M. Hansen, L. Lo Iacono, D. Reinhardt, and H. Zwingelberg. Vergleichbare Transparenz von IoT-Privatheitseigenschaften. Datenschutz und Datensicherheit - DuD, 49(7):425–430. DOI: 10.1007/s11623-025-2115-2

Marit Hansen, Luigi Lo Iacono, Delphine Reinhardt, Harald Zwingelberg

Vergleichbare Transparenz von IoT-Privatheitseigenschaften

Der Einsatz von IoT-Geräten ist mit Risiken für die Privatheit der Nutzenden und ihrer Umgebung verbunden. Eine Plattform soll dabei helfen, die Privatheitseigenschaften von IoT-Geräten darzustellen und sie miteinander zu vergleichen.

Dr. h.c. Marit Hansen

ist Landesbeauftragte für Datenschutz Schleswig-Holstein und damit Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein
E-Mail:marit.hansen@datenschutzzentrum.de

Prof. Dr.-Ing. Luigi Lo Iacono

ist Professor für IT-Sicherheit an der Justus-Liebig-Universität Gießen und dort auch der gesamtuniversitäre Informationssicherheitsbeauftragte

E-Mail: luigi.lo_iacono@uni-giessen.de

Prof. Dr.-Ing. Delphine Reinhardt

ist W3-Professorin an der Georg-August-Universität Göttingen und leitet dort die Forschungsgruppe Computer Sicherheit und Privatheit.

E-Mail: reinhardt@cs.uni-goettingen.de

Harald Zwingelberg

ist Jurist und Referatsleiter für Datenschutz-Forschungsprojekte beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

E-Mail: hzwingelberg@datenschutzzentrum.de

1 Herausforderungen für die Privatheitim Internet of Things (IoT)[1]

Die Anzahl der IoT-Geräte in unserem privaten und beruflichen Umfeld steigt stetig an. Prognosen zufolge wird es im Jahr 2025 mehr als 30 Milliarden dieser Geräte geben.[2] Durch eingebettete Sensoren und Hyperkonnektivität verbessern IoT-Geräte einerseits unsere Lebensqualität. Andererseits ermöglichen sie jedoch das umfangreiche und invasive Erheben und Sammeln von Daten. Die Kombination dieser Daten kann zu detaillierten Profilen führen, die umfassende Rückschlüsse auf die persönlichen Gewohnheiten und Vorlieben der Betroffenen zulassen. Beispielsweise haben zahlreiche Untersuchungen gezeigt, dass feingranulare Stromverbrauchsdaten mit hoher Genauigkeit Aufschluss über die Art und Betriebsmodus benutzter Haushaltgeräte oder im Fall von Fernsehern über Videoinhalte[3] geben können.[4]

In der Praxis ist oft nicht nachvollziehbar, welche personenbezogenen Daten von den IoT-Geräten erfasst, verarbeitet und mit Dritten geteilt werden. Demzufolge birgt der Einsatz von IoT ein erhebliches Risiko für die Privatheit der Nutzenden. Im Smart Home betrifft dies zusätzlich Familienmitglieder, Freunde sowie ggf. völlig unwissende Bekannte und Besucher. IoT-Nutzende müssen in derartigen Kontexten deshalb nicht nur den Schutz ihrer eigenen Daten und Interessen beachten, sondern auch die Schutzinteressen Dritter, deren Privatheit vom Betrieb der IoT-Geräte berührt wird. Damit finden sich IoT-Nutzende in einer Doppelrolle als betroffene Personen sowie als datenschutzrechtlich Verantwortliche – bei der Nutzung von IoT-Geräten außerhalb der persönlichen Sphäre – wieder.

2 Aktueller Stand

Angesichts dieser Herausforderungen ist die Auswahl von IoT-Geräten anhand ihrer Privatheitseigenschaften von großer Be-

1 Das Vorhaben *Unboxing.IoT.Privacy* wird mit Mitteln des Bundesministeriums für Bildung und Forschung gefördert (Förderkennzeichen: 16KIS1931K), https://iot-privacy.info/.

2 Statistica, „Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025". https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.

3 Ulrich Greveler u. a., „Identifikation von Videoinhalten über granulare Stromverbrauchsdaten". In: *SICHERHEIT 2012–Sicherheit, Schutz und Zuverlässigkeit*.

4 Andreas Reinhardt u. a., „Averting the Privacy Risks of Smart Metering by Local Data Preprocessing". In: Pervasive and Mobile Computing (PMC), 2015.

deutung. Um den Nutzenden zu ermöglichen, informierte Entscheidungen zu treffen, sind *transparente, verständliche und vergleichbare Bewertungskriterien* erforderlich. Die bisherige Forschung in Bezug auf IoT-Privatheit nimmt primär technische Schutzmaßnahmen in den Blick, die während des Betriebs von IoT-Geräten zum Einsatz kommen. IoT-Nutzende sollten jedoch bereits bei der Auswahl und dem Vergleich von IoT-Geräten die Risiken für die Privatheit noch vor dem Kauf abwägen können. Obwohl häufig detaillierte Informationen zu den Funktionen des IoT-Geräts oder Kundenrezensionen vorliegen, sind spezifische Details zur Verarbeitung personenbezogener Daten oft weniger oder gar nicht zugänglich. Aufgrund dieser mangelhaften Informationslage kann meist nur gemutmaßt werden, ob und ggf. welche Verarbeitungen personenbezogener Daten tatsächlich stattfinden.

