

Privatheits-relevante Eigenschaften von IoT-Produkten für Verbraucher:innen*

Florian Dehling, Sebastian Koch, Luigi Lo Iacono, Lindrit Kqiku, Delphine Reinhardt und Harald Zwingelberg

Zusammenfassung

Das Internet der Dinge (IoT) hält zunehmend Einzug in private Haushalte und ermöglicht durch Sensorik und Konnektivität weitreichende Datenerhebungen in der privaten Sphäre. Für Verbraucher:innen ist vor dem Kauf jedoch häufig nur schwer nachvollziehbar, welche Daten ein IoT-Produkt – typischerweise bestehend aus Gerät, Begleit-App und Backend-Dienst – verarbeitet, an welche Empfänger Daten übertragen werden und welche Privatheitsrisiken daraus resultieren. Privacy Labels werden als Ansatz diskutiert, diese Informationslücke zu schließen; ihre Aussagekraft ist in der Praxis jedoch oftmals durch unvollständige, unspezifische oder herstellerabhängige Informationen eingeschränkt. Vor diesem Hintergrund identifizieren wir privatheits-relevante Eigenschaften von IoT-Produkten, die sich herstellerunabhängig erheben und vergleichen lassen. Auf Grundlage einer Literaturrecherche zu Privacy- und Security-Labels, relevanten rechtlichen Rahmenwerken sowie Studien zum privatheitsbezogenen Nutzerverhalten und ergänzt durch interdisziplinäre Expertenworkshops entwickeln und kuratieren wir eine Sammlung von 54 Eigenschaften. Die resultierende Merkmalsbasis unterstützt eine nachvollziehbare, unabhängige Beurteilung von IoT-Produkten und liefert eine Grundlage für die Ausgestaltung aussagekräftiger Privacy Labels, die Verbraucherberatung sowie eine regulatorische Einordnung.

* Dieser Beitrag ist im Rahmen des durch das Bundesministerium für Forschung, Bildung, Technologie und Raumfahrt geförderten Verbundprojekts „Unboxing.IoT.Privacy“ entstanden (Förderkennzeichen: 16KIS1931K).

1. Einleitung

Die fortschreitende Digitalisierung dringt zunehmend in zahlreiche Bereiche unseres Alltagslebens ein und etabliert das Internet der Dinge (engl. Internet of Things, IoT) als einen Bestandteil moderner Gesellschaften. IoT-Geräte umfassen unter anderem intelligente Haushaltsgeräte, die durch integrierte Sensoren und erweiterte Konnektivität unsere Lebensqualität verbessern können. Gleichzeitig schaffen diese Geräte jedoch die Möglichkeit für umfassende und potenziell invasive Datenerhebungen innerhalb der privaten Sphäre der eigenen vier Wände (Subahi/Theodorakopoulos 2019). Die gesammelten Daten lassen sich zu detaillierten Profilen verdichten, die tiefgehende Einblicke in die persönlichen Gewohnheiten und Vorlieben der Nutzenden gewähren. Forschungen belegen beispielsweise, dass durch die Analyse von Stromverbrauchsdaten präzise Informationen über die Art und Betriebsmodi von genutzten Haushaltsgeräten extrahiert werden können. Im Fall von Fernsehern lassen sich sogar Rückschlüsse auf die konsumierten Inhalte ziehen (Greveler u. a. 2012; Reinhardt u. a. 2015).

Angesichts der Vielzahl an IoT-Produkten und den zunehmenden Datenmengen, die durch vielfältige Sensoren in privaten Räumen erfasst werden, ist es entscheidend, Datenschutzaspekte vor dem Erwerb zu berücksichtigen, um das Grundrecht auf informationelle Selbstbestimmung fundiert ausüben zu können. Für Verbraucher:innen gestaltet es sich häufig herausfordernd, die Datenverarbeitungsprozesse, die mit IoT-Geräten verbunden sind, vor dem Kauf zu durchschauen und potenzielle Datenschutzrisiken zu identifizieren. Im Gegensatz zur Nutzung von Apps oder Onlinediensten besteht für IoT-Anbieter keine unmittelbare Verpflichtung, die Verbraucher:innen vor dem Kauf über die spezifische Datenverarbeitung zu informieren. Ein wesentlicher Grund hierfür ist u. a., dass die Art der Datenverarbeitung bei einigen IoT-Gerätekategorien erst durch die tatsächliche Nutzung bestimmt wird. Somit ergibt sich der Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) erst im konkreten Nutzungskontext. Eine Überwachungskamera kann z. B. in sehr unterschiedlichen Anwendungsfällen betrieben werden. Wird sie ohne Anbindung an eine vom Hersteller bereitgestellte Cloud ausschließlich zur Überwachung des eigenen schlafenden Babys verwendet, fällt eine solche IoT-Nutzung oftmals noch unter die Haushaltsausnahme (Art. 2 Abs. 2 lit. c DSGVO) und damit aus dem Anwendungsbereich der DSGVO (Fuhrken 2026). Wird die Kamera indes mit einem Clouddienst des Herstellers verbunden, greifen die Bestimmungen der DSGVO. Wenn der Betrieb Einfluss auf die Privatheit von

Dritten nimmt, die sich beispielsweise als Besuchende im Aufnahmebereich aufhalten (Saqib u. a. 2025), können sich aus der DSGVO Pflichten für den Betreiber ergeben, unabhängig davon, ob die Kamera mit einer Cloud verbunden ist oder nicht.

Um die Informationslücke hinsichtlich der Privatheitseigenschaften von IoT-Geräten zu schließen, empfehlen Forschende den Einsatz von Privacy Labels (Emami-Naeini u. a. 2022; Shen/Vervier 2019). Diese Labels sollten bereits vor dem Kauf eines IoT-Produkts wichtige Informationen zielgruppenspezifisch bereitstellen. Als besonders nützlich für Verbraucher:innen haben sich Privacy Labels erwiesen, die spezifische Beschreibungen privatheits-relevanter Merkmale bieten, anstatt auf Bewertungsskalen oder binäre Siegel zu setzen (Johnson u. a. 2020). Solche Labels informieren beispielsweise über die im IoT-Produkt integrierten Sensoren, die Verarbeitung personenbezogener Daten und die potenzielle Weitergabe dieser Daten an Dritte (Railean/Reinhardt 2021).

Die Datenquellen für Privacy Labels können entweder bestehende Datenschutzerklärungen oder vom Hersteller bereitgestellte Informationen sein (Johnson u. a. 2020). Da Datenschutzerklärungen bei IoT-Produkten teils unvollständig sind, insbesondere wenn es um verkettbare, aber nicht eindeutig personenbezogene Daten geht, hängt die Zuverlässigkeit von Privacy Labels, die auf Herstellerinformationen basieren, stark von der Transparenzbereitschaft der Hersteller ab. Um unabhängigen Prüfstellen oder technikaffinen Einzelpersonen die Möglichkeit zu geben, die Privatheitsaspekte eines IoT-Produkts unabhängig zu untersuchen, müssen Eigenschaften identifiziert werden, die auch ohne aktive Unterstützung der Hersteller überprüfbar sind.

