Internet der Dinge: Die Produkte gehören gar nicht uns

Eine perfide Steigerung im Überwachungskapitalismus

[3]

Landen bei Ihnen „smarte“ Weihnachtsgeschenke unter dem Tannenbaum? Unsere Gastautorin zeigt auf, warum wir misstrauisch werden sollten, wenn Technik mit zusätzlichem Abo-Modell daherkommt. Am Ende könnten wir gleich doppelt im Dunkeln sitzen.

Barbara Wimmer ist langjährige und preisgekrönte netzpolitische Journalistin aus Österreich. Seit 2010 schreibt sie bei der Futurezone [4]. Dieser Beitrag ist ein Auszug aus ihrem neuen Buch „Hilfe, ich habe meine Privatsphäre aufgegeben!“.

von Mag. Barbara Wimmer, Wien

► Ohne Cloud-Verbindung kein Licht

Unsere digitale Unmündigkeit geht noch weiter, als sich viele von Ihnen vorstellen können. Viele der Produkte, die wir erwerben, gehören uns gar nicht mehr selbst und wir haben daher auch keine Kontrolle über sie. Wir können nicht frei über sie verfügen, das letzte Wort hat immer der Hersteller. Wir bezahlen also für Produkte, die wir am Ende wegschmeißen können, wenn der Hersteller pleitegeht. Oder wenn wir das Abo-Modell kündigen. Ich will Ihnen das anhand von Beispielen veranschaulichen.

Im Jahr 2014 sammelte das Start-up Emberlight [5] auf der Crowdfunding-Plattform Kickstarter 300.000 Dollar ein, um eine smarte Lampenfassung auf den Markt zu bringen, die mit herkömmlichen Glühlampen funktioniert. Damit sollen sich Lampen auch ohne Lichtschalter steuern lassen. Doch dieselbe Geschäftsidee hatten auch andere Unternehmen. Diese brachten ähnliche Produkte für die Hälfte des Geldes und auch noch schneller auf den Markt und zwangen Emberlight damit dazu, ihr Produkt aufzugeben, weil es sich finanziell nicht mehr rechnete. Für die Kunden und Investoren des Start-ups bedeutete dies in der Folge: Licht aus.

Denn die vernetzte Lampenfassung kommunizierte im Hintergrund permanent mit den Cloud-Servern von Emberlight. Als das Start-up in Konkurs ging, wurden auch diese Server abgedreht – und damit auch die Cloud. Die Lampen, die in den smarten Sockeln steckten, konnten nicht mehr ein- und ausgeschaltet werden. Die Betroffenen mussten die Sockel, die sie ausgewechselt hatten, schon nach wenigen Monaten mühsam wieder abmontieren und zurücktauschen, um nicht im Dunklen zu sitzen. Das Produkt konnten sie nur noch in die Mülltonne werfen. Um es plakativer auszudrücken: Sie haben für einen smarten Lampensockel Geld ausgegeben, der ausschließlich mit der Cloud-Verbindung eines bestimmten Unternehmens funktioniert hat. Ergo: Das Produkt hat ihnen gar nicht wirklich vollständig gehört.

Gut, sagen Sie jetzt: Bei Crowdfunding muss man vorsichtig sein. Das weiß doch jeder. Da haben Sie recht, dass man da generell vorsichtig sein muss, weil man praktisch Experimente finanziert. Falls Sie das noch nicht gewusst haben, haben Sie es hiermit gelernt. Bei Crowdfunding-Produkten, die das Internet der Dinge betreffen, sollten Sie aber besonders vorsichtig sein und sich Produkte ganz genau ansehen, bevor Sie diese finanziell unterstützen und erwerben.

► Von der smarten Überwachungskamera geschröpft

Doch dass Ihnen das vernetzte Produkt, das Sie erworben haben, nicht wirklich gehört, kann Ihnen auch bei bekannten und völlig seriösen Herstellern passieren. So stellt die Firma Nest Labs [6] etwa beliebte Überwachungskameras her. Nest Labs ist ein Vernetzungs- und Automatisierungsunternehmen mit Sitz in Palo Alto (USA), das im Februar 2018 Teil der Hardware-Abteilung von Google wurde.

Nest bietet verschiedene vernetzte Produkte an, unter anderem Überwachungskameras, um Einbrüche aufzuzeichnen oder Einbrecher mit den Kameras präventiv abzuschrecken.

Die Kameras funktionieren allerdings wie die Glühbirne, die [Michael] Steigerwald [auf dem 35. Chaos Communication Congress [7]] untersucht hatte, ausschließlich mit einer aktiven Internetverbindung. Ohne Internet keine Überwachung und kein Schutz vor Einbrechern.

