

Meine Wohnung gehört mir

- Über Hausautomation und die (Vor-)Herrschaft der großen Konzerne

Antonia Uhle

Forschungsgruppe Prof. Aschenbrenner

Hochschule Aalen

In Deutschland garantiert das Grundgesetz (1949, Art. 13 Abs. 1 ff.) die Unverletzlichkeit der Wohnung. Der Artikel steht im engen Zusammenhang mit dem allgemeinen Persönlichkeitsrecht und schützt die räumliche Privatsphäre, in der die einzelne Person das Recht hat, „in Ruhe gelassen zu werden“.

Gleichzeitig existiert auch hier ein wachsender Markt für alle Arten von Hausautomation. Von der Industrie über das Netz ist das Konzept der "selbstarbeitenden Dinge" inzwischen auch in den Wohnorten der Menschen angekommen. Ein breites Angebot an digitalen Helfern, Assistenz- und Komfortfunktionen steht zur Verfügung um sich selbst das Leben etwas bequemer zu gestalten. Diverse Online-Services werben damit von überall und zu jeder Tageszeit z.B. seine Wohnungstür für den Paketboten zu öffnen (Ring), die Temperatur zu regeln (Nest), oder auch die Katze zu beobachten.

Alle diese Angebote bedienen ein menschliches Bedürfnis nach Bequemlichkeit, empfundener Einfachheit und dem Gefühl Dinge unter Kontrolle zu haben. Hier stellt sich jedoch die Frage ob eben dieses Gefühl hier gerechtfertigt ist.

Anbieter der Dienste und Geräte sind meist die auch als "Hypergiganten" (Labovitz, C., 2010) bezeichneten großen IT Konzerne wie beispielsweise Google oder Amazon. Diese bieten zu oft sehr günstigen Preisen Methoden an, viele der kleinen Alltäglichkeiten für den Nutzer zu erledigen. Über Vernetzung der Geräte und Dienste sind dann auch komplexere Aktionen denkbar: Die Heizung wird eingeschaltet, sobald der Nutzer den Arbeitsort verlässt, die Beleuchtung geht an, sobald man die Wohnung betritt. Der Nutzende glaubt hier selbst die absolute Kontrolle zu haben, dies ist jedoch ein Trugschluß. Ein Scheingefühl, welches durch elegante Oberflächen und Funktionalität vermittelt wird, in Wirklichkeit aber eine absolute Transparenz der Nutzenden gegenüber den Hypergiganten erzwingt.

Dafür öffnen die Nutzenden den Firmen bereitwillig ihre Türen, Terminkalender und Telefone, und machen sich damit abhängig von Unternehmen die für "too big to fail" (infoworld, 2009) gehalten werden. Die Unternehmen gewinnen damit zum einen immer mehr Informationen über ihre Kunden, zum anderen, teils sogar physisch, kontrollierenden Einfluss auf deren Leben. Letztendlich also Macht.

Die Kritik an der Machtakkumulation der Hypergiganten wird meist und insbesondere unter dem Stichwort Netzneutralität diskutiert. Fiebig & Aschenbrenner beschäftigen sich 2022 allerdings auch mit der Zukunft des Internets in Zeiten knapper werdender Ressourcen und formulieren mit ihrer dritten These das Spannungsverhältnis zwischen Privatsphäre und Sicherheit, sowie in der fünften These, dass man auf das Scheitern von Hypergiganten vorbereitet sein soll. Viele IT Systeme und Teile des Internets sind aktuell sehr eng mit den Hypergiganten Amazon, Facebook, Apple und Google verknüpft.

Keiner rechnet damit dass sie auch Konkurs gehen oder verschwinden könnten - ähnlich wie bei Lehman Brothers. Als möglichen Auslöser nennen die Autoren die explodierenden Energiepreise, da ein einziges Rechenzentrum den Strom von 50.000 Haushalten verbrauchen kann (Monserrate, 2022).

Beispiele für Ausfälle, Versagen, oder auch Privatsphärenverletzungen dieser Hypergiganten und deren Hausautomatisierungssysteme sind dagegen zahlreich:

2022 fiel beim dem SmartHome Anbieter Wink der Cloudservice für mehr als 2 Wochen aus. Nutzende konnten ihre verbundenen Geräte, darunter auch Türschlösser, nicht bedienen (TheVerge, 2022).

Im Jahr 2021 hatte Amazon Web Services (AWS) einen Ausfall, der sich auf die Cloud-Dienste von Ring, einem Hersteller von intelligenten Türklingeln und Überwachungskameras, auswirkte. Dadurch konnten einige Benutzer keine Verbindung zu ihren Geräten herstellen oder diese steuern (BleepingComputer, 2021).