Basierend auf einer Literaturrecherche mit Fokus auf Privacy- und Security-Labels, rechtliche Rahmenwerke sowie Studien zu privatheits-relevantem Nutzerverhalten wurde eine initiale Sammlung für Verbraucher:innen relevanter Privatheits-Eigenschaften erarbeitet. Diese wurde anschließend durch interdisziplinären Expertenkonsens geprüft, sortiert und verfeinert. Die Expertengruppe umfasste zwei Universitätsprofessoren, einen Postdoktoranden, zwei Doktoranden im Bereich menschenzentrierte IT-Sicherheit und Datenschutz, einen Vertreter aus der Industrie sowie einen Rechtspraktiker. Die Kuratierung erfolgte im Rahmen eines initialen Workshops mit anschließenden mehrfachen Online-Diskussionsrunden und wurde fortgeführt, bis eine konzeptuelle Sättigung erreicht war, das heißt, keine neuen Kandidateneigenschaften mehr aufkamen und verbleibende Meinungsverschiedenheiten im Konsens gelöst werden konnten.

Für die Aufnahme in die finale Sammlung musste eine Eigenschaft drei Einschlusskriterien erfüllen: Sie musste (a) einem IoT-Produkt oder seinem zugehörigen Dienst zuordenbar sein, (b) operationalisiert werden können, um verbraucherorientierte Kaufentscheidungen zu unterstützen, und (c) hinreichend spezifisch sein, um grundsätzlich bewertet oder überprüft werden zu können. Ausgeschlossen wurden Kandidaten, die primär Richtlinien für die Gestaltung von Benutzeroberflächen oder Labels beschrieben (z. B. Formulierungen, barrierefreie Farbgebung), plattform- oder werkzeutechnische Anforderungen betrafen (z. B. Installationsaufwand, plattformübergreifende Bereitstellung) oder nicht hinreichend klar formuliert waren.

Daraus resultierte eine Sammlung von 54 für Verbraucher:innen relevanten Privatheits-Eigenschaften samt zugehöriger Metriken, die eine herstellerunabhängige Prüfung und Bewertung von IoT-Geräten ermöglicht. Dabei werden sowohl technische Fakten als auch die Gebrauchstauglichkeit verfügbarer Datenschutz- und Transparenzfunktionen berücksichtigt.

2. Anatomie eines IoT-Produktes

Ein IoT-Produkt lässt sich zunächst als ein vernetztes Gerät verstehen, das in vielfältigen Ausprägungen existieren kann. Charakteristisch ist, dass ein solches IoT-Gerät häufig nicht isoliert betrieben wird, sondern typischerweise durch eine begleitende Smartphone-App ergänzt wird. Diese Begleit-App dient dazu, das Gerät zu steuern, Konfigurationen vorzunehmen oder Sensordaten auszulesen und in einer für Nutzer:innen zugänglichen Form darzustellen. Bereits an dieser Stelle zeigt sich, dass die Datenverarbeitung häufig nicht nur durch das IoT-Gerät selbst stattfindet, sondern auch auf mit ihm vernetzten Geräten wie beispielsweise Smartphones.

Im Betrieb kommunizieren IoT-Gerät und/oder begleitende App in vielen Fällen mit einem oder mehreren Backend-Diensten im Internet. Diese Backend-Dienste sind für den Betrieb des Produkts teilweise essenziell und können unterschiedliche Aufgaben übernehmen, etwa die Vermittlung von Steuerbefehlen, die Speicherung von Daten oder die Bereitstellung weiterer Funktionalitäten. Dabei ist zu berücksichtigen, dass solche Kommunikationsbeziehungen für Außenstehende beziehungsweise Nutzer:innen häufig nicht transparent sind. Insbesondere bleiben Kommunikationsverbindungen und die beteiligten Dienste oft intransparent, obwohl sie für die datenschutzrechtliche und privatheitsbezogene Bewertung des Gesamtsystems maßgeblich sind.

3. Privatheits-relevante Eigenschaften und ihre Kategorien

Privatheits-relevante Eigenschaften von IoT-Produkten sind ähnlich vielfältig wie die Produkte selbst. Sie hängen unter anderem von der Existenz bestimmter Funktionen, deren technischer Implementierung sowie der Ausgestaltung privatheitsbezogener Transparenz- und Kontrollmechanismen ab. Die in diesem Beitrag verwendete Kategorisierung wurde induktiv aus einer durch Literaturrecherche und Expertenworkshops generierten Liste potenzieller Eigenschaften abgeleitet. Im Folgenden werden die Kategorien und zugehörigen Eigenschaften vorgestellt, die im Hinblick auf eine herstellerunabhängige Überprüfbarkeit ausgewählt und entsprechend gefiltert wurden.

3.1 Funktionsumfang

Der Funktionsumfang umfasst technische Funktionen eines Produktes, die einen Einfluss auf die Privatheit haben können (s. Tab. 1). Privatheitsrelevanz ergibt sich hierbei nicht nur aus der Art der bereitgestellten Funktion, sondern auch aus den Voraussetzungen, unter denen diese Funktion genutzt werden kann. Beispielsweise kann zur Nutzung ein Account bei einem Online-Dienst erforderlich sein. Ebenso kann eine begleitende App Zugriffsberechtigungen benötigen, die ihrerseits datenschutzrelevant sind, weil sie Zugriff auf gerätespezifische oder personenbezogene Daten eröffnen.

Weiterhin kann das IoT-Produkt eine Benutzerverwaltung ermöglichen, wodurch sich Möglichkeiten der Abgrenzung verschiedener Nutzer:innen ergeben. Auch die Erforderlichkeit von Backend-Diensten für den Betrieb ist ein zentraler Bestandteil des Funktionsumfangs, weil damit ein kontinuierlicher Datenaustausch mit externen Systemen verbunden sein kann. Schließlich ist auch relevant, wenn das Produkt im Betrieb das lokale Netzwerk durchsucht, da dadurch Informationen über das Umfeld, andere Geräte oder Netzwerkstrukturen verarbeitet werden können.

Tabelle : Privatheits-relevante Eigenschaften aus der Kategorie *Funktion*.