2.1 Unabhängige Informationsplattformen

Die oft einzig verbleibende Alternative besteht darin, eigenständig zu recherchieren. Diese Recherche stellt besonders für Laien eine Herausforderung dar, da es für sie heutzutage kaum möglich ist, Informationen zu finden, die allgemeinverständlich sind und ihnen ein Gesamtbild über alles für sie Relevante vermitteln. Außerdem sind die online auffindbaren Informationen oft unzuverlässig.

Hier setzt die Plattform „*Privacy Not Included*“[5] der Mozilla Foundation an. Sie bietet eine praktische Lösung, indem sie eine Liste von Produkten zur Verfügung stellt, die in Bezug auf Datenschutz, Informationssicherheit und den Einsatz von Künstlicher Intelligenz bewertet werden. Diese Bewertungen beruhen auf einer Kombination aus moderierten Beiträgen der Mozilla Foundation und Bewertung von Nutzenden, zudem können Nutzende neue Produkte zur Bewertung vorschlagen. Allerdings führen die häufigen Veränderungen von Hardware und Firmware dazu, dass die Bewertungen schnell veralten. Zudem fehlt es an standardisierten Bewertungskriterien, was transparente und faire Vergleiche erschwert. Eine mögliche Lösung könnte in der Zertifizierung von IoT-Geräten liegen. Dies stellt jedoch angesichts der schieren Masse an im Markt verfügbaren IoT-Geräten, deren typischerweise kurzen Lebenszyklen und der hochfrequenten Aktualisierungen eine Herausforderung dar.

Mit der Cyberresilienz-Verordnung (Cyber Resilience Act, CRA) wurde im November 2024 eine europäische Verordnung zur Regelung von Produkten mit digitalen Elementen verabschiedet, die auch IoT-Geräte umfasst. Ziele des CRA sind, dass Produkte mit digitalen Elementen für einen ausreichend sicheren Einsatz („Security by Design“) entwickelt und betrieben werden und aufgrund von Synergien mit „Data Protection by Design“ und besonderen Datenschutzkriterien auch zum Privatsphärenschutz Einzelner beigetragen wird.[6] Hersteller, Importeure und Händler werden verpflichtet, eine Reihe von Anforderungen an die Produkte umzusetzen. Der CRA regelt für IoT-Produkte u. a. verpflichtende nach Risiko gestaffelte[7] Konformitätsbewertungsverfahren, deren Durchführung die Voraussetzung für ein CE-Zeichen ist. Diese reichen von herstellerinternen Kontrollverfahren über Baumusterprüfungen und umfassenden Qualitätsmanagementsysteme bis zu einer (noch nicht verfügbaren) Zertifizierung. Abgedeckt werden neben Sicherheitszielen auch einige Datenschutzaspekte. Für wichtige oder kritische Produkte sind über den Lebenszyklus des Produkts wiederkehrende externe Prüfungen erforderlich. Für Produkte, die weder als wichtig noch als kritisch eingestuft werden, können Selbstattestierungen ausreichen.

2.2 Siegel und Kennzeichnungen

Neben der Bereitstellung unabhängiger Bewertungen zur Privatheit existieren Ansätze, um Verbraucher*innen mithilfe von Siegeln und Kennzeichnungen über die Informationssicherheit und Datenschutzfreundlichkeit von IoT-Geräten zu informieren. Diese Ansätze lassen sich grob in drei Typen einteilen:[8]

- *Binäre Gütesiegel*, die angeben, ob ein Gerät gemäß bestimmten Vorgaben zertifiziert ist oder nicht,
- *abgestufte Gütesiegel*, die Informationssicherheit und Datenschutz quantifizieren, um zwischen unterschiedlichen Niveaus unterscheiden zu können und
- *informative Kennzeichnungen*, die wesentliche Informationen über ein Gerät mitteilen.

In der Praxis kommen aktuell fast ausschließlich binäre und abgestufte Gütesiegel zur Informationssicherheit zum Einsatz. Solche Siegel werden sowohl von privaten Unternehmen als auch staatlichen Stellen angeboten. So vergibt die Business Improvement Company das „BSI Kitemark for IoT Devices“[9] und die Internet of Secure Things (ioXt)-Allianz die „ioXt Authorized Lab Certification“[10], wenn bestimmte Sicherheitsstandards eingehalten und Penetrationstests bestanden werden. Des Weiteren bieten Singapur und die ioXt-Allianz abgestufte Gütesiegel an, je nachdem, ob IoT-Geräte lediglich im Rahmen einer Selbstverpflichtung der Hersteller zertifiziert oder unabhängig und mittels Penetrationstests geprüft wurden. Von öffentlicher Seite existieren beispielsweise in Deutschland und in Finnland ebenfalls Zertifizierungsprogramme, die grundsätzlich auch für die Zertifizierung von IoT-Produkten herangezogen werden können.[11,12]