2020 kündigt Google an das Nest-Security-System einzustellen. Damit würden die teuren Geräte von einem Tag auf den anderen nutzlos (Wagoner, 2020).

Im Jahr 2019 führte ein Ausfall von Google Cloud zu einer Beeinträchtigung der Nest-Heizungssteuerung. Benutzer konnten nicht auf ihre Thermostate zugreifen oder die Temperatur einstellen (BusinessInsider, 2019). Etwas ähnliches war drei Jahr zuvor schon einmal passiert. Ebenfalls in 2019 mehrten sich die Berichte über gehackte Ring-Kameras, welche dann von Kriminellen genutzt wurden, um das Verhalten der Bewohnenden auszuspionieren oder sie zu bedrohen (Heise, 2019).

Bereits im Jahr 2017 bereits kam es zu einem Problem mit der Smart-Home-Schließanlage Lockstate 6i, als ein herstellerseitiges Software-Update schief lief und dazu führte, dass die Schlösser nicht mehr funktionierten. Das Update sollte eigentlich dazu dienen, eine Sicherheitslücke zu schließen. Das Problem betraf rund 500 Kunden, die nicht mehr in ihre Häuser oder Geschäfte konnten (TheVerge, 2017).

Diese Beispiele verdeutlichen, wie die Abhängigkeit von Clouddiensten dazu führt, dass Ausfälle in der Cloud auch Auswirkungen auf die individuelle Person haben. Die Wohnung, als ehemals rein privater Raum, wird darüber zunehmend öffentlich und verletzlich, häufig auch ohne dass es den Bewohnenden bewusst ist.

Es wird also Zeit, dass diese Entwicklung nicht nur kritisch in Frage gestellt wird, sondern dass aktiv nach anderen Lösungen gesucht wird. In meiner Langfassung und meinem Vortrag möchte ich auf existierende alternative Lösungen eingehen und das Praxisbeispiel meiner eigenen Wohnung vorstellen.

GG. (1949). https://www.gesetze-im-internet.de/gg/art_13.html

Ring. (2023). *Videotürklingeln von Ring*. <https://de-de.ring.com/pages/doorbells>

Nest. (2023). *Nest Learning Thermostat*. https://store.google.com/ch/product/nest_learning_thermostat_3rd_gen?hl=de

Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J., & Jahanian, F. (2010). *Internet inter-domain traffic*. ACM SIGCOMM Computer Communication Review, 40(4), 75-86.

Infoworld. (15 Oct 2009). *Is Google too big to fail?* <https://www.infoworld.com/article/2630232/is-google-too-big-to-fail-.html>

Fiebig, T., & Aschenbrenner, D. (2022). *13 propositions on an internet for a "burning world"*. In Proceedings of the ACM SIGCOMM Joint Workshops on Technologies, Applications, and Uses of a Responsible Internet and Building Greener Internet (pp. 1-5).

Monserrate, Steven Gonzalez (2022). *The Staggering Ecological Impacts of Computation and the Cloud*. <https://thereader.mitpress.mit.edu/the-staggering-ecologicalimpacts-of-computation-and-the-cloud/>

TheVerge. (14. Jul 2022). *Wink says it's down but not out*. <https://www.theverge.com/2022/7/14/23217086/wink-smart-home-hub-outage>

BleepingComputer. (7 Dez 2021). *AWS outage impacts Ring, Netflix, and Amazon deliveries*. <https://www.bleepingcomputer.com/news/technology/aws-outage-impacts-ring-netflix-and-amazon-deliveries/>

Ara Wagoner. (2020). *Nest Secure is being discontinued and current owners are losing their minds*. <https://www.androidcentral.com/nest-secure-being-discontinued-and-people-are-rightfully-losing-their-minds>

BusinessInsider. (2 Jun 2019). *Google Cloud outage takes down Snapchat, YouTube, and Gmail in parts of the United States*. <https://www.businessinsider.com/google-cloud-outage-snapchat-youtube-gmail-down-2019-6>

Heise. (17 Dez 2019). *Der Hacker im Smart Home: Amazons Ring-Kameras werden immer öfter gehackt*. <https://www.heise.de/news/Der-Hacker-im-Schlafzimmer-Amazons-Ring-Kameras-werden-massenhaft-gehackt-4617254.html>

TheVerge. (15. Aug 2017). *Smart lock vendor accidentally bricks its own locks through firmware update*. <https://www.theverge.com/circuitbreaker/2017/8/15/16151798/lockstate-6i-software-update-break-lock>