Name der Eigenschaft	Beschreibung	Quelle
Konto für Geräte-Inbetriebnahme erforderlich ^{D,B}	Ob für den Betrieb ein Konto bei einer Online-Plattform erforderlich ist.	(Hudig u. a. 2023)
Erforderliche App-Berechtigungen ^{D,Q}	Welche Zugriffsberechtigungen die Begleit-App benötigt.	(Zhang/Sadeh 2023)
Zugriffskontrolle für Nutzende ^B	Ob es möglich ist, mehrere Nutzerprofile zu verwalten.	(Norval/Singh 2023)
Erforderlichkeit eines Backend-Dienstes ^B	Ob für den Betrieb ein Backend-Dienst notwendig ist.	(EU 2024; Norval/Singh 2023)
Durchsuchen des lokalen Netzwerks ^B	Ob das Gerät das lokale Netzwerk scannt.	(Norval/Singh 2023)
Open-Source-Basis ^B	Ob das Gerät auf Open-Source-Software basiert.	(EU 2024)
Datenverarbeitung auf dem Gerät ^B	Ob die Datenverarbeitung ausschließlich lokal auf dem Gerät stattfinden kann.	(Norval/Singh 2023)
Steuerbare Erkennungsfunktion ^B	Ob die Suche im lokalen Netzwerk deaktiviert werden kann.	(Norval/Singh 2023)

^B Binär, ^D Details, ^Q Quantifizierend (s. Kapitel 5)

Zur Veranschaulichung zeigen zwei Beispiele, wie die genannten Eigenschaften in der Praxis auftreten können: Ein smartes Türschloss, das biometrische Daten wie Fingerabdrücke ausschließlich lokal auf dem Gerät speichert und verarbeitet, erfüllt die Eigenschaft *Datenverarbeitung auf dem Gerät*. Smart Speaker hingegen sind häufig auf eine aktive Internetverbindung angewiesen, da Sprachbefehle an externe Server übertragen und dort verarbeitet werden (Khalesi 2025). Ohne diese Verbindung ist eine Nutzung des Geräts nicht möglich, was die Relevanz der Eigenschaft *Erforderlichkeit eines Backend-Dienstes* verdeutlicht.

3.2 Datensicherheit und technische Schutzmaßnahmen

Neben dem Funktionsumfang sind Datensicherheit und technische Schutzmaßnahmen als eigenständige Kategorie zu betrachten (s. Tab. 2). Hierzu zählen technische Maßnahmen zum Schutz der Privatheit, etwa sichere und privatheitsfreundliche Grundeinstellungen, die bereits bei der Inbetriebnahme wirksam werden. Zudem sind Funktionen zum Zurücksetzen

der Einstellungen relevant, weil sie eine Wiederherstellung sicherer Zustände oder eine kontrollierte Übergabe des Geräts ermöglichen können.

Ebenso gehören mögliche Authentifizierungsmethoden in diese Kategorie, da sie darüber entscheiden, wie zuverlässig unautorisierte Zugriffe verhindert werden können. Verschlüsselte Kommunikation stellt einen weiteren Kernaspekt dar, weil sie Schutz vor dem Mitlesen oder Manipulieren von Datenübertragungen bietet. Schließlich spielt die Bereitstellung von Updates eine wichtige Rolle: Updates sind Bestandteil technischer Schutzmechanismen, da sie Sicherheitslücken schließen und technische Mindestanforderungen an die Sicherheit eines vernetzten Produkts unterstützen können.

Tabelle 2: *Privatheits-relevante Eigenschaften aus der Kategorie Datensicherheit und technische Schutzmaßnahmen*

Name der Eigenschaft	Beschreibung	Quelle
Sichere und datenschutzfreundliche Grundeinstellungen ^{D,B,W}	Ob das Gerät mit sicheren und datenschutzfreundlichen Standardeinstellungen ausgeliefert wird.	(EU 2016; EU 2024)
Zurücksetzen auf sichere Grundeinstellungen ^B	Ob das Gerät auf sichere und datenschutzfreundliche Standardeinstellungen zurückgesetzt werden kann.	(EU 2016; EU 2024)
Authentifizierungsmethoden ^D	Welche Authentifizierungsmethoden das Gerät anbietet.	(Chen u. a. 2023)
Verschlüsselte Datenübertragung ^{B,W}	Ob das Gerät Daten über verschlüsselte Verbindungen überträgt.	(Railean/Reinhardt 2021; Chhetri/Motti 2022; Lin u. a. 2023; EU 2024; Li u. a. 2024)
TLS-Zertifikatsvalidierung ^{B,W}	Ob TLS-Zertifikate bei verschlüsselter Übertragung validiert werden.	(EU 2024)
(Sicherheits-)Anzeige des Update-Status ^B	Ob der Status von Sicherheitsupdates angezeigt wird.	(Norval/Singh 2023)
Historie von Datenlecks ^D	Welche Vorfälle von Datenlecks in der Vergangenheit im Zusammenhang mit dem Hersteller aufgetreten sind.	(Emami-Naeini u. a. 2019)
Datenschutzverletzungen ^D	Welche Datenschutzverletzungen in der Vergangenheit im Zusammenhang mit dem Hersteller aufgetreten sind.	(EU 2024; EU 2016)
Verschlüsselungsstatus von Nutzerpasswörtern ^B	Ob das Nutzerpasswort verschlüsselt auf dem Gerät gespeichert wird.	(Zhang/Sadeh 2023)

Name der Eigenschaft	Beschreibung	Quelle
Optionale Sicherheitsprüfung ^{D,B}	Ob es zusätzliche Sicherheitsuntersuchungen für das Gerät gibt.	(Zhang/Sadeh 2023)
Privacy-Enhancing Technologies (PETs) ^D	Welche datenschutzfördernden Technologien eingesetzt werden.	(Hudig u. a. 2023; Bermejo Fernandez u. a. 2021)
Update-Fähigkeit ^{B,W}	Ob das Gerät aktualisiert werden kann.	(EU 2024; Chen u. a. 2023; Railean/Reinhardt 2018; Railean/Reinhardt 2021)

^B Binär, ^D Details, ^W Bewertend (s. Kapitel 5)

Die folgenden Beispiele veranschaulichen die Relevanz dieser Kategorie in der Praxis. Ein Smart-TV, der mit aktivierter ACR-Funktion ausgeliefert wird, verdeutlicht die Eigenschaft *Sichere und datenschutzfreundliche Grundeinstellungen*: ACR erfasst standardmäßig Bildschirmaufnahmen und übermittelt diese an Hersteller und Werbetreibende, ohne dass Nutzende davon in der Regel Kenntnis haben (Anselmi u. a. 2024). Eine smarte Video-Türklingel, die Videostreams unverschlüsselt überträgt, illustriert die Eigenschaften *Verschlüsselte Datenübertragung* und *TLS-Zertifikatsvalidierung*: Ohne Verschlüsselung können Bilddaten im Netzwerkverkehr abgefangen werden, und eine fehlende Zertifikatsvalidierung ermöglicht Man-in-the-Middle-Angriffe (Khetagourova u. a. 2025).

