*Handout Gruppe J: Helmut Hörner, Dragan Božic*

# *Abschätzung der Auswirkungen von „Smart Home“ Technologien im privaten Wohnbereich*

*(13.12.2020)*

## 1 Einführung

**Definition:** Der „Smart-Home“-Begriff existiert bereits seit den frühen 2000-er Jahren. [20] Die Definition von „Smart Home“ variiert von Autor zu Autor, aber umfasst im Allgemeinen elektronische Systeme, die in Wohnungen und Häusern Haushaltsgeräte, Unterhaltungselektronik, Haushaltsinstallationen (wie Strom und Heizung), digitale Assistenten (wie z.B. „Alexa“) und Sicherheitstechnik vernetzen, automatisieren, und remote über das Internet zugänglich machen. [1]

**Eingrenzung:** Das vorliegende Projekt fokussiert sich auf den Einsatz von Smart-Home Technologien im engeren Sinn, d.h. auf den Einsatz solcher Technologien im privaten Wohnbereich. Nicht betrachtet wurden spezielle oder abweichende Auswirkungen dieser Technologien im nicht-privaten Bereich (z.B. in Büros, Krankenhäusern, Hotels, etc.)

**Annahmen:** Aufgrund des aktuellen Trends (siehe Kapitel 3) gehen wir gehen davon aus, dass sich Smart-Home Technologien vermehrt durchsetzen und zur Anwendung kommen werden. [6], [11] Dass diese Technologien dabei das Potential haben, problematische Effekte zu zeigen, die den intendierten Zwecken zuwiderlaufen, ist bereits jetzt durch aktuelle Auswirkungen evident. [7, S. 35ff], [8, S. 719ff]

## 2 Methode

Wir wählen die Methode der „Szenarioentwicklung“ und Berücksichtigung gesellschaftlicher Entwicklunsdimensionen: „Quantitative Daten und Information werden mit qualitativen Informationen, Einschätzungen und Meinungen verknüpft, so dass als Ergebnis detaillierte Beschreibungen einer bzw. mehrerer möglichen Zukunftssituationen unter ganzheitlichem Aspekt entstehen“ [2, S. 12]

## 3 Horizon Scanning

Wie Abbildung 1 zeigt, wächst der Smart-Home Markt global beständig. Eine Extrapolation dieses Trends legt den Schluss nahe, dass Smart-Home Systeme in naher Zukunft immer mehr an Bedeutung gewinnen werden.

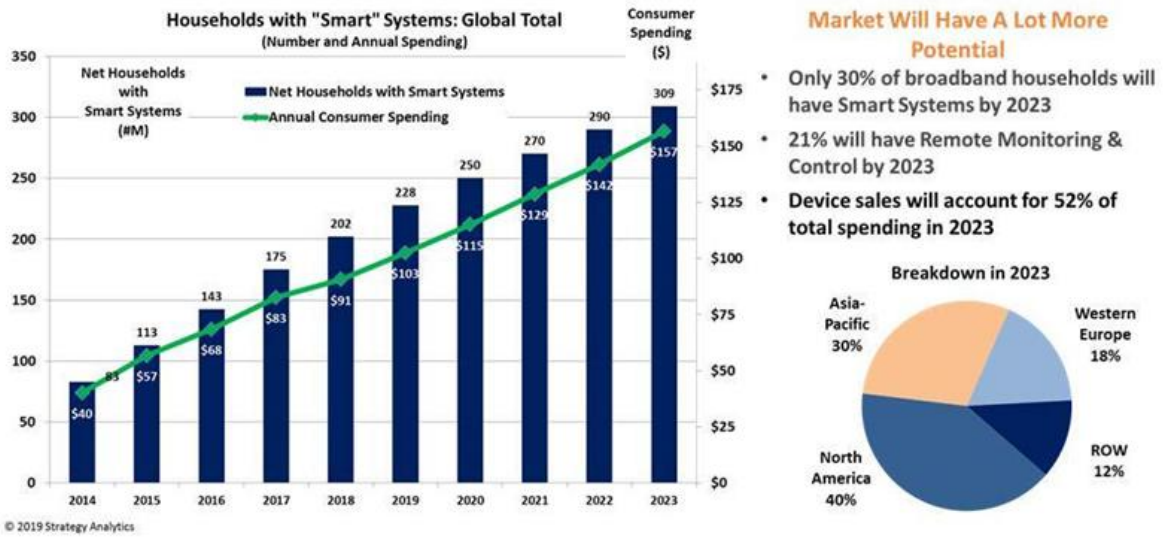


Abbildung 1: Entwicklung des Smart-Home Marktes (aus [10])

