzende die Möglichkeit, die Daten einzusehen und sogar eine Übertragung vollständig abzulehnen.[192]

Die Möglichkeit einer detaillierten Zuschauermessung über HbbTV wurde erstmalig 2013[193] nachgewiesen und durch den **Privacy Protector**[194] prototypisch durch den Nutzenden steuerbar gemacht. Selbst wenn ein Benutzertracking datenschutzrechtskonform gestaltet ist, hat jeder Nutzende ein Recht, diese Messung zu erkennen und auch ausschalten zu können. Die vorgestellte Gegenmaßnahme erlaubt es dem Betroffenen, den jeweiligen Datenstrom zu kontrollieren. Mit dem Privacy Protector wurde eine Konzeptimplementierung für einen kleinen Computer (hier: Raspberry Pi) vorgestellt, die es dem Konsumenten ermöglicht, das Laden von HbbTV-Inhalten ohne seine Zustimmung zu unterbinden. Der Raspberry Pi wird dabei zwischen dem Smart-TV-Gerät und dem herkömmlichen Internet-Router angeschlossen. Die Verbindung zwischen Smart-TV-Gerät und Raspberry Pi ist üblicherweise ein Kabelanschluss, und die Verbindung zum Internet kann ebenfalls per Kabel oder drahtlosem Adapter bewerkstelligt werden. Das Gerät kann hinter ein Smart-TV-Gerät montiert werden und ist damit nicht sichtbar. Nach Inbetriebnahme wird eine HbbTV-Anwendung standardmäßig nicht geladen. Der Nutzende bekommt auf dem Bildschirm mitgeteilt, dass eine Internetaktivität durch HbbTV blockiert wurde, woraufhin der Nutzende diese mit dem Drücken des „Green Button“ zulassen kann. Drückt er auf der Fernbedienung nun die grüne Taste, wird die ursprünglich vom Sender angeforderte Webseite geladen.[195] Eine prototypische Implementierung des Systems kann auf den Seiten der TU Darmstadt[196] heruntergeladen werden. In einer weiteren HbbTV-Analyse wurde nachgewiesen, dass eine Nutzermessung auch auf Radiokanälen, die über Satellit übertragen werden, möglich ist.[197] Um dieses Risiko ebenfalls zu adressieren, wurde das oben genannte System entsprechend erweitert.

191 *Ghiglieri* (2015).
192 Ausführlich zu diesem Verfahren *Ghiglieri* (2015).
193 *Ghiglieri/Oswald/Tews* (2013).
194 *Ghiglieri/Tews* (2014).
195 Für technische Details ausführlich *Ghiglieri/Tews* (2014).
196 http://www.smarthome.sit.tu-darmstadt.de/
197 *Ghiglieri* (2014).

7
Fazit

In diesem Beitrag wurde eine Einführung in die Sicherheits- und Datenschutzproblematik von Smart-TV-Systemen gegeben. Dabei hat sich gezeigt, dass trotz einer starken Zunahme von modernen internetfähigen Fernsehgeräten bislang nur unzureichende Ansätze existieren, um Geräte oder sensible Nutzerdaten zu schützen. Mögliche Gefahren für Nutzende bestehen einerseits durch Angriff auf das Fernsehgerät selbst (zum Beispiel durch Angriffe auf Sensoren wie Kamera und Mikrofon oder durch Kompromittierung der Software), andererseits durch intransparente und unangemessene Zugriffe auf sensible Nutzerdaten mittels Tracking oder durch Abhören der Kommunikationskanäle. Die Art der von Smart-TV-Geräten übertragenen Daten erlauben weitgehende Rückschlüsse auf Nutzerverhalten und spezifische Gewohnheiten. Durch Tracking können ferner gezielt Nutzerprofile erstellt werden, ohne dass dies für die Nutzenden transparent oder zu verhindern ist.