3.3 Transparenz

Transparenz bezieht sich auf Informationen zur Verarbeitung von Daten und umfasst unter anderem typische Transparenzinformationen im Sinne der DSGVO (s. Tab. 3). Dazu zählt nicht nur die Beschreibung, welche Daten verarbeitet werden, sondern auch aggregierte Eigenschaften wie das Teilen von Daten mit Dritten. Eine besondere Rolle spielt zudem die Auflistung verarbeiteter Datentypen, einschließlich der expliziten Benennung nicht-personenbezogener Daten. Diese sind wichtig, weil auch nicht-personenbezogene Daten durch Verkettung mit anderen Daten privatheits-relevant werden können.

Zentral sind außerdem Angaben zu Datenempfängern und zu Zwecken der Datenverarbeitung. Diese Informationen sind notwendig, um Verarbeitungskontexte nachvollziehen zu können und um zu verstehen, welche Akteure in Datenflüsse eingebunden sind.

Tabelle 3: Privatheits-relevante Eigenschaften aus der Kategorie Transparenz

Name der Eigenschaft	Beschreibung	Quelle
Verarbeitete Datentypen ^{D,Q}	Welche Daten beim Betrieb des Geräts verarbeitet werden.	(Zhang/Sadeh 2023)
Auflistung nicht-personenbezogener Daten ^{D,Q}	Welche nicht-personenbezogenen Daten beim Betrieb des Geräts verarbeitet werden.	(Railean/Reinhardt 2021)
Besondere Kategorien personenbezogener Daten ^{D,B,Q}	Welche besonderen Kategorien personenbezogener Daten beim Betrieb des Geräts verarbeitet werden.	(EU 2016; EDPB 2020)
Datenweitergabe ^{B,Q}	Welche Daten mit Dritten geteilt werden.	(Zhang/Sadeh 2023)
Datenempfänger ^{D,Q}	Welche Datenempfänger (Unternehmen, Herkunft) beteiligt sind.	(Zhang/Sadeh 2023)
Datenverarbeitung außerhalb der EU ^B	Ob Daten außerhalb der EU verarbeitet werden.	(EU 2016; Railean/Reinhardt 2021)
Profiling ^{D,B}	Ob Profiling stattfindet.	(EU 2016)
Rechtsgrundlage der Datenverarbeitung ^D	Auf welcher Rechtsgrundlage die Daten verarbeitet werden.	(EU 2016)
Speicherdauer ^D	Wie lange die Daten gespeichert werden.	(EU 2016; Railean/Reinhardt 2018; Railean/Reinhardt 2021)
Beteiligte Akteure in der Verarbeitung ^D	Welche Akteure an der Datenverarbeitung beteiligt sind.	(EU 2016)
Zweck der Datenverarbeitung ^{D,Q}	Zu welchen Zwecken die Daten verarbeitet werden.	(EU 2016; Railean/Reinhardt 2018; Railean/Reinhardt 2021; Cranor u. a. 2024; Chen u. a. 2023)
Datenminimierung ^D	Inhaltlich ähnlich wie „Verarbeitete Datentypen“, ergänzt um den Abgleich mit der Erforderlichkeit (Einordnung, welche Übermittlungen üblicherweise für eine Geräteklasse stattfinden).	(EU 2016; EU 2024)
Häufigkeit der Datenübertragung ^D	Wie oft Daten übertragen werden.	(Railean/Reinhardt 2018; Railean/Reinhardt 2021)
Einhaltung des Cyber Resilience Act ^B	Ob das Gerät die Anforderungen des Cyber Resilience Act erfüllt.	(EU 2024)
Zielort der Datenübertragung ^{D,Q}	Wohin Daten übertragen werden.	(EU 2016; Railean/Reinhardt 2021)

^B Binär, ^D Details, ^Q Quantifizierend (s. Kapitel 5)

Wie relevant die Betrachtung der Eigenschaften *Datenempfänger*, *Datenweitergabe* und *Zweck der Datenverarbeitung* in der Praxis ist, zeigt eine Studie, die für 43 IoT-Produkte DSGVO-Auskunftsanfragen stellte: Nur bei 16 der 43 Produkte wurden überhaupt Informationen zu Drittempfängern bereitgestellt, meist nur in vagen Kategorien wie „Cloud-Dienste“ oder „Werbetreibende“, ohne konkrete Namen oder Standorte der Empfänger zu nennen. Beim Verarbeitungszweck verwendeten die meisten Hersteller Formulierungen wie „zur Verbesserung unserer Dienste“, ohne eine klare Zuordnung zu konkreten Datenkategorien oder Rechtsgrundlagen (Hudig u. a. 2025).

3.4 Kontrolle

Kontrolle umfasst Funktionen, die eine Steuerung oder Begrenzung der Nutzung eigener Daten ermöglichen (s. Tab. 4). Dazu gehören Möglichkeiten, Einfluss auf verarbeitete Datentypen oder Datenempfänger zu nehmen, soweit entsprechende Konfigurationsoptionen vorhanden sind. Weiterhin ist die Implementierung der Betroffenenrechte ein Bestandteil dieser Kategorie, ebenso wie Datenübertragbarkeit. In diesem Zusammenhang ist Kontrolle nicht nur als abstraktes Prinzip zu verstehen, sondern als konkrete Funktionalität, die im Produkt oder in der App implementiert sein kann.

Tabelle 4: Privatheits-relevante Eigenschaften aus der Kategorie Kontrolle

Name der Eigenschaft	Beschreibung	Quelle
Kontrolle des Verarbeitungs-orts ^{D,B}	Ob der Nutzer wählen kann, wo Daten verarbeitet werden.	(Norval/Singh 2023)
Kontrolle der verarbeiteten Daten ^{D,B}	Ob ausgewählt werden kann, welche Daten verarbeitet werden.	(EU 2016)
Kontrolle des Datenempfängers ^{D,B}	Ob ausgewählt werden kann, welche Empfänger Daten erhalten.	(EU 2016)
Umsetzung der Betroffenenrechte ^{D,W}	Ob die Betroffenenrechte umgesetzt wurden.	(EU 2016)
Datenportabilität ^{B,W}	Ob Daten vom Gerät auf andere Geräte übertragen werden können.	(EU 2016)

^B Binär, ^D Details, ^W Bewertend (s. Kapitel 5)

3.5 Usability

Usability adressiert die Gebrauchstauglichkeit privatheits-relevanter Funktionen (s. Tab. 5). Hier stellt sich unter anderem die Frage, ob eine informierte Einwilligung zur Datenverarbeitung ermöglicht wird. Falls andere Rechtsgrundlagen genutzt werden, ist es relevant, ob die Datenverarbeitung klar kommuniziert wird. Ebenfalls entscheidend ist, ob überhaupt eine gebrauchstaugliche Benutzeroberfläche für Privatheitseinstellungen bereitgestellt wird. Damit wird Usability zu einem Faktor, der unmittelbar beeinflusst, ob vorhandene Schutz- oder Kontrollfunktionen praktisch genutzt werden können.