Das ist schon einmal der erste Knackpunkt. Ein smarter Einbrecher, der etwa das Nest-Logo auf der Haustür sieht, das Zeichen dafür, dass ein Heim mit Nest-Kameras überwacht wird, wird als Erstes das Internet abdrehen, bevor er in das Haus eindringt. Dann zeichnet die Überwachungskamera nämlich nichts auf. Gar nichts.

Sollte der Einbrecher allerdings nicht so schlau sein und einfach das tun, was er normalerweise tut, heißt das noch nicht, dass SIE ihn am Ende auch tatsächlich auf einer Video-Aufzeichnung zu Gesicht bekommen. Denn das Bildmaterial, das die Kamera mitschneidet, wird zwar auf die Google-Server übertragen, Sie bekommen allerdings nur dann umfangreichen Zugriff darauf, wenn Sie ein Abo-Modell abschließen.

Ohne Nest-Aware-Abo können Sie lediglich auf die Aufnahmen der letzten drei Stunden zugreifen – und auch nur auf Screenshots. Wer versucht, den Screenshot des Einbrechers auf seiner lokalen Festplatte oder in seiner eigenen Cloud-Lösung zu speichern, wird daran ebenfalls scheitern – und das, obwohl Sie die Überwachungskamera vorher für teures Geld erworben haben. Die 'Nest Cam Indoor' kostete 2019 etwa 199 Euro, die 'Nest Cam Outdoor' wurde für 229 Euro verkauft.

Etwas mehr Zugriff gibt es für Kunden, die ein Abo abschließen. Wer auf Videoaufnahmen zehn Tage lang zugreifen möchte, wurde von Nest im Jahr 2019 mit 100 Euro im Jahr oder zehn Euro pro Monat geschröpft. Für den 30-Tage-Verlauf waren 300 Euro im Jahr oder 30 Euro pro Monat fällig.

Wer also im Sommer 14 Tage in Urlaub fährt, muss entweder darauf hoffen, dass der Einbruch ins Eigenheim nicht in den ersten vier Tagen seiner Abwesenheit stattfindet, um eine Videoaufnahme davon zu Gesicht zu bekommen, oder 300 Euro pro Jahr extra zu den Produktkosten berappen.

Wer mehr als eine Kamera installiert hat, weil er etwa ein großes Haus hat, das von mehreren Seiten zugänglich ist – beispielsweise über einen Keller, die Haustür und die Terrassentür, muss entsprechend mehr zahlen. Pro Kamera fallen 50 Euro pro Jahr zusätzlich an oder fünf Euro pro Monat.

Das ist doch absurd, oder? Es ist auf jeden Fall eine Steigerung imÜberwachungskapitalismus [8]: Man gibt nicht nur seine privaten Daten an Google her, weil die Geräte ständig per Internet mit dem Hersteller verbunden sind, sondern zahlt auch noch dafür, sie selbst abrufen zu dürfen.

► Wirklich grausam: Roboter-Hunde mit Abo-Modell

Ein Experte, der diese Problematik bereits ausführlich analysiert hat, istJoshua A. T. Fairfield [9], Jura-Professor an der 'Washington and Lee University' in den USA und Autor von »Owned. Property, Privacy and the New Digital Serfdom«. Er beschäftigt sich mit dem Besitz von digitalen Gütern und vernetzten Geräten und gilt als Rechtskoryphäe im Technologie-Bereich.

Seine These ist, dass uns das Internet der Dinge wieder ins Mittelalter zurückschickt. Damals besaß der König alles und was die anderen Menschen besaßen, hing von ihren Beziehungen zum König ab. Die Arbeiter besaßen nicht einmal die Werkzeuge, die sie für ihre Arbeit benötigten. In der jetzigen Zeit gäbe es “Digital-Barone“, die derartige Besitzverhältnisse wieder aufleben lassen. “Ein Grund, warum wir keine Kontrolle über unsere Geräte haben, ist, dass die Unternehmen, die sie herstellen, anscheinend glauben – und definitiv so handeln, nachdem wir sie gekauft haben – als würden sie diese noch besitzen“, sagt der Rechtsexperte.

Das bedeutet: Auch wenn Sie ein Hardware-Produkt kaufen, verwalten die Hersteller die dazugehörige Software – und ohne diese funktioniert das Produkt nun einmal nicht. Das ist etwa auch bei der Nest-Überwachungskamera der Fall. Das Kameragehäuse alleine bringt Ihnen nichts. Sie brauchen die Software, die die Einbrecher aufzeichnet, um Aufnahmen sehen zu können. Das gilt aber auch für viele Smartphones. Die laufen ohne Betriebssystem ebenfalls nicht.