## 3.1 Kritische Komponenten

Bereits heute lassen sich zahlreiche Smart-Home Komponenten identifizieren, die problematische Effekte zeigen, die den intendierten Zwecken zuwiderlaufen und Risikobehaftet sind. Unsere Analyse hat dabei vor allem die folgenden Komponenten identifiziert:

### 3.1.1 Smart-Home-Komponenten mit Risiko für die Privatsphäre

**Smart-Speaker:** Smart-Speaker haben nachweislich private Gespräche von Benutzer*innen ohne deren Wissen aufgezeichnet. Mitarbeiter des Herstellers haben Gesprächsprotokolle angelegt um „die Spracherkennung zu verbessern". [14]

**Smart-TV:** Mittels Smart-TVs überwachen und dokumentieren bereits heute Unternehmen nachweislich den Videokonsum der Benutzer*innen. Hinzu kommt, dass viele Smart-TVs Mikrofone, manche sogar Kameras integriert haben, mit denen der Hersteller, aber prinzipiell auch Hacker oder staatliche Institutionen die Benutzer*innen im privaten Bereich ausspionieren können. [15], [17]

**„Smarte" Internet-Sicherheitsanlagen:** Viele moderne Sicherheitssysteme bieten (oder verlangen) einen Internetanschluss, damit Anwender*innen ihre Wohnung auch in Abwesenheit überwachen können. Oft sind solche Sicherheitssysteme auch mit Kameras ausgestattet. [4] Es ergeben sich dieselben Risiken wie zuvor.

**Smart-Meter:** Smart-Meter („intelligente" Stromzähler) senden Informationen über den aktuellen Stromverbrauch laufend an den Netzbetreiber. Ein Hacker kann diese Informationen nutzen, um Informationen über An- und Abwesenheitszeiten zu bekommen. [5], [13]

### 3.1.2 Smart-Home-Komponenten mit Risiko für die persönliche Sicherheit

**Smart-Locks:** Smart-Locks mögen komfortabler sein, jedoch können Sie gehackt werden. [11], [12] Zudem macht die Komplexität des Systems Smart-Locks anfälliger für Fehlfunktionen: Technische Versagen, oder einfach nur ein Stromausfall, kann dazu führen, dass man/frau unverschuldet aus der eigenen Wohnung ausgesperrt wird. [2]

**Sicherheitssystem mit Internetanschluss:** Ein vergleich aktueller Alarmanlagen mit Internetanschluss hat ergeben, dass viele davon leicht gehackt werden können. Bei einem Hersteller waren hierfür zudem nur geringe Kenntnisse erforderlich [3], [4]

**Smart-Meter:** Smart-Meter („intelligente" Stromzähler) werden als wesentliche Komponenten künftiger flexibler und adaptiver Stromnetze angesehen. Sie bringen jedoch das Risiko, dass durch einen Hackerangriff großflächig falsche Verbrauchsinformationen an die Strombetreiber geschickt werden, was zu einem Zusammenbruch der Stromversorgung führen kann. [13]

### 3.1.3 Smart-Home-Komponenten mit Obsoleszenzrisiko

**Smart-Speaker:** Smart-Speaker mit Assistenzfunktion sind auf die Server der Hersteller angewiesen. Sobald diese nicht mehr bereitstellen, funktionieren sie nicht mehr.

**Smart-TV:** Ähnliches gilt für Smart-TVs. Bereits im Jahr 2018 mussten Anwender von Samsung-TVs die Erfahrung machen, dass ihr „smartes" Gerät plötzlich (möglicherweise kaufentscheidende) Funktionen verlor, weil der Hersteller bzw. dessen Vertragspartner beschlossen hatten, die entsprechenden Dienste für diese „alten" Geräte (Baujahr 2013) einzustellen. [18], [19]

**Smart-Bulbs mit App-Steuerung:** Die gleiche Erfahrung mussten Kund*innen machen, die die erste Generation der Phillips Hue Bridge Beleuchtungssystems angeschafft hatten: Ab Frühjahr 2020 war es nicht mehr möglich, die Leuchtmittel über die Fernverbindung zu steuern, weil der Support eingestellt wurde. [16]

# 4 360° Envisioning

**Auswirkungen:** Auf Basis der recherchierten Risiken lässt sich extrapolieren, dass die Wahrscheinlichkeit des Eindringens in die Privatsphäre von Anwender*innen durch Hersteller, staatliche Institutionen oder Hacker zunehmen wird [4], [5], [13], [13], [15], [17]. Gleiches gilt für die erwähnten Sicherheitsrisiken[2], [3], [4], [11], [12], [13] und Obsoleszenzeffekte[16], [18], [19].