Die unterschiedlichen Zertifizierungen haben gemeinsam, dass sie Verbraucherinnen und Verbrauchern Mindeststandards zusichern, beispielsweise bei der Verfügbarkeit von Sicherheitsupdates, der Datenverschlüsselung und der Betriebssicherheit. Umfang und Anwendungsbereich variieren jedoch erheblich. Während viele Zertifizierungen auf freiwilliger Basis arbeiten, ist beispielsweise in Indien eine Zertifizierung verpflichtend. Inwieweit Hersteller Anreize haben, freiwillige Zertifizierungen zu durchlaufen, ist unklar.[13]

Das binäre IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird wiederum ohne gesonderte Prüfung auf Antrag der Anbieter verliehen, wenn

5 Mozilla Foundation, „Privacy Not Included“. https://foundation.mozilla.org/en/privacynotincluded/.

6 Vergl. ErwGr. 32 CRA. Voigt/Falk, Der Cyber Resilience Act, MMR 2023, 88, 89.

7 Skierka-Canton in Hornung/Schallbruch, IT-Sicherheitsrecht § 8 Rn. 114.

8 Shane D. Johnson u. a., „The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay“. In: PLOS One 15.1 (2020).

9 Business Improvement Company, „BSI Kitemark for IoT Devices“. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bs-launches-kitemark-for-internet-of-things-devices/.

10 Internet of Secure Things (ioXt) Alliance, „The Global Standard for IoT Security“. https://www.ioxtalliance.org.

11 Bundesamt für Sicherheit in der Informationstechnik, „IT-Sicherheitskennzeichen“. https://bsi.bund.de/IT-SIK.

12 Finnish Cybersecurity Label, https://tietoturvamerkki.fi/en/

13 Pardis Emami-Naeini u. a., „An Informative Security and Privacy “Nutrition” Label for Internet of Things Devices“. In: IEEE Security & Privacy, 2022.

sich diese zur Einhaltung der Vorgaben – meist die entsprechende Technische Richtlinie des BSI – selbst verpflichten. Das Siegel wird erst dann widerrufen, wenn das BSI von einer Nichteinhaltung Kenntnis erhält.

Die Datenschutzfreundlichkeit von IoT-Geräten wird von den oben genannten Zertifizierungsprogrammen im Allgemeinen bisher allenfalls in Teilen und nur indirekt abgedeckt. Im Prinzip könnte künftig die Verarbeitung personenbezogener Daten im IoT-Bereich Gegenstand einer Zertifizierung nach Art. 42 Datenschutz-Grundverordnung sein, sofern dafür geeignete Konformitätsbewertungsprogramme samt Kriterienkatalogen zur Verfügung stehen.

Ohnehin sind die Effekte von binären und abgestuften Siegeln auf Nutzende bisher kaum erforscht. Zwar belegen Forschungsarbeiten, dass Siegel auf Kaufentscheidungen im Bereich des IoT einen positiven Effekt haben. Dieser Effekt tritt jedoch demnach insbesondere bei informativen Kennzeichnungen auf, die detailliertere Angaben zur Informationssicherheit bereitstellen.[14] Die Risikoeinschätzung und die Kaufentscheidung hängen von vielen verschiedenen Eigenschaften der IoT-Geräte ab, die nur durch informative Kennzeichnungen vermittelt werden können.[15]

Wie lassen sich quantifizierte Bewertungen von Informationssicherheit und Datenschutz darstellen? In der Forschung wurden bereits zahlreiche Ansätze für informative Kennzeichnungen vorgeschlagen[16,17,18,19,20,21], die Verbraucherinnen und Verbraucher vor und/oder nach dem Kauf über wesentliche Eckpunkte der Datenverarbeitung informieren (siehe Abb. 1).

In einigen Fällen werden die mitgelieferten Kennzeichnungen durch Online-Werkzeuge ergänzt, um zusätzliche und aktualisierte Details zur Verarbeitung bereitzustellen und den Vergleich verschiedener Geräte zu ermöglichen.[22,23]

Erste Untersuchungen mit Nutzenden zeigen, dass solche Lösungen auch Laien effektiv und in verständlicher Weise über bestimmte datenschutzrelevante Eigenschaften informieren können. Fraglich ist jedoch, inwieweit Nutzende Kennzeichnungen, die Hersteller im Rahmen einer Selbstverpflichtung aufbringen könnten, vertrauen würden. Hier legen Studien nahe, dass sie Herstellerangaben im Allgemeinen wenig Vertrauen schenken.[24] Jüngste Untersuchungen zeigten außerdem, dass z. B. die von Apple eingeführten „Privacy Labels" sowie die von Google Play verwendeten „Data Safety Labels" gar nicht diejenigen Kriterien abdecken, die eigentlich notwendig wären, um Antworten auf die von App-Nutzenden

Abb. 1 | Beispiel einer „Privacy facts"- Kennzeichnung für IoT-Geräte

häufig gestellte Fragen zur Privatheit zu geben.[25]