Schutzmöglichkeiten sind derzeit nicht zureichend umgesetzt. Perspektivisch bestehen jedoch unterschiedliche Ansätze, um den Daten- und Privatheit-Schutz in Smart-TV-Systemen zu erhöhen: Eine konsequente Umsetzung des Prinzips der Datensparsamkeit und transparenter Datenübertragung könnte Nutzenden die derzeit nicht gewährleistete Entscheidungsautonomie über die eigenen Daten zurückgeben. Dazu wird es notwendig sein, einen etablierten Datenschutzprozess zu definieren. Ein Schutz der Kommunikationskanäle könnte ferner durch eine systematische Verwendung entsprechender Verschlüsselungstechniken erreicht werden. Ein umfassender Schutz würde jedoch erfordern, dass die Nutzenden die Übertragung ihrer Daten kontrollieren können (beispielsweise unterstützt durch Technik, wie dies beispielsweise das Konzept des so genannten Privacy Protectors vorsieht). Eine Implementierung dieser Schutzmöglichkeiten wurde bereits prototypisch umgesetzt. In Zukunft ist die flächendeckende Verwendung solcher Systeme notwendig, die den Datenstrom überwachen und die Nutzenden vor unerwünschter Datenübertragung schützen. Eine zentrale Rolle wird dabei die Benutzungsfreundlichkeit spielen, die für eine flächendeckende Verwendung entscheidend ist.

Danksagung

Diese Arbeit entstand im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projekts „Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt“ (www.forum-privatheit.de). Einzelne Teile der Arbeit gehen darüber hinaus auf das vom BMBF und dem Land Hessen geförderte „Center for Research in Security and Privacy" kurz CRISP zurück. Wir möchten uns darüber hinaus für die zahlreichen Anmerkungen und Korrekturen unserer Kollegen, allen voran Rasmus Robrahn vom ULD Schleswig-Holstein, bedanken, die wesentlich dazu beigetragen haben, diesen Beitrag zu verbessern.

Literaturverzeichnis

ACLU, Samsung Slammed for "Smart TV" Spying, 2015. http://aclunc-tech.org/primer/case-studies/samsung

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell, V.0.9, 2015, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf.

Albers, M., Informationelle Selbstbestimmung, Baden-Baden 2005.

Alich, S./Nolte, G., Zur datenschutzrechtlichen Verantwortlichkeit (außereuropäischer) Hostprovider für Drittinhalte, in: Computer und Recht (CR) 2011, 741-745.

Angwin, J., Own a Vizio Smart TV? It's Watching You Vizio, one of the most popular brands on the market, is offering advertisers "highly specific viewing behavior data on a massive scale", ProPublica vom 9. November 2015, https://www.propublica.org/article/own-a-vizio-smart-tv-its-watching-you.

Arning, M./Moos, F., Big Data bei verhaltensbezogener Online-Werbung, in: Zeitschrift für Datenschutz (ZD) 2014, 242-248.

Art. 29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, WP 179.

Auriemma, L., http://aluigi.altervista.org/adv/samsux_1-adv.txt, 2012.

Bachy, Y./Basse, F./Nicomette, V./Alata, E./Kaâniche, M./Courrege, J. C./Lukjanenko, P., Smart-TV security analysis: practical experiments, 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2015, pp. 497-504. IEEE.

Bergmann, L./Möhrle, R./Herb, A., Datenschutzrecht, Kommentar, Band 2, 48. Ergänzungslieferung, Stuttgart 2015.

Bitkom e.V., Vor dem Boom - Marktaussichten für Smart Home, Fokusgruppe Connected Home des Nationalen IT-Gipfels, 2014, https://www.bitkom.org/Presse/Anhaenge-an-Pls/2014/Oktober/141023-Marktaussichten-SmartHome.pdf.

BLM – Bayrische Landeszentrale für neue Medien, HbbTV beinhaltet Chancen für Lokalfernsehen – Smart-TV-Anwendungen können Reichweiten und Umsätze lokaler TV-Anbieter erhöhen, 2012, http://www.blm.de/de/infothek/pressemitteilungen/2012.cfm?object_ID=436.

Borgmann, M./Hahn, T./Herfert, M./Kunz, T./Richter, M./Viebeg, U./Vowé, S., On the Security of Cloud Storage Services, in *Technical Report SIT-TR-2012-001*, Darmstadt 2012.

Buchmann, J. (Hrsg.), Internet Privacy: Eine multidisziplinäre Bestandsaufnahme / A multidisciplinary analysis, Springer (acatech Studie), Heidelberg/Berlin 2012.

Buchmann, J. (Hrsg.), Internet Privacy, Options for adequate realisation, Berlin 2013.