Tabelle 5: Privatheits-relevante Eigenschaften aus der Kategorie Usability

Name der Eigenschaft	Beschreibung	Quelle
Informierte Einwilligung einholen (falls erforderlich) ^{B,W}	Ob eine informierte Einwilligung zur Datenverarbeitung eingeholt wird.	(Bermejo Fernandez u. a. 2021)
Aufklärung über Datenverarbeitungsprozesse ^{B,W}	Ob die Datenverarbeitung klar kommuniziert wird, auch wenn keine Einwilligung notwendig ist.	(Emami-Naeini u. a. 2019)
Benutzeroberfläche zur Datenschutzkontrolle ^B	Ob es datenschutzbezogene Einstellungen gibt.	(Cruz u. a. 2023)
Datenschutzinfo getrennt von AGB ^{B,W}	Ob Datenschutzinformationen und AGB klar voneinander getrennt sind.	(EU 2016)
Klare und transparente Informationen zur Verarbeitung personenbezogener Daten ^B	Ob klare und transparente Informationen zur Verarbeitung personenbezogener Daten bereitgestellt werden.	(Emami-Naeini u. a. 2019)
Visuelle Darstellung von Datenflüssen ^B	Ob eine Visualisierung der Datenflüsse bereitgestellt wird.	(Cruz u. a. 2023)
Unterschiedliche Granularität von Datenschutzeinstellungen in der UI ^B	Ob Datenschutzeinstellungen in unterschiedlichen Detailgraden verfügbar sind.	(Chhetri/Motti 2022)
Explorationsfunktionen ^B	Ob das Gerät das Erkunden von Systeminteraktionen unterstützt (z. B. Kommunikationsliste, Visualisierung von Aktivitäten).	(Norval/Singh 2023)
Untersuchungsfunktionen ^B	Ob das Gerät Funktionen zur Untersuchung bereitstellt (z. B. Fehlerprotokolle).	(Norval/Singh 2023)
Benachrichtigung bei Handlungsbedarf ^B	Ob das Gerät den Nutzer benachrichtigt, wenn Handlungen erforderlich sind.	(Norval/Singh 2023)
Kontextbezogene Datenoffenlegung ^B	Ob das Gerät kontextbezogene Informationen bereitstellt, wenn Daten offengelegt werden.	(Bermejo Fernandez u. a. 2021)

Name der Eigenschaft	Beschreibung	Quelle
Zusätzliche Transparenzmechanismen ^D	Ob das Gerät zusätzliche Transparenzmechanismen bietet.	(Chhetri/Motti 2022)

^B Binär, ^D Details, ^Q Quantifizierend, ^W Bewertend (s. Kapitel 5)

Datenschutzerklärungen für Smart-Home-Geräte sind häufig unvollständig oder lassen unklar, ob sie für ein bestimmtes Gerätemodell, die zugehörige App oder die Herstellerwebsite gelten, was die Relevanz der Eigenschaft *Klare und transparente Informationen* unterstreicht (Manandhar u. a. 2022; Rauti u. a. 2023). Kontextuelle Datenschutzrichtlinien, die relevante Hinweise direkt an der entsprechenden Stelle in der App-Oberfläche einblenden, erzielen hingegen eine deutlich höhere Lesebereitschaft bei Nutzenden und veranschaulichen damit die Bedeutung der Eigenschaft *Kontextbezogene Datenoffenlegung* (Pan u. a. 2024).

3.6 Datenschutz-Support

Datenschutz-Support beschreibt die Unterstützung von Nutzer:innen bei der Erfüllung datenschutzrechtlicher Pflichten (s. Tab. 6). Gerade bei IoT-Geräten ist dies bedeutsam, weil der Besitzer eines IoT-Produktes in die Rolle des für die Datenverarbeitung Verantwortlichen geraten kann. Ein Beispiel ist der Betrieb einer Kamera auf dem eigenen Grundstück, bei dem Gäste gefilmt werden. In solchen Fällen können Eigenschaften wie Compliance-Unterstützung oder Vertragsvorlagen für gemeinsame Verantwortlichkeit relevant sein. Datenschutz-Support zielt somit darauf ab, weniger versierte Nutzer:innen nicht nur technisch, sondern auch in ihrer potenziellen rechtlichen Rolle zu unterstützen.

Tabelle 6: Privatheits-relevante Eigenschaften aus der Kategorie Datenschutz-Support

Name der Eigenschaft	Beschreibung	Quelle
Unterstützung bei Compliance ^{D,B}	Ob der Hersteller Informationen zur Einhaltung von Anforderungen bereitstellt (z. B. Privatsphäre von Unbeteiligten).	(Railean/Reinhardt 2021)
Verfügbarkeit von Vertragsvorlagen für gemeinsame Verantwortliche/Auftragsverarbeiter ^{D,B}	Ob der Hersteller Vertragsvorlagen für eine Konstellation als gemeinsam Verantwortliche bzw. Auftragsverarbeiter bereitstellt.	(EU 2016)

^B Binär, ^D Details (s. Kapitel 5)

Smart-Home-Nutzende können durch die Einschränkung der Haushaltsausnahme unter Umständen selbst zur datenschutzrechtlich verantwortlichen Stelle werden, was die Relevanz der Eigenschaft *Unterstützung bei Compliance* unterstreicht (Urquhart/Chen 2021; Chen u. a. 2020). Die von Herstellern angebotene Unterstützung beschränkt sich dabei häufig auf den Verweis, dass Nutzende selbst für die Einhaltung geltenden Rechts verantwortlich seien, sowie auf die Empfehlung, Unbeteiligte durch physische Hinweisschilder auf die Datenerfassung aufmerksam zu machen (Alshehri u. a. 2022).

4. Analyseverfahren und Messbarkeit

Eine zentrale Herausforderung im Zusammenhang mit privatheits-relevanten Eigenschaften von IoT-Geräten besteht darin, dass Messungen und Analysen auch durch Laien ermöglicht werden müssen. Grundsätzlich lassen sich zwei Ansätze unterscheiden.

4.1 Manuelle Untersuchungen

Ein Ansatz ist die manuelle Untersuchung anhand von Checklisten und Analyseprotokollen. Diese ermöglichen es, Eigenschaften systematisch zu erfassen, die anderweitig nicht zu erheben sind, etwa aus den Kategorien Funktion (z. B. ob ein Benutzerkonto für den Betrieb notwendig ist), Datensicherheit und technische Schutzmaßnahmen (z. B. das Zurücksetzen eines Geräts auf sichere Grundeinstellungen), Datenschutz-Support (z. B. Unterstützung bei Compliance), Usability (z. B. Aufklärung über Datenverarbeitung oder Granularität der Datenschutzeinstellungen) oder Kontrolle (z. B. Kontrolle über Verarbeitungsort, Datenkategorien und Empfänger). Durch die Strukturierung mittels Checklisten werden Beobachtungen reproduzierbarer und die Vergleichbarkeit wird erleichtert, ohne dass hierfür zwingend spezialisierte Messtechnik erforderlich wäre.