Für Joshua A. T. Fairfield ist das in etwa so, als würde man von einem Händler ein Auto kaufen, dieser behält aber den Motor in seinem Besitz. “Es ist wichtig, dass wir das erkennen und ablehnen, was diese Unternehmen machen. Wir müssen unsere Rechte, etwas im digitalen Zeitalter zu verwenden, zu reparieren und zu modifizieren, stärken“, fordert der Rechts-Professor. Das bedeutet:

Wir müssen uns gegen derartige Praktiken wehren – und die Herstellernicht dabei unterstützen.

Auch beim Roboterhund Aibo von Sony, der in seiner Neuauflage mit seinen Besitzern interagieren und eine digitale Persönlichkeit entwickeln kann, setzt man auf ein Abo-Modell. Der Konzern zwingt Menschen, die sich Aibo kaufen, dazu, dafür zu bezahlen, dass Aibo die von ihnen beigebrachten Kunststücke und Gewohnheiten beibehält – und von seinen Besitzern lernt. Wer immer zur selben Zeit mit seinem Roboterhund Gassi gehen mag, muss rund 650 Euro zahlen, um das drei Jahre lang tun zu dürfen. Ansonsten “vergisst“ Aibo alles, was er gelernt hat.

Das ist wirklich grausam, anders kann man es nicht ausdrücken. Jemand, der sich Aibo anschafft, hat vielleicht nicht ausreichend Zeit, sich um ein echtes Tier zu kümmern, will aber trotzdem nicht alleine sein. Dass es sich dabei um eine Maschine handelt, die lediglich ein Tier imitiert, ist egal. Bei den Besitzern sind hier, anders als bei einer Überwachungskamera, auf jeden Fall auch Gefühle im Spiel.

Als Sony die Produktion des ersten Aibo-Modells eingestellt und es auch keine Ersatzteile mehr gegeben hatte, gab es in Japan Hunderte buddhistische Begräbnisse für die Roboterhunde. Menschen haben zu ihren Roboterhunden eine Bindung aufgebaut, sie wie Tiere behandelt und gepflegt. Daher ist "Bindung mit Drei-Jahres-Abo" wirklich nicht hübsch. Dennoch wurden in Japan nach der Wiedereinführung bis August 2018 rund 20.000 Stück des lernfähigen Aibos mit digitaler Persönlichkeit verkauft. In Japan kostet Aibo rund 1.500 Euro.

► Unmündig im Internet der Dinge

Leider versuchen, wie diese Beispiele zeigen, immer mehr Hersteller, Profit zu machen, indem sie unsere vernetzten Produkte softwareseitig vollständig kontrollieren und uns für die Daten, die durch unsere Nutzung generiert werden, extra bezahlen zu lassen. Jura-Professor Fairfield fordert daher zu Recht, dass dieser Praxis ein Ende gesetzt wird, bevor sie sich so richtig durchsetzt.

In erster Linie ist es daher wichtig, dass Sie diese Produkte nicht kaufen, wenn Sie etwas von »zusätzlichem Abo-Modell« lesen. Sehen Sie sich weiter um, welche ähnlichen Produkte es noch gibt, die darauf verzichten. Derzeit gibt es noch Alternativen. Langfristig betrachtet braucht es aber eine Regulierung dieser Geschäftspraxis und die Daten gehören in die Hände der Kunden, die schließlich bereits dafür gezahlt haben. Was bringt es uns etwa, wenn Nest weiß, wer in unsere Wohnung eingebrochen hat, aber wir nicht – oder nur gegen Extra-Cash?

Privatpersonen sollten außerdem selbst darüber entscheiden können, wem sie ihre Daten überhaupt anvertrauen. Solange wir diese Entscheidungsmacht nicht zurückerobert haben, sind wir in eine digitale Unmündigkeit gedrängt. Und das Internet der Dinge trägt – leider – dazu bei, diese digitale Unmündigkeit weiter auszubauen, statt sie zu überwinden.

Mag. Barbara Wimmer, **Wien**.

_____

Barbara Wimmer ist eine preisgekrönte Journalistin, Autorin und Speakerin. Seit November 2010 bei der Kurier-Futurezone. Schreibt und spricht über Netzpolitik, Datenschutz, Algorithmen, Künstliche Intelligenz, Social Media, Digitales und alles, was (vermeintlich) smart ist.

Kontakt: shroombab(at)gmx(dot)at // shroombab(at)gmail(dot)com

Ihre Webseite: **https://shroombab.at/** [10] .

_____

»**Hilfe, ich habe meine Privatsphäre aufgegeben! Wie uns Spielzeug, Apps, Sprachassistenten und Smart Homes überwachen und unsere Sicherheit gefährdet**«. von Barbara Wimmer, mitp Verlags GmbH & Co. KG, Frechen >> https://www.mitp.de/ . 1. Auflage, ersch. 10. Dez. 2020, ISBN 978-3-7475-0164-1, **Buch** 16,99 € [D], **E-Book** (PDF & EPUB) 14,99 € [D]. **Buch + E-Book** 19,99€ [D]. alle 272 Seiten.