Bugiel, S./Nürnberger, S./Pöppelmann, T./Sadeghi, A./Schneider, T., AmazonIA: When Elasticity Snaps Back, in: ACM CCS Proceedings 2011, Chicago, IL, USA, 389-400, http://dl.acm.org/citation.cfm?id=2046753.

CSA – Cloud Security Alliance, The Notorious Nine: Cloud Computing Top Threats in 2013, 2013, https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/.

Dammann, U., Internationaler Datenschutz, in: Recht der Datenverarbeitung (RDV) 2002, 70-77.

Derene, G., Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, consumerreports.org vom 27. Februar 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm.

Deutsche TV Plattform, Marktanalyse Smart-TV, Eine Bestandsaufnahme der Deutschen TV-Plattform, 2014, http://www.tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2014_de.pdf.

DoctorBeet's Blog, LG Smart TVs logging USB filenames and viewing info to LG servers, 2013, http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html.

DoctorBeet's Blog, LG Disables Smart TV features in the EU to force users to accept new oppressive Privacy Policy, 2014, http://doctorbeet.blogspot.de/2014/05/lg-disables-smart-tv-features-in-eu-to.html.

Düsseldorfer Kreis und die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, Gemeinsame Position: Smartes Fernsehen nur mit smartem Datenschutz, 2014, http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/05/Beschluss_Smart_TV.pdf.

Düsseldorfer Kreis – Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste, V1.0, September 2015, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/OH_Smart_TV_v1.0.pdf.

Ehmann, E., Lexikon für das IT-Recht 2014/2015, Heidelberg 2014.

Elhage, N., Virtunoid: A KVM Guest – Host privilege escalation exploit; Black Hat USA, 2011, https://media.blackhat.com/bh-us-11/Elhage/BH_US_11_Elhage_Virtunoid_WP.pdf.

Emarketer, Connected TVs Reach One in Four Homes, 2013, http://www.emarketer.com/Article/Connected-TVs-Reach-One-Four-Homes/1009581.

Epping, V./Hillgruber, C., Beck'scher Online-Kommentar Grundgesetz, Ed. 24, München 2015.

ETSI, ETSI TS 102 796 V1.2.1 (2012-11), 2012, http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf.

Europäisches Parlament, Ausschuss für Kultur und Bildung, Entwurf eines Berichts über Hybridfernsehen („Connected TV"), 2012/2300 (INI), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-504.075%2B01%2BDOC%2BPDF%2BV0%2F%2FDE.

Ghiglieri, M., Incorrect HTTPS Certificate Validation in Samsung Smart TVs, Technische Universität Darmstadt, Darmstadt 2014.

Ghiglieri, M. (2014a), I Know What You Watched Last Sunday - A New Survey Of Privacy In HbbTV, in: Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy, San Jose, CA, USA 2014.

Ghiglieri, M., PriMSED – Privacy-Friendly Measurement of Smart Entertainment Devices, IEEE 12th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2015 im Erscheinen.

Ghiglieri, M./Lange, B./Simo, H./Waidner, M., Security und Privacy bei SmartTV: Bedrohungspotential und technische Lösungsansätze, in: Weiterdenken, Heinrich-Böll-Stiftung Sachsen, Lichdi, J. (Hrsg.), Digitale Schwellen, Privatheit und Freiheit in der digitalen Welt, Dresden 2015.

Ghiglieri, M./Oswald, F./Tews, E., HbbTV – I Know What You Are Watching, 13. Deutschen IT-Sicherheitskongress, Bonn 2013.

Ghiglieri, M./Oswald, F./Tews, E., HbbTV: Neue Funktionen mit möglichen Nebenwirkungen, in: Die Fachzeitschrift für Fernsehen, Film und elektronische Medien (FKT) 2013, 563-566.

Ghiglieri, M./Tews E., A Privacy Protection System for HbbTV in Smart TVs, in: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2014.

Gilbert, D., Samsung smart TVs listen to your private conversations and share details with advertisers, International Business Times vom 9.2.2015, http://www.ibtimes.co.uk/ -1487153.

Gola, P./Schomerus, R., Bundesdatenschutzgesetz, Kommentar, 12. Aufl., München 2015.

Goodin, D., Beware of ads that use inaudible sound to link your phone, TV, tablet, and PC. Privacy advocates warn feds about surreptitious cross-device tracking. Arstechnica, Nov 13, 2015.