**Schlüsselfaktoren:** Wir konnten die folgenden Schlüsselfaktoren, die einen wesentlichen Einfluss auf die beschriebenen Auswirkungen haben werden, identifizieren:

- **Gesetzgebung und Regulierung:** Die regulatorische und legistische Situation wird wesentlichen Einfluss darauf haben, ob die (im derzeitigen, nur schwach regulierten, Umfeld stark auftretenden) Probleme reduziert werden können.
- **Gesellschaftliche Entwicklung:** Es gibt auch in westlichen Gesellschaften eine merkliche Tendenz dazu, die „präventive" Überwachung der Bürger*innen durch staatliche Behörden zuzulassen. Sollte sich dieser Trend durchsetzen, dann droht ein Eindringen des Staates in die Privatsphäre mittels

# 5 Szenarioentwicklung

Basierend auf den identifizierten Schlüsselfaktoren wurden Szenarien mit zwei „Achsen" entwickelt:

**Horizontale Szenario-Achse:**

Diese Achse stellt die Antipoden „wenig gesetzliche Regulierung" vs. „starke Regulierung der Hersteller" dar.

- „Wenig gesetzliche Regulierung" ist ein Szenario, in dem keine spezifischen (bzw. keine wirksamen) Regulierungen erlassen werden, die Hersteller zwingen, bei ihren Produkten auf Datensicherheit und Kompatibilität zu achten.
- „Starke Regulierung der Hersteller" ist ein Szenario, in dem spezifische und wirksame Regulierungen erlassen werden, so dass Hersteller gezwungen sind, bei ihren Produkten auf Datensicherheit und Kompatibilität zu achten.

**Vertikale Szenario-Achse:**

Diese Achse stellt die Antipoden „Überwachungsstaat" vs. „liberaler Rechtsstaat" dar.

- „Überwachungsstaat" ist ein Szenario, in dem bestimmte staatliche Organe befugt sind, die Bürger und Bürgerinnen „präventiv" zu überwachen.
- „Liberaler Rechtsstaat" ist ein Szenario, in dem der Staat dies nicht präventiv und nur unter strengen rechtsstaatlichen Auflagen tut.

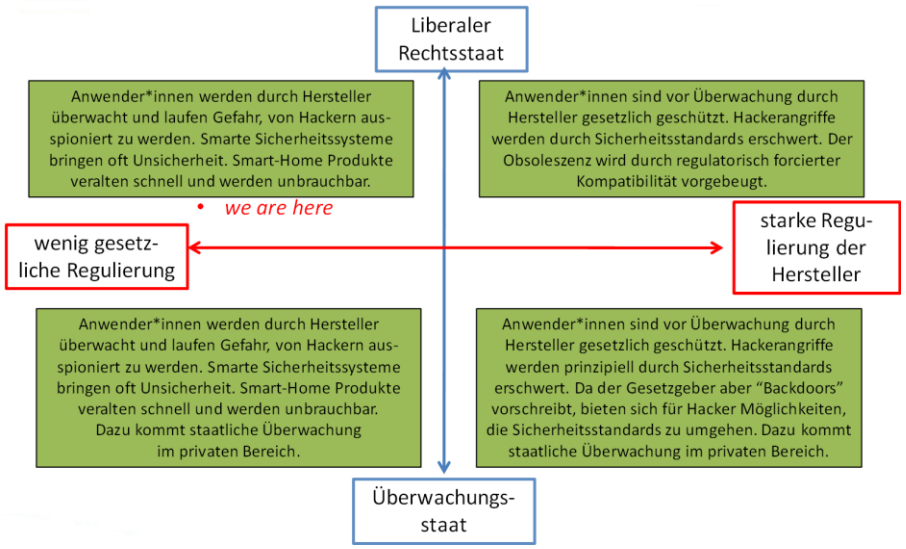


**Abbildung 2: Szenarien entwickelt aufgrund der Schlüsselfaktoren**

# 6 Reflexion und Empfehlungen

Als Ergebnis der dargelegten Analyse scheint es uns wesentlich, dass Regulierer auf supranationaler Ebene (z.B. legistisch auf europäischer Ebene, oder auf Ebene von internationale Normierungsinstitutionen) möglichst rasch *verbindliche und durchsetzbare Sicherheitsstandards* für „Smart-Home"-Produkte verabschieden. Anderenfalls dürfte sich der derzeitige Trend, gekoppelt mit den beschriebenen Risiken, ungebremst fortsetzen.