4.2 Automatisierte Analysen

Daneben existieren automatisierte Analyseverfahren, die insbesondere dort relevant werden, wo Datenflüsse technisch erfasst oder große Mengen an Informationen ausgewertet werden sollen.

Netzwerkschnittstellen

Die Kommunikation von IoT-Geräten kann vielfältig ausgestaltet sein. Sie kann entweder über eine direkte Verbindung mittels WLAN-Access-Point erfolgen, alternativ über die App ins Internet oder über ein spezielles IoT-Gateway. Um möglichst viele der Kommunikationspfade abdecken zu können, bietet sich eine Messung am lokalen Router, also am Übergang vom lokalen zum öffentlichen Netz, an. Dadurch wird ein Ort gewählt, an dem sich verschiedene Kommunikationsvarianten zusammenführen und beobachten lassen. Für den Fall, dass die Kommunikation eines IoT-Geräts mit dem Internet hauptsächlich über eine Begleit-App erfolgt, entsteht hierbei jedoch die Herausforderung, die Kommunikation im Zusammenhang mit dem IoT-Gerät vom Datenverkehr zu trennen, der durch andere Anwendungen auf dem Smartphone initiiert wird.

Durch die Analyse von IP-Netzwerkschnittstellen können Eigenschaften aus den Kategorien Datensicherheit und technische Schutzmaßnahmen (z. B. Verschlüsselung der Kommunikation) und Transparenz (z. B. Datenverarbeitung außerhalb der EU, Datenempfänger) erhoben werden. Die Netzwerkanalyse wird damit zu einem Instrument, um intransparente Kommunikationsbeziehungen zumindest teilweise sichtbar zu machen (Jakaria u. a. 2024).

Datenschutzerklärungen

Ein weiterer Gegenstand automatisierter Analyse ist die Auswertung von Datenschutzerklärungen (Yang u. a. 2025). Ziel ist hierbei die automatisierte Extraktion von Angaben, beispielsweise zu verarbeiteten Datentypen, zum Einsatz von Profiling, zu Verarbeitungszwecken und Datenempfängern. In der Praxis werden Datenschutzerklärungen jedoch häufig nicht spezifisch für einzelne IoT-Produkte bereitgestellt, sondern global für einen Hersteller. Dadurch enthalten sie Informationen zu vielen verschiedenen Kontexten, etwa zur Nutzung der Website oder zu Bewerbungsprozessen.

Für eine automatisierte Analyse ergibt sich daraus die Notwendigkeit, den Kontext der Informationen aus Datenschutzerklärungen festzustellen und zu berücksichtigen. Ohne Kontextbezug besteht das Risiko, dass Aussagen aus nicht passenden Abschnitten fälschlich einem IoT-Produkt zugeordnet werden. Ist diese Voraussetzung erfüllt, können insbesondere Eigenschaften aus der Kategorie Transparenz (z. B. Verarbeitungszwecke oder Profiling) automatisiert erhoben werden.

5. Vergleichbarkeit und Bewertbarkeit gesammelter Eigenschaften

Für die Einordnung privatheits-relevanter Informationen stellt sich die Frage, wie Eigenschaften vergleichbar und bewertbar gemacht werden können. Bisherige Privacy Labels arbeiten oft mit Skalen, um die Privatheitsfreundlichkeit in unterschiedlichen Kategorien zu bewerten. Studien haben jedoch gezeigt, dass Nutzende weniger an Bewertungen als an konkreten Details beziehungsweise Informationen interessiert sind (Johnson u. a. 2020). Insbesondere für die Abwägung des Kaufs eines Produktes ist eine schnelle Vergleichbarkeit jedoch unabdingbar, was im Widerspruch zu detaillierten Angaben bezüglich der Privatheit stehen kann. Um die vorgestellten Eigenschaften dennoch strukturiert im Rahmen einer Plattform darstellen zu können, können diese in Bezug auf ihre Vergleichbarkeit und in Teilen auch Bewertbarkeit kategorisiert werden.

5.1 Binäre Eigenschaften

Binäre Eigenschaften ermöglichen eine Aussage über die Existenz einer Funktion oder Gegebenheit. Beispiele sind die Notwendigkeit eines Accounts oder die Nutzung von Backend-Diensten. Solche Eigenschaften erlauben meist keine differenzierte Bewertung oder Anwendung von Skalen, können aber für eine grundlegende Vergleichbarkeit herangezogen werden, weil sie klare Ja-/Nein-Aussagen liefern.

5.2 Detailangaben

Detailangaben sind strukturierte Informationen, die Eigenschaften eines Produktes beschreiben, beispielsweise eine Liste der App-Zugriffsberechtigungen oder die Benennung von Datenempfängern. Auch hier ist eine Bewertung meist nicht möglich, da diese Angaben oft mit dem Empfinden und den Präferenzen der Nutzer:innen in Verbindung stehen. Eine konsistente Struktur der Detailangaben ermöglicht jedoch Vergleiche und Filterungen, bei denen persönliche Präferenzen berücksichtigt werden können.

5.3 Quantifizierende Eigenschaften

Quantifizierende Eigenschaften beschreiben eine Eigenschaft über eine Anzahl, etwa die Anzahl der App-Zugriffsberechtigungen oder die Menge

verarbeiteter Datentypen. Auch dies stellt keine Bewertung dar, ermöglicht aber einfache Vergleiche zwischen ähnlichen Produkten, weil Unterschiede numerisch darstellbar werden.

5.4 Bewertungen

Nur wenige Eigenschaften erlauben direkte Bewertungen eines Produktes. Dies steht häufig im Zusammenhang mit technischen und rechtlichen Mindeststandards. Beispielsweise gilt ein Produkt, das mit dem Internet verbunden wird, aber nicht geupdatet werden kann, nach heutigem Stand der Technik als unzureichend. Werden beim Betrieb eines IoT-Gerätes personenbezogene Daten durch einen Cloud-Dienst verarbeitet, ist die Implementierung der Betroffenenrechte nach DSGVO unverzichtbar. Ebenso ist unverschlüsselte Kommunikation mit Backend-Diensten ein Beispiel für eine Eigenschaft, die einen aufklärenden Hinweis nahelegt, weil sie grundlegende Schutzziele der IT-Sicherheit verletzt.

6. Individualisierbare Bewertungssystematik

Da das Privatheitsempfinden grundsätzlich subjektiv ist und IoT-Produkte sich über vielfältige Produktkategorien erstrecken, ergibt sich die Notwendigkeit einer flexiblen Bewertungssystematik. Diese sollte insbesondere berücksichtigen, dass vergleichende Aussagen nur innerhalb einer Produktkategorie sinnvoll sind, weil Eigenschaften spezifisch für bestimmte Kategorien sein können. So ist etwa die Verarbeitung von Videodaten bei Kameras trivial, während sie bei Kinderspielzeug in einem anderen Kontext steht und anders gewichtet werden kann.