Grabitz, E./Hilf, M./Nettesheim, M., Das Recht der Europäischen Union, 40. EL, München 2009.

Grattafiori, A./Yavor, J., The Outer Limits: Hacking the Samsung Smart TV, in: Black Hat US, Las Vegas, NV, USA 2013.

Hansen, M./Jensen, M./Rost, M., Protection Goals for Privacy Engineering, in: Proc. 2015 International Workshop on Privacy Engineering – IWPE'15, 2015.

Harris, S., Your Samsung SmartTV Is Spying on You, Basically, The Daily Beast vom 5.2.2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.

hbbtv-infos.de, HbbTV® Infoportal, 2014, http://www.hbbtv-infos.de/.

Heckmann, D. (Hrsg.), juris Praxiskommentar Internetrecht, 4. Auflage, Saarbrücken 2014.

Hoeren, T./Sieber, U./Holznagel, B. (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 40. Ergänzungslieferung, München 2014.

Hoffmann-Riem, W., Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzer informationstechnischer Systeme, in: JuristenZeitung (JZ) 2008, 1009-1022.

Holznagel, B., Internetdienstefreiheit und Netzneutralität, in: Zeitschrift für Medien und Kommunikationsrecht (AfP) 2011, 532-539.

Hornung, G., Ein neues Grundrecht, Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme", in: Computer und Recht (CR) 2008, 299-306.

IRT GmbH, HbbTV mit Second-Screen-Funktion, 2014, http://www.irt.de/no_cache/de/aktuell/news/view/article/hbbtv-with-second-screen-function.html.

Jandt, S., Grenzenloser Mobile Commerce, Schutzwirkung und Durchsetzbarkeit datenschutzrechtlicher Ansprüche gegenüber ausländischen Diensteanbietern, in: Datenschutz und Datensicherheit (DuD) 2008, 664-669.

Jandt, S./Roßnagel, A., Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, in: Multimedia und Recht (MMR) 2011, 637-642.

Jarass, H. D./Pieroth, B., Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 12. Aufl., München 2012.

Kandias, M./Virvilis, N./Gritzalis, D., The insider threat in Cloud computing, in: Critical Information Infrastructure Security, Springer Berlin Heidelberg 2013, pp. 93-103.

Karaboga, M./Matzner, T./Morlok, T./Nebel, M./Ochs, C./von Pape, T./Pittroff, F./Pörschke, J. V./Schütz, P./Simo, H., White Paper Das versteckte Internet: Zu Hause – Im Auto – Am Körper, in: Peter Zoche et al. (Hrsg.), Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe 2015.

Keber, T., Big Data im Hybrid-TV – Mit dem Zweiten sieht das Erste besser, in: Recht der Datenverarbeitung (RDV) 2013, 236-243.

Kipker, D.-K., Privacy by Default und Privacy by Design, in: Datenschutz und Datensicherheit (DuD) 2015, 410.

Kortchinsky, K., CLOUDBURST – A VMware Guest to Host Escape Story; BlackHat USA 2009.

Krüger, S./Maucher, S.-A., Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, in: Multimedia und Recht (MMR) 2011, 433-439.

Kutscha, M., Das „Computer-Grundrecht" – eine Erfolgsgeschichte?, in: Datenschutz und Datensicherheit (DuD) 2012, 391-394.

KVJS-Fachtagung, My Smart Home is my Castle – Wohnqualität durch benutzerfreundliche Technik, 2012, http://www.bundesanzeiger-verlag.de/betreuung/aktuelles/aktuelle-meldungen/newsdetails/artikel/my-smart-home-is-my-castle-wohnqualitaet-durch-benutzerfreundliche-technik-6789.html.

Lee, W.-P./Kaoli, C./Huang, J.-Y., A smart TV system with body-gesture control, tag-based rating and context-aware recommendation, Knowledge-Based Systems 56/2014, 167-178.

Lendino, J., Panasonic Unveils Voice-Activated TVs With Facial Recognition, 2014, http://www.pcmag.com/article2/0,2817,2429165,00.asp.

Lerch, H./Krause, B./Hotho, A./Roßnagel, A./Stumme, G., Social Bookmarking-Systeme – die unerkannten Datensammler, Ungewollte personenbezogene Datenverarbeitung?, in: Multimedia und Recht (MMR) 2010, 454-458.