Voraussetzung hierzu ist, dass beim Gesetzgeber überhaupt erst einmal ein Bewusstsein für die beschriebenen Probleme im Zusammenhang mit Smart-Home Produkten entsteht. Experten sind aufgerufen, Organe Gesetzgebender Körperschaften entsprechend zu informieren.

Gleichzeitig scheint es den Autoren wichtig, auch in der Öffentlichkeit ein Bewusstsein für die Gefahr der präventiven Überwachung im privaten Bereich durch staatliche und nichtstaatliche Stellen mittels „Smart-Home" Systemen zu schaffen.

# 7 Referenzen


[1] M. Chana, D. Estève, C. Escriba und . Campo, "A review of smart homes—Present state and future challenges" in "Computer Methods and Programs in Biomedicine", Vol 91, Issue 1, July 2008, S. 55-81

[2] O. Albers, A. Broux, "Zukunftswerkstatt und Szenariotechnik: ein Methodenbuch für Schule und Hochschule", Beltz, 1999.

[3] J. Merkert und S. Hansen, "Smart Alarm - Sechs vernetzte Alarmanlagen im Test" in c't 3/2017, S. 90

[4] N. Jurran, "Hintereingang inklusive - Fatales Sicherheitsleck beim Smart-Home-System von Loxone" in c't Magazin für Computertechnik 19/2016, S. 72

[5] O. Ur-Rehman, N. Zivic und C. Ruland, "Security issues in smart metering systems," 2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, 2015, pp. 1-7, doi: 10.1109/SEGE.2015.7324615.

[6] N. Balta-Ozkana, B. Botelerb, O. Amerighic, "European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy", doi: 10.1016/j.erss.2014.07.007

[7] T. Hargreaves, C. Wilson (2017) Perceived Benefits and Risks of Smart Home Technologies. In: Smart Homes and Their Users. Human–Computer Interaction Series. Springer, Cham. DOI: 10.1007/978-3-319-68018-7_3

[8] A. Jacobsson, M. Boldt, B. Carlsson, A risk analysis of a smart home automation system, Future Generation Computer Systems, Volume 56, 2016,
S. 719-733

[9] S. Kozubaev, F. Rochaix, C. F. DiSalvo, C. A. LeDantec. Spaces and Traces: Implications of Smart Technology in Public Housing.
Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 2019, Paper No.: 439, S. 1–13, DOI: 10.1145/3290605.3300669

[10] W. Ablondi, J. Narcotta, "2019 Global Smart Home Forecast - September 2019",Strategy Analytics Report September 2019

[11] C. Dardaman, Breaking & Entering with Zipato SmartHubs, https://blackmarble.sh/zipato-smart-hub/

[12] E. Fernandes, J. Jung and A. Prakash, "Security Analysis of Emerging Smart Home Applications," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 636-654, doi: 10.1109/SP.2016.44.

[13] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in IEEE Security & Privacy, vol. 7, no. 3, pp. 75-77, May-June 2009, doi: 10.1109/MSP.2009.76.

[14] J. Lau, B. Zimmerman, F. Schaub, "Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers", Proceedings of the ACM on Human-Computer Interaction, November 2018, Article No.: 102, doi: 10.1145/3274371

[15] S Lee, S Kim : "Hacking, surveilling and deceiving victims on smart tv", Blackhat Briefing 2013 (2013)

[16] Jonas: "Das wars: Keine Unterstützung mehr der 1. Philips Hue Bridge Generation" https://www.smartlights.de/licht/philips-hue/das-wars-keine-unterstuetzung-mehr-der-1-philips-hue-bridge-generation/ (Mai 2020)

[17] B. Michéle and A. Karpow, "Watch and be watched: Compromising all Smart TV generations," 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2014, pp. 351-356, doi: 10.1109/CCNC.2014.6866594.

[18] M. Moon: "Samsung's older smart TVs are losing remote control app support", https://www.engadget.com/samsung-killing-smart-view-app-103148010.html

[19] A. Villas-Boas: "Netflix will soon stop working on some older Samsung smart TVs", Nov, 2019, https://www.businessinsider.de/international/netflix-stop-working-old-samsung-smart-tvs-december-1-2019-11

[20] L. Jiang, D.-Y. Liu und B. Yang, "Smart Home Research" in Proc. of 2004 International Conference on Machine Learning and Cybernetics, Vol.2, pp.659-663, 26- 29 Aug. 2004, DOI 10.1109/ICMLC.2004.1382266