Unklar ist auch, ob datenschutzbezogene Informationen das Kaufverhalten oder Schutzverhalten in ähnlicher Weise beeinflussen wie Hinweise zur Informationssicherheit.[26] Für einige der vorgeschlagenen Kennzeichnungen fehlen zudem Evaluationen der Gebrauchstauglichkeit,[27,28] sodass die Kennzeichnungen nicht abschließend validiert sind. Zudem wurden nur zwei der in diesen Publikationen aufgeführten Kennzeichnungen basierend auf den Anforderungen der DSGVO entwickelt.[29,30]

2.3 Leitfäden und Richtlinien

Neben Vorschlägen für Siegel und Kennzeichen existieren heutzutage auch zahlreiche Leitfäden und Richtlinien für die Entwicklung eines sicheren und datenschutzfreundlichen IoT. Im März 2022 zählte die IoT Security Foundation 61 Leitfäden und Richtlinien weltweit. Diese werden sowohl von der Industrie als auch von (halb)öffentlichen Stellen, wie beispielsweise NIST und ENISA, bereitgestellt.[31] Darüber hinaus hat die Forschung vorgeschlagen, Kriterien zu bestimmen, wie und welche Informationen den IoT-Nutzenden transparent gemacht werden sollten.[32] Diese Leitfäden richten sich primär an Hersteller und Personen in Ingenieurstätigkeiten und setzen technisches Verständnis voraus.

Mit dem vollständigen Wirksamwerden der Regelungen des CRA im Dezember 2027 müssen Hersteller für ihre Produkte mit digitalen Elementen – also auch IoT-Produkte – eine ausführliche technische Dokumentation erstellen, die sie für Kontrollbehörden bereithalten müssen, und den Nutzenden für sie verständliche Informationen und Anleitungen zum Einsatz an die Hand geben (siehe Abschnitt 5.1).[33] Künftig wird sich damit die Informationslage zu IoT-Geräten deutlich verbessern.

14 Shane D. Johnson u. a., oben Fn. 8

15 Pardis Emami-Naeini u. a., „Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?". In: IEEE Security & Privacy, 2021.

16 Pardis Emami-Naeini u. a., oben Fn. 13.

17 Grace Fox u. a., „Communicating Compliance: Developing a GDPR Privacy Label". In: AMCIS, 2018.

18 Philipp Morgner u. a., „Security update labels: establishing economic incentives for security patching of IoT consumer products". In: IEEE Security & Privacy, 2020.

19 Alexandr Railean/Delphine Reinhardt, „Let There Be LITE: Design and Evaluation of a Label for IoT Transparency Enhancement". In: MobileHCI, ACM, 2018.

20 Yun Shen/Pierre-Antoine Vervier, „IoT Security and Privacy Labels". In: APF, Springer, 2019.

21 Rob van Dierman, „The Internet of Things: A Privacy Label for IoT Products in a Consumer Market", 2018.

22 Pardis Emami-Naeini u. a., oben Fn. 13.

23 Alexandr Railean/Delphine Reinhardt, „OnLITE: Online Label for IoT Transparency Enhancement". In: NordSec, Springer, 2021.

24 Pardis Emami-Naeini u. a., oben Fn. 16.

25 Shikun Zhang/Norman Sadeh, „Do Privacy Labels Answer Users' Privacy Questions?". In: USEC, 2023.

26 Philipp Morgner u. a., oben Fn. 19.

27 Yun Shen/Pierre-Antoine Vervier, oben Fn. 21.

28 Rob van Dierman, oben Fn. 22.

29 Grace Fox u. a., oben Fn. 18.

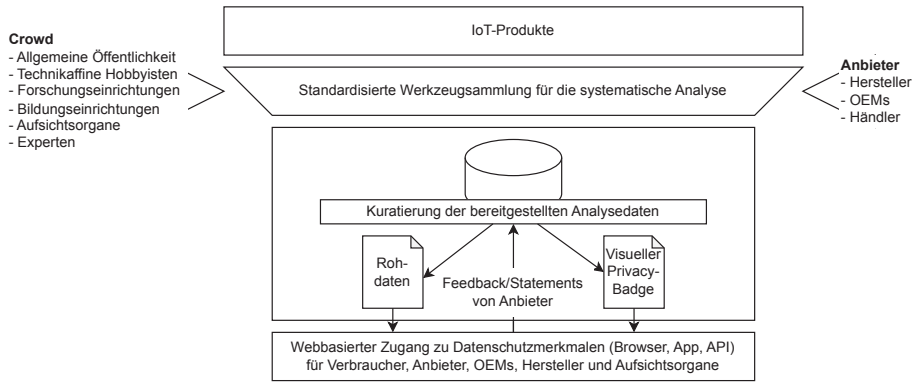
30 Alexandr Railean/Delphine Reinhardt, oben Fn. 20.

31 IoT Security Foundation, „IoT Security Resources". https://www.iotsecurityfoundation.org/iot-security-resources/

32 Pardis Emami-Naeini u. a., „Specification for CMU IoT Security and Privacy Label", CISPL 1.0, 2021.

33 Marit Hansen, „Dokumentation als Normalfall? Cyberresilienz-Verordnung und KI-Verordnung helfen bei der Rechenschaftspflicht", DuD 2025, im Erscheinen.