Darüber hinaus sollte die Priorisierung der Darstellung privatheits-relevanter Eigenschaften personalisierbar sein, da das Empfinden der Sensitivität unterschiedlicher Eigenschaften individuell abweichen kann. Zusätzlich kann jeweils nur eine begrenzte Auswahl an privatheits-relevanten Eigenschaften gleichzeitig präsentiert werden. Dies macht eine Priorisierung erforderlich, die nicht allein allgemein festgelegt ist, sondern anpassbar gestaltet werden muss, um unterschiedlichen Bedürfnissen und Präferenzlagen gerecht zu werden. Um eine solche Priorisierung fundiert gestalten zu können, sollte die empfundene Relevanz privatheitsrelevanter Eigenschaften durch Nutzerstudien erhoben werden. Da diese Wahrnehmung subjek-

tiv und kontextabhängig ist, gilt dies sowohl allgemein als auch in Abhängigkeit von der jeweiligen Produktkategorie. Die Ergebnisse können als Grundlage dienen, um sinnvolle Standardpriorisierungen abzuleiten und den Gestaltungsraum für individuelle Anpassungen empirisch abzusichern.

7. Fazit

Die identifizierten Privatheitseigenschaften ermöglichen es Endnutzer:innen, fundierte Entscheidungen beim Erwerb von IoT-Geräten zu treffen. Darüber hinaus bieten sie Verbraucherzentralen eine belastbare Grundlage für die Erstellung von Berichten sowie für die Beratung im Kontext des IoT. Auch Aufsichtsbehörden und Gesetzgeber profitieren von diesen Erkenntnissen, da sie einen aktuellen Überblick über bestehende Datenschutzpraktiken erhalten und darauf aufbauend langfristige Maßnahmen zur Verbesserung des Datenschutzes und des Schutzes der Privatheit entwickeln können.

Gleichwohl ist die resultierende Sammlung von 54 Eigenschaften nicht als abschließend zu betrachten. Die gewählte Methodik – eine fokussierte Literaturrecherche, ergänzt durch Expertenworkshops – war darauf ausgelegt, eine breite und praxisrelevante Merkmalsbasis zu erarbeiten, nicht jedoch darauf, sämtliche denkbaren Eigenschaften lückenlos zu erheben, wie es etwa eine systematische Literaturrecherche anstreben würde. Der interdisziplinären Zusammensetzung der Expertengruppe kam dabei eine kompensierende Rolle zu, da die Vielfalt der fachlichen Perspektiven dazu beitrug, wesentliche Lücken im Eigenschaftsraum zu vermeiden. Darüber hinaus sind weiterführende Arbeiten erforderlich, um die Sammlung auf eine übersichtlichere und damit gebrauchstauglichere Anzahl zu reduzieren. Eine solche Reduktion sollte sowohl die Komplexität der Erhebung einzelner Eigenschaften berücksichtigen, die eng mit der konkreten Implementierung der jeweiligen Messinstrumente zusammenhängt, als auch die Perspektive von Nutzer:innen einbeziehen. Hierzu sind Nutzerstudien notwendig, die untersuchen, welche Eigenschaften als besonders relevant wahrgenommen werden und in welcher Priorisierung sie dargestellt werden sollten.

Literaturverzeichnis

- Alshehri, Ahmed Mohammed; Spielman, Joseph; Prasad, Amiya und Yue, Chuan (2022): Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders. *Proceedings on Privacy Enhancing Technologies*. URL: <https://petsymposium.org/popets/2022/popets-2022-0064.pdf>
- Anselmi, Gianluca; Vekaria, Yash; D'Souza, Alexander; Callejo, Patricia; Mandalari, Anna Maria und Shafiq, Zubair (2024): Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs. In: *Proceedings of the 2024 ACM on Internet Measurement Conference (IMC '24)*, S. 622–634. New York: Association for Computing Machinery. <https://doi.org/10.1145/3646547.3689013>
- Bermejo Fernandez, Carlos; Lee, Lik Hang; Nurmi, Petteri und Hui, Pan (2021): PARA: Privacy Management and Control in Emerging IoT Ecosystems Using Augmented Reality. In: *Proceedings of the International Conference on Multimodal Interaction*. <https://doi.org/10.1145/3462244.3479885>
- Chen, Jiahong; Edwards, Lilian; Urquhart, Lachlan und McAuley, Derek (2020): Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption. *International Data Privacy Law* 10 (4): S. 279–298. <https://doi.org/10.1093/idpl/ipaa011>
- Chen, Claire; Ravishankar, Hamsini; Shu, Dillon; Jain, Laxita; Zeng, Yifeng; Agarwal, Yuvraj und Cranor, Lorrie Faith (2023): Ask the Consumers: What Should Be On IoT Privacy & Security Labels. Poster at the *Symposium on Usable Privacy and Security (SOUPS)*.
- Chhetri, Chola und Motti, Vivian (2022): Designing and Evaluating a Prototype for Data-Related Privacy Controls in a Smart Home. In: *International Symposium on Human Aspects of Information Security and Assurance*. https://doi.org/10.1007/978-3-031-12172-2_19
- Cranor, Lorrie Faith; Agarwal, Yuvraj und Emami-Naeini, Pardis (2024): Internet of Things Security and Privacy Labels Should Empower Consumers. *Communications of the ACM* 67.
- Cruz, Stefany; Danek, Logan; Liu, Shinan; Kraemer, Christopher; Wang, Zixin; Feamster, Nick; Huang, Danny Yuxing; Yao, Yaxing und Hester, Josiah (2023): Augmented Reality's Potential for Identifying and Mitigating Home Privacy Leaks. In: *Symposium on Usable Security and Privacy (USEC)*. <https://doi.org/10.14722/usec.2023.238930>
- Emami-Naeini, Pardis; Dixon, Henry; Agarwal, Yuvraj und Cranor, Lorrie Faith (2019): Exploring How Privacy and Security Factor Into IoT Device Purchase Behavior. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3290605.3300764>
- Emami-Naeini, Pardis; Dheenadhayalan, Janarth; Agarwal, Yuvraj und Cranor, Lorrie Faith (2022): An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. *IEEE Security & Privacy* 20 (2): S. 31–39. <https://doi.org/10.1109/MS-EC.2021.3132398>