Maunz, T./Dürig, G., Grundgesetz, Kommentar, 73. Aufl., München 2014.

McSorley, A., The Anatomy of an IoT Hack - Avast researchers hacked a Vizio Smart TV to gain access to a home network, AVAST Blog, 9. November 2015, https://blog.avast.com/2015/11/11/the-anatomy-of-an-iot-hack/

Michéle, B., Broadcast, in Smart TV Security, Springer International Publishing 2015, (pp. 35-80).

Michéle, B./Karpow, A., Watch and be Watched: Compromising All Smart TV Generations, in: 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA 2014.

Müller-Broich, J., Telemediengesetz, Kommentar, Baden-Baden 2012.

Mulliner, C./Michéle, B., Read It Twice! A Mass-Storage-Based TOCTTOU Attack, in: WOOT 2012, August, pp. 105-112.

Niemietz, M./Somorovsky, J./Mainka, C./Schwenk, J., Not so Smart: On Smart TV Apps, International Workshop on Secure Internet of Things (SIoT 2015, Vienna, Austria).

Nolte, N., Zum Recht auf Vergessen im Internet, Von digitalen Radiergummis und anderen Instrumenten, in: Zeitschrift für Rechtspolitik (ZRP) 2011, 236-240.

Oren,Y./Keromytis, A. D., From the Aether to the Ethernet – Attacking the Internet using Broadcast Digital Television, in: USENIX Security 14, San Diego, CA, USA 2014.

Piltz, C., Der räumliche Anwendungsbereich europäischen Datenschutzrechts, in: Kommunikation und Recht (K&R) 2013, 292-297.

Piltz, C., Nach dem Google-Urteil des EuGH: Analyse und Folgen für das Datenschutzrecht, in: Kommunikation und Recht (K&R) 2014, 566-570.

PricewaterhouseCoopers, Media Trend Outlook. Smart-TV: Mehrwert für den Konsumenten, mehr Umsatz für die Medienbranche, 2013, www.pwc.de/de/technologie-medien-und-telekommunikation/assets/whitepaper-smart-tv.pdf.

Ragan, S., Report: Using silent updates boosts browser security, 2009, http://www.thetechherald.com/articles/Report-Using-silent-updates-boosts-browser-security/5714/.

Rengeling, H.-W./Middeke, A./Gellermann, M., Handbuch des Rechtsschutzes in der EU, 3. Aufl., München 2014.

Richter, P. (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, Baden-Baden 2015.

Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Roßnagel, A., Das Telemediengesetz, Neuordnung für Informations- und Kommunikationsdienste, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2007, 743-748.

Roßnagel, A. (Hrsg.), Recht der Telemediendienste, Kommentar, München 2013.

Roßnagel, A., Big Data – Small Privacy?, Zeitschrift für Datenschutz (ZD) 2013, 562-567.

Roßnagel, A./Schnabel, C., Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, in: Neue Juristische Wochenschrift (NJW) 2008, 3534-3538.

Rost, M./Bock, K., Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen, in: Datenschutz und Datensicherheit (DuD) 2011, 30-35.

Rost, M./Pfitzmann, A., Datenschutz-Schutzziele – revisited, in: Datenschutz und Datensicherheit (DuD) 2009, 353-358.

Sachs, M., Grundgesetz, Kommentar, 6. Aufl., München 2011.

Sattler, C., Smart TV: Wer erringt die Portalhoheit auf dem Fernseher, Goldmedia Innovation GmbH, Düsseldorf 2011.

Schaar, P., Das Ende der Privatsphäre – Der Weg in die Überwachungsgesellschaft, 2. Aufl., München 2007.

Schmidtmann, K./Schwiering, S., Datenschutzrechtliche Rahmenbedingungen bei Smart-TV, Zulässigkeit von HbbTV-Applikationen, ZD 2014, 448-453.

Schwartmann, R. (Hrsg.), Praxishandbuch Medien-, IT- und Urheberrecht, 3. Aufl., Heidelberg 2014.

Seidel, M., Die Direkt- oder Drittwirkung von Richtlinien des Gemeinschaftsrechts, in: Neue Juristische Wochenschrift (NJW) 1985, 517-522.