Abb. 2 | Tool-gestützte, moderierte und nutzendenzentrierte Community-Plattform von vergleichbaren IoT-Privatheitseigenschaften



3 Moderierte Community-Plattform

Um diesen Herausforderungen zu begegnen, wird zurzeit im Forschungsprojekt „*Unboxing.IoT.Privacy*“ eine toolgestützte, moderierte und nutzendenzentrierte Community-Plattform zur Privacy-Einstufung von IoT-Geräten als Grundlage für ein verbessertes Informationsverfahren entwickelt und evaluiert. Die Plattform wird es IoT-Nutzenden sowie Interessierten ermöglichen, sich über die Datenverarbeitung zu informieren. Um die hohe Dynamik und Vielfältigkeit des IoT beherrschbar zu machen, setzt das Projekt auf den bereits in anderen Bereichen erprobten Einsatz der „*Power of the Crowd*“. Ziel ist es, die Bereitschaft und technischen Kompetenzen vieler zu bündeln, um Transparenz über die Datenverarbeitungspraktiken von IoT-Geräten und der zugehörigen Infrastruktur (Gateways, Apps, Cloud-Server) für die breite Öffentlichkeit zu schaffen. Um das Missbrauchsrisiko, z. B. durch Manipulationsversuche, bei einem solchen offenen Bewertungssystem einzudämmen, wird ein Kontrollmechanismus implementiert, der eine moderierte, transparente und nachvollziehbare Konsensbildung auf Grundlage der bereitgestellten Testwerkzeuge und der standardisierten Analyseprotokolle ermöglicht. Dieser Mechanismus schließt die Hersteller aktiv ein und bietet zusätzliche Möglichkeit für Feedback und Stellungnahmen.

Die moderierte Plattform, die zurzeit entwickelt wird, soll der interessierten Community durch verständliche Metriken, nachvollziehbare Verfahren und nutzendenzentrierte Werkzeuge ermöglichen, Privacy-Tests und darauf basierende Privacy-Einstufungen für IoT-Produkte durchzuführen (siehe Abb. 2). Zur Bündelung der Beiträge aus der Community werden standardisierte Testverfahren, strukturierte Dokumentationsvorlagen und bereitgestellte Testwerkzeuge für die Privacy-Einstufung von IoT-Produkten genutzt. Mit diesem Ansatz möchte das Projekt langwierige Zertifizierungen durch aktuelle, standardisierte und transparente Informationen zu Privatheitseigenschaften ergänzen, die zur Auswahl und Beschaffung geeigneter IoT-Produkte hilfreich sind, und zusätzlich Verantwortliche in ihrer Rechenschaftspflicht unterstützen.

4 Privatheitseigenschaften

Um die vielfältigen IoT-Produkte über eine Community-Plattform zu untersuchen und miteinander vergleichen zu können, werden möglichst generalisierbare Privatheitseigenschaften benötigt. Diese Eigenschaften ergeben sich einerseits aus rechtlichen Rahmenbedingungen, wie beispielsweise Transparenzpflichten von Verantwortlichen, und andererseits aus Anforderungen vonseiten der Nutzenden. Im Projekt *Unboxing. IoT.Privacy* wurde ein Katalog von 52 relevanten Privatheitseigenschaften auf strukturierte Weise (systematische Literaturanalyse, Expert*innen-Walkthroughs, iterative Feedbackschleifen) zusammengestellt und zu messbaren Kriterien für die Anwendung auf IoT-Geräte weiterentwickelt.

Dieser Katalog an Privatheitseigenschaften umfasst sowohl offensichtliche Transparenzinformationen und Kontrollfunktionen, wie Angaben über verarbeitete Datenkategorien und Empfänger dieser Daten, als auch Möglichkeiten, die Verarbeitung der Daten zu steuern, indem beispielsweise über einzelne Empfänger oder Datenkategorien entschieden werden kann. Auch die Gebrauchstauglichkeit der angebotenen Datenschutzinformationen und -funktionen wird untersucht, beispielsweise die Zugänglichkeit von Datenschutzinformationen während der Inbetriebnahme und Nutzung des IoT-Geräts oder angebotene Prozesse zur Umsetzung der Betroffenenrechte oder. Weitere Eigenschaften beschreiben technische Details, wie die eingesetzten Verfahren zur Transportverschlüsselung von Daten, sowie verfügbare Ressourcen zur Unterstützung jener Nutzenden, die durch den Betrieb eines IoT-Geräts selbst zu Verantwortlichen mit entsprechenden Auskunftspflichten werden.

5 Informationsquellen

Die Informationsquellen können vielfältig sein. Besonders relevant sind aber sicherlich die bereitgestellten Informationen des Herstellers des IoT-Geräts sowie die Daten, die durch den Einsatz spezifischer Tools hervorgehen.