- Europäische Union (EU) (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung, DSGVO).
- Europäische Union (EU) (2024): Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates (Cyber Resilience Act, CRA).
- European Data Protection Board (EDPB) (2020): Guidelines 05/2020 on Consent Under Regulation 2016/679. Version 1.1.
- Fuhrken, Stefan (2026): BGH Verhandlungsterminhinweis I ZR 289/25 (Videoüberwachung in der Wohnküche) – Lünedatenschutz. Februar 9. URL: <https://xn--luedatenschutz-gsb.de/2026/02/09/bgh-verhandlungsterminhinweis-i-zr-289-25-videoueberwachung-in-der-wohnekueche/> (besucht am: 14.04.2026)
- Greveler, Ulrich; Justus, Benjamin und Löhr, Dennis (2012): Identifikation von Videoinhalten über granulare Stromverbrauchsdaten. *SICHERHEIT 2012 – Sicherheit, Schutz und Zuverlässigkeit*, S. 35–45. Bonn: Gesellschaft für Informatik eV.
- Hudig, Anna Ida; Norval, Chris und Singh, Jatinder (2023): Transparency in the Consumer Internet of Things: Data Flows and Data Rights. London: Information Commissioner's Office.
- Hudig, Anna Ida; Mandalari, Anna Maria; Norval, Chris; Haddadi, Hamed; Binns, Reuben und Singh, Jatinder (2025): Rights Out of Sight: Data Practices and Transparency Gaps in Smart Consumer IoT Ecosystems. In: *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25)*, S. 2260–2273. New York: Association for Computing Machinery. <https://doi.org/10.1145/3715275.3732154>
- Jakaria, Md; Huang, Danny Yuxing und Das, Anupam (2024): Connecting the Dots: Tracing Data Endpoints in IoT Devices. *Proceedings on Privacy Enhancing Technologies*. URL: <https://petsymposium.org/popets/2024/popets-2024-0090.php>
- Johnson, Shane D.; Blythe, John M.; Manning, Matthew und Wong, Gabriel T. W. (2020): The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay. *PLOS ONE* 15 (1). <https://doi.org/10.1371/journal.pone.0227800>
- Khalesi, Ben (2025): I Thought I Had a Smart Home, but Then I Turned Off the Internet. *Android Police*, Juli 20. URL: <https://www.androidpolice.com/smart-home-vs-no-wifi/>
- Khetagourova, Natalia; Lundh, Christoffer und Kävrestad, Joakim (2025): Evaluating Security and Data Privacy in Smart Home Devices. In: *Socio-Technical Perspectives in Information Systems 2025: Proceedings of the 11th International Workshop on Socio-Technical Perspectives in Information Systems (STPIS 2025)*, CEUR Workshop Proceedings, Bd. 4134.
- Li, Tianshi; Cranor, Lorrie Faith; Agarwal, Yuvraj und Hong, Jason I. (2024): Matcha: An IDE Plugin for Creating Accurate Privacy Nutrition Labels. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 8 (1). <https://doi.org/10.1145/3643544>
- Lin, Yanzi; Juneja, Jaideep; Birrell, Eleanor und Cranor, Lorrie Faith (2023): Data Safety vs. App Privacy: Comparing the Usability of Android and iOS Privacy Labels. *arXiv preprint arXiv:2312.03918*.

- Manandhar, Sunil; Roundy, Kevin; Tamersoy, Acar; Memon, Nasir; Kirda, Engin; Yao, Daphne und Kang, Byungkoon (2022): Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage. In: *31st USENIX Security Symposium* (USENIX Security 22). USENIX Association. <https://www.usenix.org/conference/usenixsecurity22/presentation/manandhar>
- Norval, Chris und Singh, Jatinder (2023): A Room With an Overview: Toward Meaningful Transparency for the Consumer Internet of Things. *IEEE Internet of Things Journal* 11 (5). <https://doi.org/10.1109/JIOT.2023.3318369>
- Pan, Shidong; Tao, Zhen; Hoang, Thong; Zhang, Dawen; Li, Tianshi; Xing, Zhenchang; Xu, Xiwei; Staples, Mark; Rakotoarivelo, Thierry und Lo, David (2024): A New Hope: Contextual Privacy Policies for Mobile Applications and An Approach Toward Automated Generation. In *33rd USENIX Security Symposium* (USENIX Security 24), S. 5699–5716. Philadelphia: USENIX Association. <https://www.usenix.org/conference/usenixsecurity24/presentation/pan-shidong-hope>
- Railean, Alexandr und Reinhardt, Delphine (2018): Let There Be Lite: Design and Evaluation of a Label for IoT Transparency Enhancement. In: *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*. <https://doi.org/10.1145/3236112.3236126>
- Railean, Alexandr und Reinhardt, Delphine (2021): OnLITE: On-Line Label for IoT Transparency Enhancement. In: *Secure IT Systems*, herausgegeben von Mikael Asplund und Simin Nadjm-Tehrani, Bd. 12556. *Lecture Notes in Computer Science*. Springer International Publishing. https://doi.org/10.1007/978-3-030-70852-8_14
- Rauti, Sampsa; Laato, Samuli und Pitkämäki, Tinja (2023): An Assessment of Privacy Policies for Smart Home Devices. In *Proceedings of the 24th International Conference on Computer Systems and Technologies*. New York: Association for Computing Machinery. <https://doi.org/10.1145/3606305.3606332>
- Reinhardt, Andreas; Englert, Frank und Christin, Delphine (2015): Averting the Privacy Risks of Smart Metering by Local Data Preprocessing. *Pervasive and Mobile Computing* 16 (Januar): S. 171–183. <https://doi.org/10.1016/j.pmcj.2014.10.002>
- Saqib, Eimaan; He, Shijing; Choy, Junghyun; Abu-Salma, Ruba; Such, Jose; Bernd, Julia und Javed, Mobin (2025): Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions. *ACM Transactions on Computer-Human Interaction*, Mai 8. <https://doi.org/10.1145/3731755>
- Shen, Yun und Vervier, Pierre-Antoine (2019): IoT Security and Privacy Labels. In: *Privacy Technologies and Policy*, APF 2019, herausgegeben von M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina und A. Bourka, Bd. 11498. *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-030-21752-5_9
- Subahi, Alanoud und Theodorakopoulos, George (2019): Detecting IoT User Behavior and Sensitive Information in Encrypted IoT-App Traffic. *Sensors* 19 (21). <https://doi.org/10.3390/s19214777>
- Urquhart, Lachlan und Chen, Jiahong (2021): On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity. In: *Privacy by Design for the Internet of Things: Building Accountability and Security*, herausgegeben von Andrew Crabtree, Hamed Haddadi und Richard Mortier, S. 19–47. Stevenage: IET.

- Yang, Mian; Atluri, Vijayalakshmi; Sural, Shamik und Kundu, Ashish (2025): Automated Privacy Policy Analysis Using Large Language Models. In: *Data and Applications Security and Privacy XXXIX: 39th IFIP WG 11.3 Annual Conference*, DBSec 2025, Gjøvik, Norway, June 23–24, 2025, Proceedings, S. 23–43. https://doi.org/10.1007/978-3-031-96590-6_2
- Zhang, Shikun und Sadeh, Norman (2023): Do Privacy Labels Answer Users' Privacy Questions? In *Workshop on Usable Security and Privacy*.