• Wieso wir auf eine Totalüberwachung zusteuern: die Macht von Sprachassistenten, Connected Cars, Smart Homes, Smart Citys, Fitness-Apps und mehr

• Was Sie im Umgang mit vernetzten Geräten beachten sollten und wie Sie Ihre Privatsphäre schützen

• Aktuelle Entwicklungen und Fallbeispiele aus Deutschland und Österreich

Neue Technologien sollen unser Leben komfortabler machen. Doch der Preis, den wir dafür zahlen, ist hoch. Die zunehmende Vernetzung durch Geräte, die permanent mit dem Internet verbunden sind, bringt eine Überwachung von ungeahntem Ausmaß mit sich. Das Absurde dabei ist, dass wir unsere Privatsphäre freiwillig aufgeben – und das, ohne uns der Auswirkungen in vollem Umfang bewusst zu sein.

Im Kinderzimmer ermöglichen App-gesteuerte Spielzeug-Einhörner böswilligen Hackern, dem Nachwuchs Sprachnachrichten zu senden. Im Wohnzimmer lauschen mit der digitalen Sprachassistentin Alexa und ihren Pendants US-Konzerne mit und ein chinesischer Hersteller smarter Lampen speichert den Standort unseres Heims auf unsicheren Servern. Nebenbei teilen Zyklus- und Dating-Apps alle Daten, die wir ihnen anvertrauen, mit Facebook & Co.

In diesem Buch zeigt Ihnen Barbara Wimmer, was Apps und vernetzte Geräte alles über Sie wissen, was mit Ihren Daten geschieht und wie Sie sich und Ihre Privatsphäre im Alltag schützen können.

Wie die zunehmende Vernetzung Ihre Privatsphäre und Sicherheit gefährdet:

• Smart Home: Überwachung und Sicherheitslücken

• Spielzeug mit Online-Funktionen und die Gefahren für Kind und Heim

• Sicherheitslücken und Unfallrisiken bei Connected Cars

• Lauschangriff der digitalen Sprachassistenten

• Datenmissbrauch zu Werbezwecken durch Apps auf dem Smartphone

• Contact Tracing mit Corona-Apps

• Gesichtserkennung und Überwachung in Smart Citys

• Perspektiven: Datenschutz und digitale Selbstbestimmung

Inhaltsverzeichnis:

Vorwort 7

Kapitel 1: Was ist das Internet der Dinge? 13

Kapitel 2: Digitale Unmündigkeit durch Vernetzung 27

Kapitel 3: Warum wir auf eine Totalüberwachung zusteuern 51

Kapitel 4: Hey, Einhorn: Wie uns Spielzeug ausspioniert 69

Kapitel 5: Warum das Internet der Dinge so unsicher ist 93

Kapitel 6: Hey Auto: Wir sind die Testpiloten 111

Kapitel 7: Hey Alexa: Digitale Assistenzwanzen 129

Kapitel 8: Privatsphäre bei Siri & Co? Fehlanzeige! 149

Kapitel 9: Hey App: Was weißt du alles über mich? 169

Kapitel 10: Corona: Apps zur Rückverfolgung von Infektionsketten 191

Kapitel 11: Hey, Smart City: Machst du wirklich alles besser? 211

Kapitel 12: Technologie gestalten und regulieren 229

Kapitel 13: Zusammenfassung und wie Sie sich wehren können 247

Stichwortverzeichnis 263

Ein paar Sätze aus dem Vorwort: (Seite 10+11)

»Durch die zunehmende Vernetzung werden wir als Gesellschaft immer abhängiger vom »Always On«. Und manchmal trifft uns das viel härter als eine Spam-Mail, die automatisiert von einem Kühlschrank verschickt wurde. Experten warnen seit Jahren davor, dass wir auf die Folgen, die die zunehmende Vernetzung haben könnte, nicht ausreichend vorbereitet sind. Dem stimme ich zu. Ihnen, liebe Leserinnen und Leser, möchte ich mit dem Buch einen Überblick über die wichtigsten Entwicklungen in diesem Bereich geben – und über die lauernden Gefahren.

Eine dieser Gefahren ist, dass wir als Gesellschaft auf eine Totalüberwachung zusteuern – denn unsere Daten werden nicht nur von kommerziellen Firmen gesammelt, auch Cyber- kriminelle und der Staat wollen gleichermaßen darauf zugreifen können.

Cyberangriffe sind nicht nur für große, kritische Anlagen ein Problem, sondern auch, wenn sie in unseren Wohn- und Kinderzimmern stattfinden, etwa wenn unbekannte Angreifer eine Baby-Cam übernehmen und die Mutter beim Stillen beobachten oder wenn sie über vernetztes Spielzeug direkt mit dem Kind in Kontakt treten und ihm den Befehl erteilen, die Haustür zu öffnen. Auch Connected Cars sind nicht sicher und auf den »Autopiloten« sollten Sie sich besser nicht allzu sehr verlassen.

Neben den Gefahren, die im Bereich der IT-Sicherheit lauern, machen sich große Konzerne wie Amazon oder Google mit digitalen Assistenzwanzen in unseren Wohnzimmern breit – und nutzen die Datensammlung auch noch dazu, ihre Produkte zu verbessern. Auch App-Hersteller sind nicht viel besser, wenn es um das Sammeln und Speichern unserer Daten geht. Von diesen Herstellern werden unsere intimsten Details oftmals an Werbetreibende weiterverkauft und landen damit auch bei Firmen, mit denen wir niemals persönlich in Kontakt waren. Immer mehr Daten werden gesammelt, auch in vernetzten Städten.

Ich möchte Ihnen aber nicht nur die Gefahren aufzeigen, sondern auch, was Sie tun können, um dieser Entwicklung nicht hilflos ausgeliefert zu sein. Wir befinden uns mitten drin in einer Entwicklung, die Teil eines »immer schneller, höher, weiter!« ist, ohne an die Konsequenzen zu denken. Das müssen wir wieder ändern. Gemeinsam.«

Mag. Barbara Wimmer, Wien. (Kurzer Auszug aus dem Vorwort des Buches **„Hilfe, ich habe meine Privatsphäre aufgegeben!**“).

netzpolitik.org ist eine Plattform für digitale Freiheitsrechte. Die Betreiber und deren Autoren thematisieren die wichtigen Fragestellungen rund um Internet, Gesellschaft und Politik und zeigen Wege auf, wie man sich auch selbst mithilfe des Netzes für digitale Freiheiten und Offenheit engagieren kann. Mit netzpolitik.org beschreiben sie, wie die Politik das Internet durch Regulation verändert. Und wie das Netz Politik, Öffentlichkeiten und alles andere verändert. Sie verstehen sich als journalistisches Angebot, sind jedoch nicht neutral. Ihr Haltung ist: Engagement für digitale Freiheitsrechte und ihre politische Umsetzung.

[3]

Lesetipps von KN-ADMIN Helmut Schnug:

»**Überwachungskapitalismus: Wie der Mensch zur Ressource wird.**« von Christian Jakob, 28. November 2020 >> **weiter** [8].

»**Nippons todkranke Gesellschaft: Wie das Land des Lächelns zu weinen beginnt.**« von Christian Jakob, 15. Mai 2019 >> **weiter** [11].

► **Quelle:** Dieser Text wurde erstveröffentlicht am 24. Dezember 2020 auf NETZPOLITIK.org >>**Artikel** [12]. **Lizenz:** Die von NETZPOLITIK verfassten Inhalte stehen, soweit nicht anders vermerkt, unter der Lizenz Creative Commons (Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-NC-SA 4.0 [13]). Die Artikelüberschrift wurde von Helmut Schnug geändert.

ACHTUNG: Die Bilder und Grafiken im Artikel sind nicht Bestandteil des Originalartikels und wurden von KN-ADMIN Helmut Schnug eingefügt. Für sie gelten ggf. andere Lizenzen, siehe weiter unten. Grünfärbung von Zitaten im Artikel und einige Verlinkungen wurden ebenfalls von H.S. als Anreicherung gesetzt.

► Bild- und Grafikquellen:

1. Emberlight-Lampenfassung: Emberlight reiht sich mit seiner intelligenten Beleuchtung [sic!] in den IoT-Totenpool ein. Die Idee von **Emberlight** war es, bestehende Leuchten und Lampen mit einem vernetzten Zuhause auszustatten. Anstatt die Leuchte komplett zu ersetzen oder drahtlose Konnektivität in eine Glühbirne einzubauen, die nur weggeworfen würde, wenn die Glühbirne selbst ersetzt wird, entwickelte das Unternehmen einen Adapter, der zwischen eine normale Glühbirne und die Fassung passt. Dieser hatte WiFi und Bluetooth an Bord, sodass er über eine Smartphone-App ferngesteuert werden konnte. **Bildbearbeitung**: H.S.

2. Turn ANY Bulb Into A Smart Light! (Verwandeln Sie JEDE Glühbirne in ein intelligentes Licht!).**Foto:** Screenshot aus dem Video [14].

3. Nest Cam Indoor: Smarte Indoor-Überwachungskamera von Nest Lab. **Foto:** Nathaniel Railroad. **Quelle:** Wikimedia Commons [15]. Diese Datei ist lizenziert unter der Creative-Commons-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 international“ (CC BY-SA 4.0 [16]).

4. Nest Cam Outdoor: Smarte Outdoor-Überwachungskamera von Nest Lab. **Foto:** Nathaniel Railroad. **Quelle:** Wikimedia Commons [17]. Diese Datei ist lizenziert unter der Creative-Commons-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 international“ (CC BY-SA 4.0 [16]).

5. Joshua A. T. Fairfield ist ein international anerkannter Rechts- und Technologiewissenschaftler, der sich auf digitales Eigentum, elektronische Verträge, Big Data Privacy und virtuelle Gemeinschaften spezialisiert hat. Er hat über das Recht und die Regulierung von E-Commerce und Online-Verträgen sowie über die Anwendung von Standardwirtschaftsmodellen auf virtuelle Umgebungen geschrieben.

Professor Fairfields aktuelle Forschung konzentriert sich auf Big-Data-Datenschutzmodelle und die nächste Generation von rechtlichen Anwendungen für Kryptowährungen. Seine Artikel über den Schutz von Verbraucherinteressen im Zeitalter von Massenverträgen erscheinen regelmäßig in führenden juristischen und juristisch-technischen Fachzeitschriften, und Grundsatzartikel über Verbraucherschutz und Technologie sind unter anderem in der New York Times, Forbes und der Financial Times erschienen.

Vor seiner Tätigkeit als Jurist war Professor Fairfield Technologieunternehmer und arbeitete als Direktor für Forschung und Entwicklung für das Sprachlernsoftware-Unternehmen Rosetta Stone. Im Jahr 2013 wurde er zum Mitglied des American Law Institute gewählt. Fairfield ist Jura-Professor an der 'Washington and Lee University' in den USA und Autor von »Owned. Property, Privacy and the New Digital Serfdom«. **Foto:** privat. Die Bildrechte bleiben beim Urheber! **Quelle:** Webseite der 'Washington and Lee University' >> Infos und Foto [9].

6. Beim Roboterhund **Aibo von Sony**, der in seiner Neuauflage mit seinen Besitzern interagieren und eine digitale Persönlichkeit entwickeln kann, setzt man auf ein Abo-Modell. **Foto:** Jacques GAIMARD, PARIS/FRANCE. **Quelle**: Pixabay [18]. Alle Pixabay-Inhalte dürfen kostenlos für kommerzielle und nicht-kommerzielle Anwendungen, genutzt

werden - gedruckt und digital. Eine Genehmigung muß weder vom Bildautor noch von Pixabay eingeholt werden. Auch eine Quellenangabe ist nicht erforderlich. Pixabay-Inhalte dürfen verändert werden. Pixabay Lizenz [19]. >> Foto [20].

7. Gassi mit Aibo: Wer immer zur selben Zeit mit seinem Roboterhund Gassi gehen mag, muss rund 650 Euro zahlen, um das drei Jahre lang tun zu dürfen. Ansonsten "vergisst" Aibo alles, was er gelernt hat. **Foto:** ETC-USC. **Quelle:** Flickr [21]. **Verbreitung** mit CC-Lizenz Namensnennung 2.0 Generic CC BY 2.0 [22]).

8. Roboterhündchen Aibo - Tier- und Menschersatz gegen zunehmende Vereinsamung: Jemand, der sich Aibo anschafft, hat vielleicht nicht ausreichend Zeit, sich um ein echtes Tier zu kümmern, will aber trotzdem nicht alleine sein. Dass es sich dabei um eine Maschine handelt, die lediglich ein Tier imitiert, ist egal. Bei den Besitzern sind hier, anders als bei einer Überwachungskamera, auf jeden Fall auch Gefühle im Spiel. **Foto:** hiroaki maeda, Tokyo / Japan. **Quelle:** Flickr [23]. **Verbreitung** mit CC-Lizenz Namensnennung-Keine Bearbeitung 2.0 Generic CC BY-ND 2.0 [24]).

9. Aibo "Inuyasha". Als Sony die Produktion des ersten Aibo-Modells eingestellt und es auch keine Ersatzteile mehr gegeben hatte, gab es in Japan Hunderte buddhistische Begräbnisse für die Roboterhunde. Menschen haben zu ihren Roboterhunden eine Bindung aufgebaut, sie wie Tiere behandelt und gepflegt. Daher ist "Bindung mit Drei-Jahres-Abo" wirklich nicht hübsch. Dennoch wurden in Japan nach der Wiedereinführung bis August 2018 rund 20.000 Stück des lernfähigen Aibos mit digitaler Persönlichkeit verkauft. In Japan kostet Aibo rund 1.500 Euro. **Foto:** Chad Kainz, Monterey, CA, USA. **Quelle:** Flickr [25]. **Verbreitung** mit CC-Lizenz Namensnennung 2.0 Generic CC BY 2.0 [22]). Bildausschnitt geändert durch H.S.

10. + 11. Buchcover: »**Hilfe, ich habe meine Privatsphäre aufgegeben! Wie uns Spielzeug, Apps, Sprachassistenten und Smart Homes überwachen und unsere Sicherheit gefährdet**«. von Barbara Wimmer, mitp Verlags GmbH & Co. KG, Frechen >> https://www.mitp.de/ . 1. Auflage, ersch. 10. Dez. 2020, ISBN 978-3-7475-0164-1, **Buch** 16,99 € [D], **E-Book** (PDF & EPUB) 14,99 € [D]. **Buch + E-Book** 19,99€ [D]. alle 272 Seiten.

Quell-URL: https://kritisches-netzwerk.de/forum/internet-der-dinge-die-produkte-gehoeren-gar-nicht-uns

Links
[1] https://kritisches-netzwerk.de/user/login?destination=comment/reply/9025%23comment-form
[2] https://kritisches-netzwerk.de/forum/internet-der-dinge-die-produkte-gehoeren-gar-nicht-uns
[3] https://netzpolitik.org/
[4] https://futurezone.at/author/barbara.wimmer
[5] https://www.emberlight.ie/
[6] https://nest.com/
[7] https://www.heise.de/newsticker/meldung/35C3-Ueber-die-smarte-Gluehbirne-das-Heimnetzwerk-hacken-4259891.html
[8] https://kritisches-netzwerk.de/forum/ueberwachungskapitalismus-wie-der-mensch-zur-ressource-wird
[9] https://law.wlu.edu/faculty/full-time-faculty/joshua-fairfield
[10] https://shroombab.at/
[11] https://kritisches-netzwerk.de/forum/nippons-todkranke-gesellschaft-wie-das-land-des-laechelns-zu-weinen-beginnt
[12] https://netzpolitik.org/2020/internet-der-dinge-die-produkte-gehoeren-gar-nicht-uns/
[13] https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de
[14] https://www.youtube.com/watch?v=AGMH5JFqY_E&list=LLOApJoLY4QMvRdJDagVpt5g&index=2860
[15] https://commons.wikimedia.org/wiki/File:Nest_Cam_Indoor.jpg
[16] https://creativecommons.org/licenses/by-sa/4.0/deed.de
[17] https://commons.wikimedia.org/wiki/File:Nest_Cam_Outdoor.jpg
[18] https://pixabay.com/
[19] https://pixabay.com/de/service/license/
[20] https://pixabay.com/de/photos/roboter-tier-hund-mechanik-design-3947585/
[21] https://www.flickr.com/photos/92587836@N04/24881871407
[22] https://creativecommons.org/licenses/by/2.0/deed.de
[23] https://www.flickr.com/photos/torisan3500/367581937/
[24] https://creativecommons.org/licenses/by-nd/2.0/deed.de
[25] https://www.flickr.com/photos/smaedli/49267362041/
[26] https://kritisches-netzwerk.de/tags/abo-modell
[27] https://kritisches-netzwerk.de/tags/aibo
[28] https://kritisches-netzwerk.de/tags/alexa
[29] https://kritisches-netzwerk.de/tags/allesnetz
[30] https://kritisches-netzwerk.de/tags/always
[31] https://kritisches-netzwerk.de/tags/amazon
[32] https://kritisches-netzwerk.de/tags/assistenzwanzen
[33] https://kritisches-netzwerk.de/tags/augmented-reality-funktion
[34] https://kritisches-netzwerk.de/tags/ausbeutung
[35] https://kritisches-netzwerk.de/tags/ausspionieren
[36] https://kritisches-netzwerk.de/tags/barbara-wimmer
[37] https://kritisches-netzwerk.de/tags/cloud-server
[38] https://kritisches-netzwerk.de/tags/cloud-speicher
[39] https://kritisches-netzwerk.de/tags/cloud-verbindung

[40] https://kritisches-netzwerk.de/tags/contact-tracing
[41] https://kritisches-netzwerk.de/tags/crowdfunding
[42] https://kritisches-netzwerk.de/tags/datenabschopfung
[43] https://kritisches-netzwerk.de/tags/datenausbeutung
[44] https://kritisches-netzwerk.de/tags/datenerfassung
[45] https://kritisches-netzwerk.de/tags/datenkrake
[46] https://kritisches-netzwerk.de/tags/datenmissbrauch
[47] https://kritisches-netzwerk.de/tags/datenschmutz
[48] https://kritisches-netzwerk.de/tags/datenschutz
[49] https://kritisches-netzwerk.de/tags/digital-barone
[50] https://kritisches-netzwerk.de/tags/digitale-personlichkeit
[51] https://kritisches-netzwerk.de/tags/digitale-selbstbestimmung
[52] https://kritisches-netzwerk.de/tags/digitale-unmundigkeit
[53] https://kritisches-netzwerk.de/tags/emberlight
[54] https://kritisches-netzwerk.de/tags/entmundigung
[55] https://kritisches-netzwerk.de/tags/entscheidungsmacht
[56] https://kritisches-netzwerk.de/tags/fremdbestimmung
[57] https://kritisches-netzwerk.de/tags/gesichtserkennung
[58] https://kritisches-netzwerk.de/tags/hausautomation
[59] https://kritisches-netzwerk.de/tags/human-capital
[60] https://kritisches-netzwerk.de/tags/humankapital
[61] https://kritisches-netzwerk.de/tags/humanressourcen
[62] https://kritisches-netzwerk.de/tags/human-resources
[63] https://kritisches-netzwerk.de/tags/internet-der-dinge
[64] https://kritisches-netzwerk.de/tags/internet-things
[65] https://kritisches-netzwerk.de/tags/joshua-t-fairfield
[66] https://kritisches-netzwerk.de/tags/kaufboykott
[67] https://kritisches-netzwerk.de/tags/kauferboykott
[68] https://kritisches-netzwerk.de/tags/kaufverhalten
[69] https://kritisches-netzwerk.de/tags/kaufverweigerung
[70] https://kritisches-netzwerk.de/tags/konditionierung
[71] https://kritisches-netzwerk.de/tags/konsumentenverhalten
[72] https://kritisches-netzwerk.de/tags/konsumsklaven
[73] https://kritisches-netzwerk.de/tags/konzernfaschismus
[74] https://kritisches-netzwerk.de/tags/konzernherrschaft
[75] https://kritisches-netzwerk.de/tags/konsumboykott
[76] https://kritisches-netzwerk.de/tags/konsumentenboykott
[77] https://kritisches-netzwerk.de/tags/korporatokratie
[78] https://kritisches-netzwerk.de/tags/kunstliche-intelligenz
[79] https://kritisches-netzwerk.de/tags/lauschangriff
[80] https://kritisches-netzwerk.de/tags/manipulationspotential
[81] https://kritisches-netzwerk.de/tags/nest-aware-abo
[82] https://kritisches-netzwerk.de/tags/nest-cam-indoor
[83] https://kritisches-netzwerk.de/tags/nest-cam-outdoor
[84] https://kritisches-netzwerk.de/tags/nest-kameras
[85] https://kritisches-netzwerk.de/tags/nest-labs
[86] https://kritisches-netzwerk.de/tags/nutzerdaten
[87] https://kritisches-netzwerk.de/tags/nutzliche-idioten
[88] https://kritisches-netzwerk.de/tags/nutzungsboykott
[89] https://kritisches-netzwerk.de/tags/nutzungsverweigerung
[90] https://kritisches-netzwerk.de/tags/personenbezogene-daten
[91] https://kritisches-netzwerk.de/tags/preisdiktat
[92] https://kritisches-netzwerk.de/tags/preistreiberei
[93] https://kritisches-netzwerk.de/tags/privatsphare
[94] https://kritisches-netzwerk.de/tags/roboterhund
[95] https://kritisches-netzwerk.de/tags/roboterhunde
[96] https://kritisches-netzwerk.de/tags/sicherheitslucken
[97] https://kritisches-netzwerk.de/tags/smart-citys
[98] https://kritisches-netzwerk.de/tags/smart-homes
[99] https://kritisches-netzwerk.de/tags/smart-home-technologie
[100] https://kritisches-netzwerk.de/tags/smarte-lampenfassung
[101] https://kritisches-netzwerk.de/tags/smarte-lampensockel
[102] https://kritisches-netzwerk.de/tags/sony
[103] https://kritisches-netzwerk.de/tags/sprachassistenten
[104] https://kritisches-netzwerk.de/tags/surveillance-assets
[105] https://kritisches-netzwerk.de/tags/surveillance-capitalism
[106] https://kritisches-netzwerk.de/tags/tech-giganten
[107] https://kritisches-netzwerk.de/tags/technikabhangigkeit

[108] https://kritisches-netzwerk.de/tags/tech-konzerne
[109] https://kritisches-netzwerk.de/tags/totaluberwachung
[110] https://kritisches-netzwerk.de/tags/uberwachung
[111] https://kritisches-netzwerk.de/tags/uberwachungsguter
[112] https://kritisches-netzwerk.de/tags/uberwachungskamera
[113] https://kritisches-netzwerk.de/tags/uberwachungskapitalismus
[114] https://kritisches-netzwerk.de/tags/uberwachungsokonomie
[115] https://kritisches-netzwerk.de/tags/vereinsamung
[116] https://kritisches-netzwerk.de/tags/verhaltensmanipulation
[117] https://kritisches-netzwerk.de/tags/vernetzte-gerate
[118] https://kritisches-netzwerk.de/tags/vernetztes-spielzeug
[119] https://kritisches-netzwerk.de/tags/vernetzung