5.1 Hersteller-Informationen

Offensichtlich sollte der Hersteller über die Informationen verfügen, wie die Verarbeitung von (personenbezogenen) Daten in den IoT-Geräten und bei ihrer Einbindung in eine Infrastruktur erfolgt. Ein Teil der Information kann über Datenschutzerklärungen oder „Beipackzettel“ zur Verfügung gestellt werden. Hierbei ist zu berücksichtigen, dass die DSGVO den Hersteller nicht unmittelbar mit Transparenzpflichten belegt (soweit er nicht selbst durch eine eigene Verarbeitung personenbezogener Daten zusätzlich zum Verantwortlichen oder Auftragsverarbeiter wird). Auf dieser Basis bliebe die Bereitstellung von vielen privatheitsrelevanten Informationen freiwillig. Allerdings können die Datenverordnung und die Cyberresilienz-Verordnung Änderungen bringen:

Mit der Daten-Verordnung (engl. Data Act, DA) erließ der EU-Gesetzgeber im Dezember 2023 Regelungen zum Ziel einer besseren und breiteren Verfügbarkeit von Daten u. a. aus IoT-Geräten. Namentlich die IoT-Nutzenden selbst sollten Zugriff auf die

von ihren Geräten generierten Daten erhalten und diese weitergeben können. Zudem müssen ab September 2025 Geräte-Hersteller und Anbieter verbundener Dienste die Nutzenden über Art und Umfang der anfallenden Daten informieren müssen, wie diese bereitgestellt und ggf. in Echtzeit abgerufen werden können (Art. 50 DA).[34]

Jenseits der Informationspflichten kann der Anspruch auf Datenbereitstellung zur Analyse von IoT-Geräten dienen. Nutzende können nämlich nach Art. 5 DA diese an eine dritte Person als Empfänger bereitstellen lassen. Im Prinzip könnte dieser Empfänger auch ein Forschungsprojekt sein, für das Nutzende ihre Daten freigeben. Davon könnten die Beobachtung und Evaluation von IoT-Geräten und verbundenen Diensten profitierten, indem die bereitgestellten Daten von mehreren Quellen verglichen und die Bereitstellungsgeschwindigkeit, Unverfälschtheit, Vollständigkeit verifiziert werden kann. Die Geräte müssten dafür nicht einmal bei den Forschenden selbst vorliegen.

Der CRA adressiert für die den europäischen Markt die Cybersicherheit von „Produkten mit digitalen Elementen", was namentlich IoT-Geräte umfasst. Nach dem CRA muss der Hersteller bestimmte Informationen wie Nutzungsanleitungen und eine ausführliche technische Dokumentation erarbeiten. Speziell für Nutzende müssen Hersteller bestimmte Informationen gemäß Anhang II des CRA zur Verfügung stellen. Neben einer ausführlichen Anleitung von der ersten Inbetriebnahme bis zur sicheren Außerbetriebnahme gehören dazu auch die Zweckbestimmung des Produkts, der Support-Zeitraum und eine zentrale Kontaktstelle für Schwachstellen.

In der technischen Dokumentation muss der Hersteller auf die Sicherheitsbewertung eingehen. Dies wird häufig auch eine Software-Stückliste (Software Bill of Materials, SBOM) umfassen, die für eine Beherrschbarkeit der Risiken über die Supply Chain wichtige Informationen bietet. Die technische Dokumentation muss zwar nicht veröffentlicht werden, jedoch könnten Hersteller, die selbst in einer Plattform authentische Informationen über Privatheitseigenschaften ihrer IoT-Produkte bereitstellen möchten, diese weitgehend aus der technischen Dokumentation ableiten.

5.2 Tools

Tools zur Erhebung von Privatheitseigenschaften von IoT-Geräten können die Informationsgewinnung ergänzen und durch Standardisierung und (Teil-)Automatisierung die Dokumentations- und Transparenzpflichten der Anbietenden sowie der Verantwortlichen unterstützen.[35] Gleichzeitig liefern sie Dritten unabhängig reproduzierbare und nachvollziehbare Daten. Verfügbare Tools lassen sich z. B. nach dem primären Analysegegenstand (IoT-Gerät oder Gateway, Apps oder Cloud-Server der zugehörigen Infrastruktur), dem Automatisierungsgrad und der Eigenschaft einer Quelloffenheit klassifizieren. Einige Tools konzentrieren sich auf den Netzverkehr (z. B. mitmproxy, Wireshark), um aus der Kommunikation Inhalte und Metadaten wie z. B. Kommunikationsendpunkte zu extrahieren. Andere Tools wiederum sind auf die Untersuchung der Firmware spezialisiert (z. B. IDA Pro, Ghidra, Binwalk), um Schwachstellen in der Software auf dem Gerät zu finden. Tools zur Überprüfung von Datenschutzerklärungen (z. B. Polisis) hingegen führen textanalytische – teils auch unter Verwendung von KI-Verfahren – Bewertungen durch, um aus Festlegungen in einer Datenschutzerklärung semantisch strukturierte Daten zu machen, die dann ihrerseits automatisierbar mit z. B. individuellen Privatheitspräferenzen abgeglichen werden können.

Bisherige Tools konzentrieren sich zumeist auf Sicherheits- und nicht auf Privatheitseigenschaften. Einige der sicherheitsrelevanten Analysen sind auch für Privacy-Einstufungen relevant und können daher verwendet werden. Für fehlende Privatheitsaspekte müssen hingegen noch spezialisierte Tools entwickelt werden. Insgesamt ist die Ausgestaltung der Tools bisher maßgeblich für Expertinnen und Experten ausgelegt, was einer breiten Verwendung entgegensteht. Eine nutzendenzentrierte Ausgestaltung der Tools ist ein Kernziel des Projekts. Zudem liegen die Analyseergebnisse, die heutige Tools erzeugen, weder in einer abgestimmten Struktur noch in einem standardisierten Format vor, was das Zusammenführen der Ergebnisse erschwert. So ist z. B. der Abgleich von URLs, die in einer Firmware-Analyse aufgefunden wurden, mit URLs aus einer Analyse der Datenschutzerklärung oder einer Protokollierung des Netzverkehrs nicht ohne Weiteres automatisiert möglich, da diese aufgrund fehlender Standardisierung in der Regel undefiniert in den Ergebnisprotokollen enthalten sind. Schließlich sind verfügbare Tools meist auf bestimmte, sehr spezialisierte Nutzendengruppen fokussiert, wie z. B. Systementwickelnde, und lassen sich kaum von Personen mit weniger spezifischen Kenntnissen und Fähigkeiten verwenden.

6 Nutzendenzentrierte Darstellung

Nicht nur die Inhalte, sondern auch deren visuelle Darstellung können das Verständnis, das Vertrauen sowie die Entscheidungen der Nutzenden der Plattform unterstützen. Die Art und Weise der Darstellung spielt eine wichtige Rolle bei der Akzeptanz der Plattform durch die Nutzenden. Hier ist es sinnvoll, verschiedene Gruppen– von Laien bis zu Expert*innen – in der Entwicklung der graphischen Darstellung der für sie relevanten Privatheitseigenschaften einzubeziehen. Dabei muss das Wichtigste auf den ersten Blick ersichtlich und gleichermaßen kompakt und ausreichend verständlich sein. Abb. 3 und 4 zeigen erste Entwürfe für Screens, die im Rahmen von *Unboxing.IoT.Privacy* partizipativ entworfen wurden und im Projekt evaluiert werden.

Zu berücksichtigen ist insbesondere auch, dass die Nutzenden nicht nur über die Risiken für ihre eigene Privatheit informiert werden, sondern auch in ihrer Rolle als Verantwortliche Erläuterungen dazu erhalten, was die Privatheit von Personen in ihrem Umfeld betrifft. Dabei werden leichtverständliche textuelle Formulierungen und selbsterklärende graphische Elemente zu entwickeln sein.

Auch rechtliche Aspekte müssen beachtet werden: Eine Bewertung ist insoweit rechtlich herausfordernd, als dass Tatsachen und Testergebnisse korrekt und jegliche Werturteile, insbesondere Abwertungen, einer soliden Begründung bedürfen. Dagegen ist es im Allgemeinen unproblematisch, vom Hersteller bereitgestellte – und als solche gekennzeichnete – Informationen mit Quellenangabe wiederzugeben. Sofern Informationen fehlen, die hilfreich oder nötig für die Privacy-Einstufung sind, kann auf diesen Umstand hingewiesen werden.

34 Zum Spannungsfeld für den Dateninhaber zwischen den beiderseits sanktionsbewehrten Pflichten zur Bereitstellung von Daten und zum Schutz personenbezogener Daten vergl. Baumann/Brunner, ZD 2025, 132; Richter, MMR 2025, 163, 165.

35 Weitere Tools siehe auch unter https://iot-privacy.info/tools

7 Diskussion

Im Projekt *Unboxing.IoT.Privacy* wird nicht nur die skizzierte Plattform entwickelt, sondern in diesem Zusammenhang insbesondere zu den folgenden Fragen geforscht:

- Wie können IoT-Nutzende für sich selbst und als datenschutzrechtlich Verantwortliche für Drittbetroffene rechtskonform und nutzungsfreundlich informiert und in deren Entscheidung unterstützt werden, um ihre Souveränität bei dem Umgang mit IoT-Geräten zu erhöhen?
- Welchen Einfluss hat eine derartige Plattform im Sinne von *Unboxing.IoT.Privacy* auf Verbraucherinnen und Verbraucher hinsichtlich datenschutzrelevanten Verhaltens? Wie lassen sich die Bewertungskriterien ausgestalten, um den größtmöglichen Nutzen für die Nutzenden zu erzielen?
- Wie können die IoT-Geräte systematisch und regelmäßig durch die Crowd analysiert werden? Inwieweit ginge dies ohne besonderes Expertenwissen?
- Wie kann die Zuverlässigkeit der resultierenden Ergebnisse der Datenschutzanalyse gewährleistet werden?
- Welche Privatheitseigenschaften sind wichtig bzw. weniger wichtig für die Nutzenden, abhängig von deren Interessen und Anforderungen? Wie wird sich die Geltung von DA und CRA auf die Privacy-Einstufung auswirken?

Die Ergebnisse des Projekts werden unter https://iot-privacy.info/ bereitgestellt.

Abb. 3 | Entwurf mit Fokus auf der Auswahl der Darstellung basierend auf Nutzendenpräferenzen

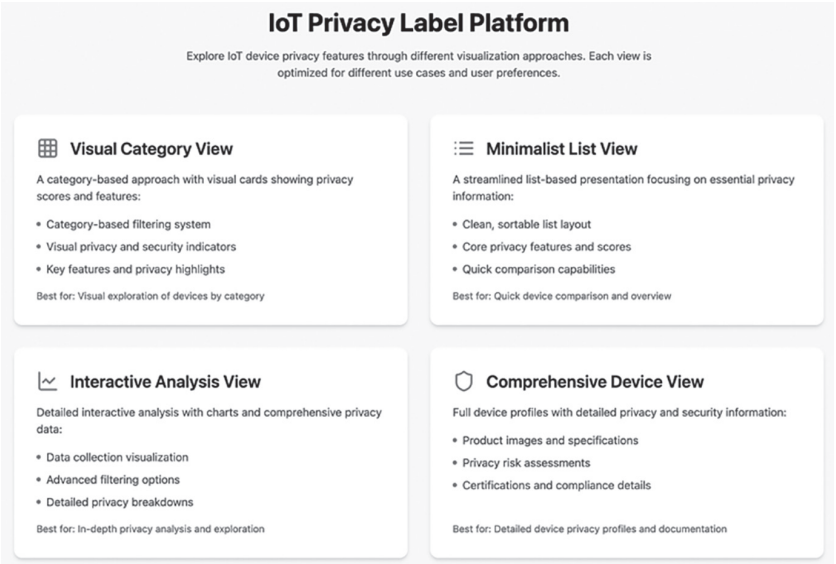
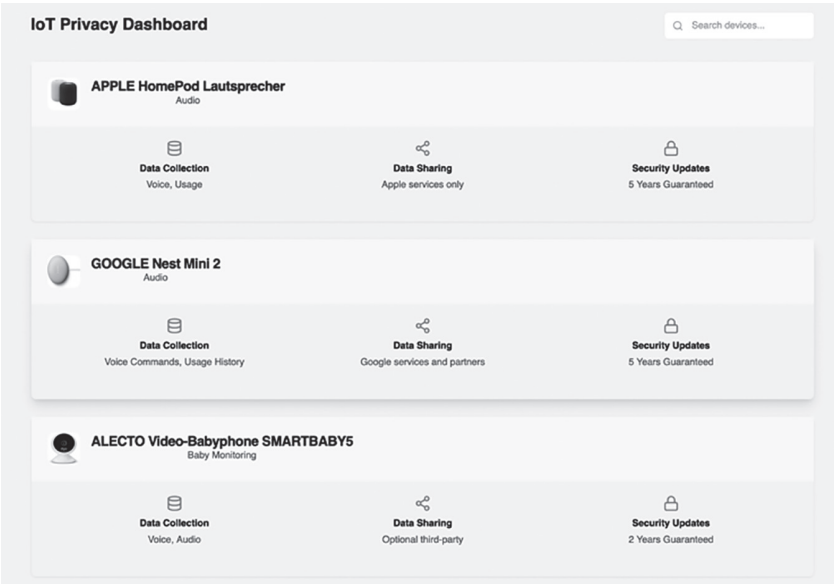


Abb. 4 | Alternativ-Entwurf mit minimalen Informationen als Einstieg und detaillierte Ansicht bei Interesse



8 Fazit und Ausblick

IoT-Produkte bringen Risiken für Sicherheit und Privatheit mit sich. Zurzeit ist es nicht nur für Laien schwierig, ausreichende Informationen zu erhalten, um die für sie relevanten Kriterien für einen sicheren und datenschutzgerechten Einsatz bewerten zu können. Der Ansatz einer moderierten Community-Plattform für eine vergleichbare Transparenz von Privatheitseigenschaften von IoT-Geräten und den zugehörigen Infrastrukturkomponenten, wie er im Projekt *Unboxing.IoT.Privacy* entwickelt wird, bietet Potenzial sowohl für Nutzende als auch für Organisationen als datenschutzrechtliche Verantwortliche, die IoT-Produkte beschaffen und einsetzen wollen. Aufsichtsbehörden für Datenschutz oder Informationssicherheit können ebenso von den vorhandenen Informationen und den Tools profitieren.

Es ist davon auszugehen, dass der CRA sich generell positiv auf die Sicherheit von IoT-Produkten auswirken und die Transparenz über bestimmte damit zusammenhängende Aspekte erhöhen wird. Dies wird die Informationsbeschaffung für die Community-Plattform erleichtern. Allerdings zielt die Plattform auch auf die Transparenz von Privatheitseigenschaften ab, die nicht vom CRA abgedeckt werden. Um Synergien nutzbar zu machen, will die Plattform Impulse geben, damit sich bisher und künftig verfügbare Aussagen zur Cybersicherheit standardisiert auswerten lassen und die zusätzlichen als relevant identifizierten Informationen zu Privatheitseigenschaften verfügbar gemacht werden.

Danksagung

Wir bedanken uns bei Christoph Wegener für die wertvollen Anregungen und Parth Sheta, Priyeshkumar, Chikhaliya, Carolin Lafeld, und Lindrit Kqiku für deren Mitarbeit an den ersten Screen-Entwürfen der Plattform (Abb. 3 und 4).