SeungJin, L./Seungjoo, K., Smart TV security, #1984 in 21st century, in: CanSecWest 2013, http://cansecwest.com/slides/2013/SmartTV Security.pdf.

Simitis, S. (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 8. Aufl., Baden-Baden 2014.

Skistims, H., Smart Home, Dissertation Universität Kassel, im Erscheinen 2015.

Spehr, M./Tunze, W., Horchposten im Wohnzimmer, Frankfurter Allgemeine Sonntagszeitung vom 15.2.2015, V9.

Spindler, G./Schuster, F. (Hrsg.), Recht der elektronischen Medien, Kommentar, 3. Aufl., München 2015.

Statista, Wie wird sich der Markt für Smart Home bis 2020 entwickeln?, 2010, http://de.statista.com/statistik/daten/studie/183271/umfrage/prognose-zur-entwicklung-von-smart-home-aus-sicht-der-hersteller/.

Statista (2011a), Anzahl der Smart TV-Haushalte in Deutschland im Jahr 2010 und Prognose bis 2016 (in Millionen), 2011, http://de.statista.com/statistik/daten/studie/208236/umfrage/prognose-zur-entwicklung-der-smart-tv-haushalte-in-deutschland/.

Statista (2011b), Prognose zur Anzahl der Haushalte mit mind. einem an das Internet angeschlossenen HbbTV-Gerät von 2011 bis 2016 (in Millionen), 2011, http://de.statista.com/statistik/daten/studie/271953/umfrage/prognose-zur-entwicklung-der-hbbtv-haushalte-in-deutschland/.

StrategyAnalytics, 2013 Smart TV Shipments Grew 55 Percent, 2014, https://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5472.

Sutherland, I./Huw, R./Konstantinos, X., Forensic analysis of smart TV: A current issue and call to arms, Digital Investigation 11.3 (2014), 175-178.

Taeger, J./Gabel, D. (Hrsg.), Kommentar zum BDSG, 2. Aufl., Frankfurt a. M. 2013.

Viefhues, W., Art.-29-Datenschutzgruppe: Hilfestellung zum Cookie-Gebrauch, ZD-Aktuell 2012, 02996.

v. Mangoldt, H./Klein, F./Starck, C., Kommentar zum Grundgesetz, Band 1, 6. Aufl., München 2010.

Wagner, S., Das Websurfen und der Datenschutz, Ein Rechtsvergleich unter besonderer Berücksichtigung der Zulässigkeit sogenannter Cookies und Web Bugs am Beispiel des deutschen und U.S.-amerikanischen Rechts, Frankfurt am Main 2006.

Weber, P., Hybridfernsehen aus der Sicht des öffentlich-rechtlichen Rundfunks, in: Zeitschrift für Urheber- und Medienrecht (ZUM) 2011, 452-457.

Weichert, T., Internet-TV und Datenschutz – ein Annäherungsversuch, https://www.datenschutzzentrum.de/vortraege/20140516-weichert-internet-tv.html.

Weichert, T., Internet-TV und Datenschutz, in: Datenschutz und Datensicherheit (DuD) 2014, 528-535.

Wojtczuk, R./Beulich, J., Advanced Exploitation of Xen Hypervisor Sysret VM Escape Vulnerability, 2012, http://www.vupen.com/blog/20120904.Advanced_Exploitation_of_Xen_Sysret_VM_Escape_CVE-2012-0217.php.

Yeong Gon, K./Kwang Yong, S./Whon Oh, L./Kang Ryoung, P./Eui Chul, L./CheonIn, O./HanKyu, L., Multimodal Biometric Systems and Its Application in Smart TV, in: Computer Applications for Database, Education, and Ubiquitous Computing, Proceedings of the International Conferences, EL, DTA and UNESST 2012, Held as Part of the Future Generation Information Technology Conference, FGIT 2012, Gangneug, Korea, December 16-19, 2012, Springer Berlin/Heidelberg, 219-226.

IMPRESSUM

Kontakt:
Peter Zoche
Koordinator Sicherheitsforschung und Technikfolgenabschätzung

Telefon +49 721 6809-152
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

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

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

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

1. Auflage: 50 Stück
Februar 2016

Druck
Stober GmbH Druck und Verlag, Eggenstein

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein