digitale woche 2017

Kiel. Sailing.City.

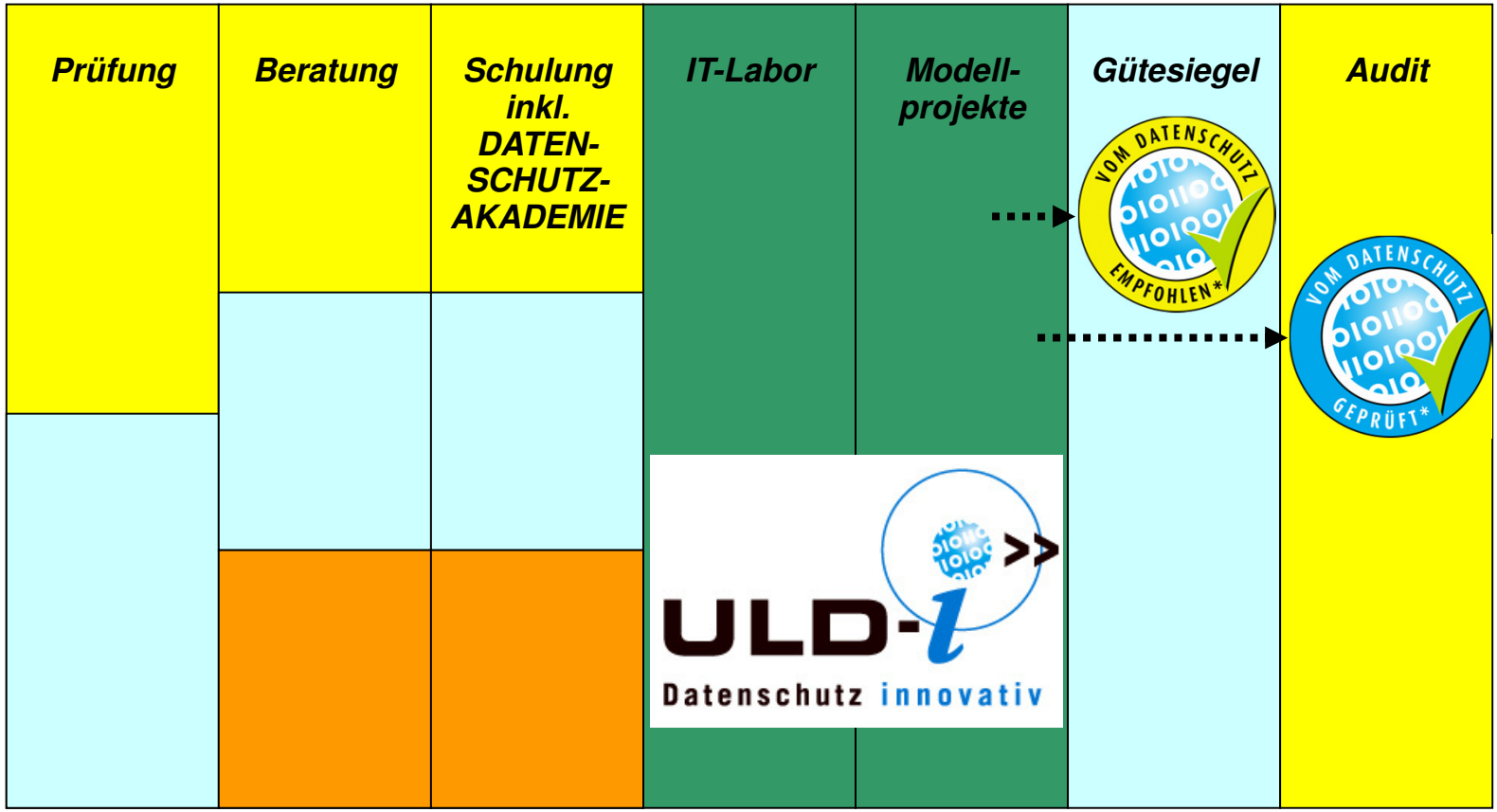
Wissen, was Ihr Fernseher über Sie weiß –
Datenschutz und Transparenz im Internet of Things

Harald Zwingelberg, ULD

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Die 7 Säulen des ULD



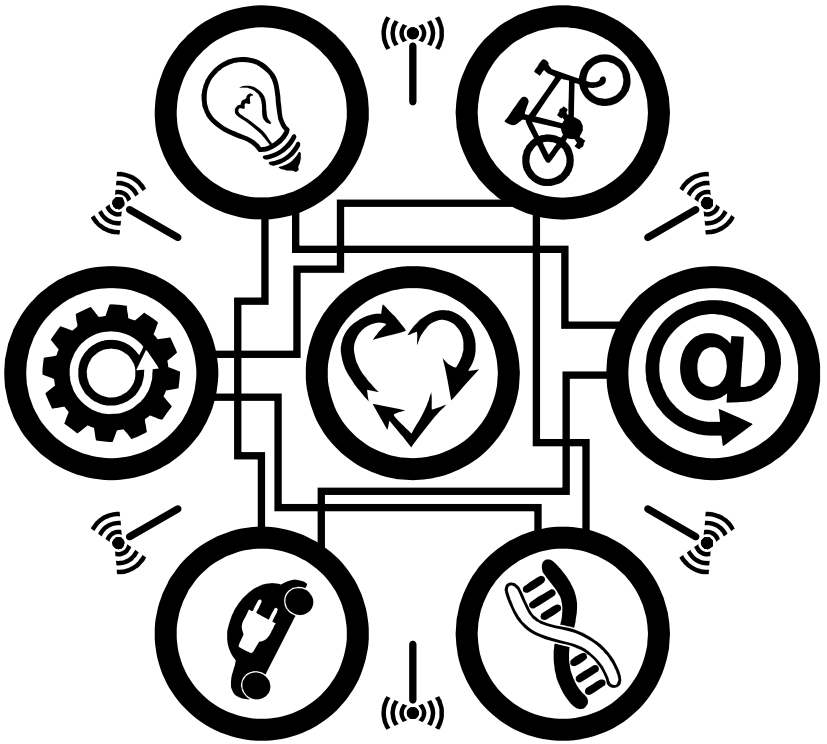
Übersicht

- Einleitung
  - Was ist das IoT?
  - Warum Datenschutz?
  - Bedeutung der Transparenz
- Verstecktes Internet
  - Smart Home (TV, AAL)
  - Smart Car,
  - IoT-Lebenszyklus
- Fragen & Diskussion

Einführung
Was ist das IoT?

- Das Internet der Dinge, (engl. Internet of Things) bezeichnet die Verknüpfung eindeutig identifizierbarer physischer Objekte (*things*) mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur. Es besteht nicht mehr nur aus teilnehmenden Personen, sondern auch aus Dingen.

Quelle: Wikipedia

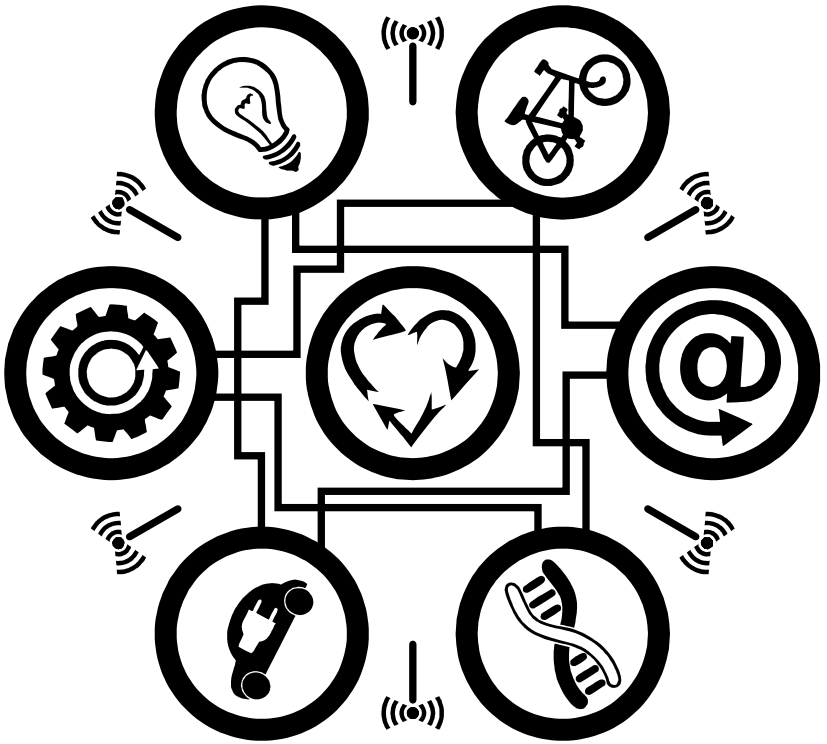


CC0: Public Domain, https://openclipart.org

Einführung
Was ist das IoT?

Beispiele

- Haushalt: Licht, Alarm, Strombezug, Steuerung von Anlagen und Energie,…
- Mobilität: Vernetzte Fahrzeuge, IT und Sensoren im Auto, Kommunikation mit Hersteller, Werkstatt etc.
- Gesundheit: Alles von Fallsensoren im Boden über vernetzte Hilfen im Heim bis hin zu implantierten Sensoren und Herzschrittmachern
- Kleidung, Waren: RFID in der Lieferkette



CC0: Public Domain, https://openclipart.org

Quelle: Wikipedia

Beim Datenschutz geht es um ~~Daten~~

Menschen mit ihren Rechten

Fragen an Gestalter von Technik

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

Beim Datenschutz geht es um das Verhältnis…

… von Organisationen, Unternehmen und Behörden …

… zu Personen.

Datenschutz ist Regelung für das Machtgefälle

Warum Datenschutz? Brauchen wir Privatsphäre?

Wenn die Mehrheit **auf Privatsphäre verzichtet** – müssen dann alle darauf verzichten?

Kann durch ein **Verhalten einer Mehrheit** eine **Regel für alle** geschaffen werden?

Die **Normative Kraft des Faktischen** - Georg Jellinek

Anonymität ist notwendig

Onlineberatung des WEISSEN RINGS

Sie oder eine Person aus Ihrem Umfeld sind von einer Straftat betroffen? Sie wurden Zeuge einer Straftat? Die Onlineberatung des WEISSEN RINGS unterstützt Sie gerne!

Die Onlineberatung ist anonym, kostenfrei und bundesweit erreichbar. Alle Daten werden auf einem externen Server verschlüsselt gespeichert und absolut vertraulich behandelt.

Bitte beachten Sie: In aller Regel erhalten Sie auf Ihre erste Anfrage innerhalb von 72 Stunden eine persönliche Antwort. Sollten Sie schnell und direkt Hilfe benötigen, wenden Sie sich bitte an eine unserer 420 Außenstellen oder an unser kostenfreies und bundesweit erreichbares Opfer-Telefon unter 116 006.

Weitere Informationen finden Sie in unseren häufig gestellten Fragen sowie unter Nutzungsbedingungen und Datenschutz.

Quelle: http://weisser-ring.de/hilfe/onlineberatung

Wie funktioniert die Onlineberatung?

Über uns

Nutzungsbedingungen und Datenschutz

Anonymität ist notwendig

kein täter werden.

Kostenlose Therapie unter Schweigepflicht

Aktuelles | Über uns | Hintergrund | Die Therapie | Erfahrungsberichte | Medien

Quelle: https://www.kein-taeter-werden.de

lieben sie kinder mehr, als ihnen lieb ist?

Das Präventionsnetzwerk bietet ein an allen Standorten kostenloses und durch die Schweigepflicht geschütztes Behandlungsangebot für Menschen, die sich sexuell zu Kindern hingezogen fühlen und deshalb therapeutische Hilfe suchen.

Im Rahmen der Therapie erhalten die betroffenen Personen Unterstützung, um mit ihrer pädophilen oder hebephilen Neigung leben zu lernen, diese zu akzeptieren und in ihr Selbstbild zu integrieren.

Ziel ist es, sexuelle Übergriffe durch direkten körperlichen Kontakt oder indirekt durch den Konsum oder die Herstellung von Missbrauchsabbildungen im Internet (sogenannte Kinderpornografie) zu verhindern.

Rückzugsräume sind wichtig für Menschen

- Räume werden von uns in öffentliche, private und intime Zonen geteilt – im Büro und Zuhause (Flur – Wohnzimmer – Schlafzimmer)

- IoT-Geräte dringen in private und intime Bereiche ein und übermitteln unter anderem Ton- und Bildaufnahmen, Nutzungsgewohnheiten und Kommunikationsverhalten an Hersteller und Dritte im Netz.

  Beispiele: vernetzte sprechende Kuscheltiere / Erotikartikel mit Audio, Video und Wifi / Fitnessuhren, -armbänder

Informationelle Selbstbestimmung ist ein Grundrecht

Bundesverfassungsgericht 1983:

- Jeder soll grundsätzlich selbst entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte verarbeitet werden.

- Kurz: Jeder soll entscheiden können, wer welche Daten zu welchen Zwecken verarbeitet.

⇒ Um das Recht mit Leben zu füllen, muss man auch entsprechend darüber informiert sein = Transparenz

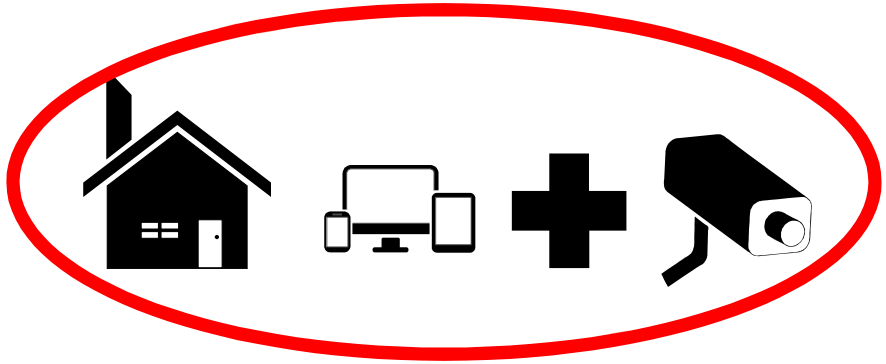
Einleitung: Transparenz im Verständnis des Datenschutzes

Transparenz bezeichnet die Anforderung, dass sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme hat.

Quelle: Standarddatenschutzmodell, S. 13.

Verstecktes Internet

1. **Smart Home, Smart TV, Assisted Living**



2. Smart Mobility

3. IoT Lebenszyklus

Smart TV und Datenschutz

- „… wo Smart draufsteht, gehen immer auch Daten raus."
  (Stiftung Warentest, Smart TV und Datenschutz, 2016)

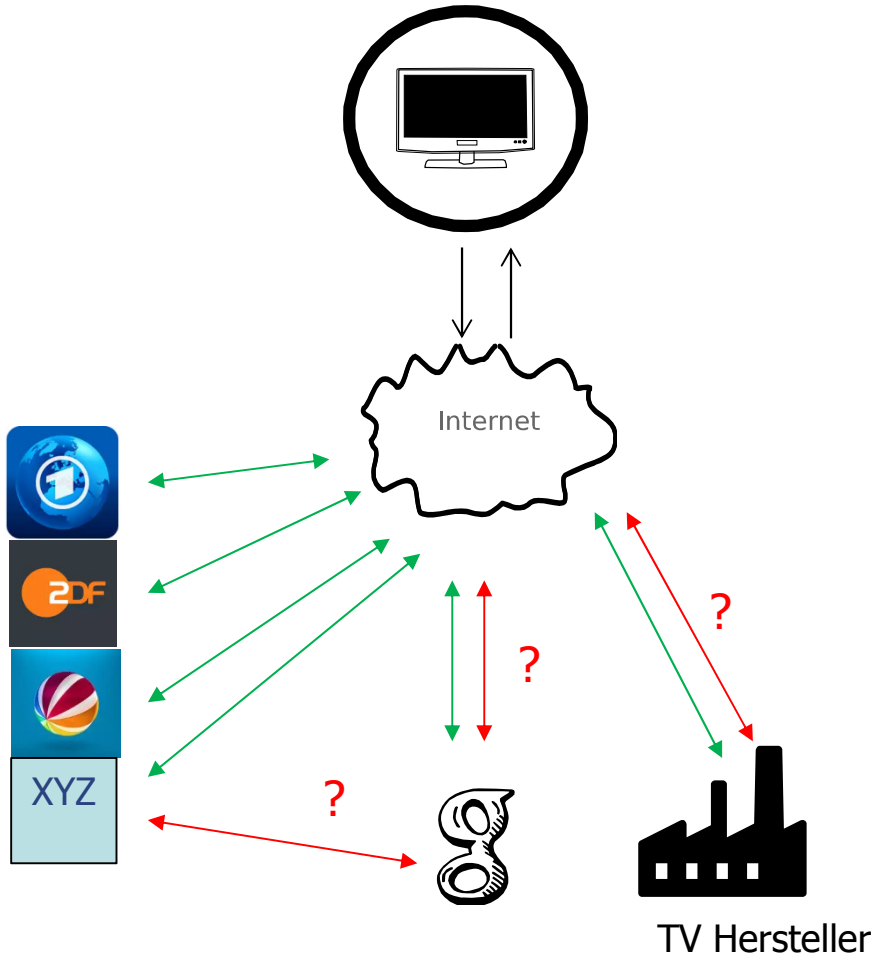
- Mehr als die Hälfte der Fernseher sind internetfähig + weitere mit Anschluss via Chrome, Prime-Stick, etc.

- Zuschauer genießen Mediatheken, Videoclips oder die diversen Video on Demand Angebote, Videotelefonie,…

- Geräte empfangen nicht nur Daten sondern senden auch Informationen an Sender, Hersteller, Werbetreibende

Datenübermittlungen

- Geräte kommunizieren mit Hersteller, teilweise auch Google (Android-Updates) und Microsoft.
- Manche TV-Sender veranlassen, dass Google über jeden Senderwechsel unterrichtet wird.
- Verkehr lässt sich kaum sinnvoll sperren oder filtern.
- Anfälligkeit für Schadsoftware besteht, bisher immerhin nicht in Praxis.
- Mikrofon und Kamera als Risiko.



Bilder: ARD, ZDF, Sat1, Rest: CC0: Public Domain, https://openclipart.org

Das komplexe Bild

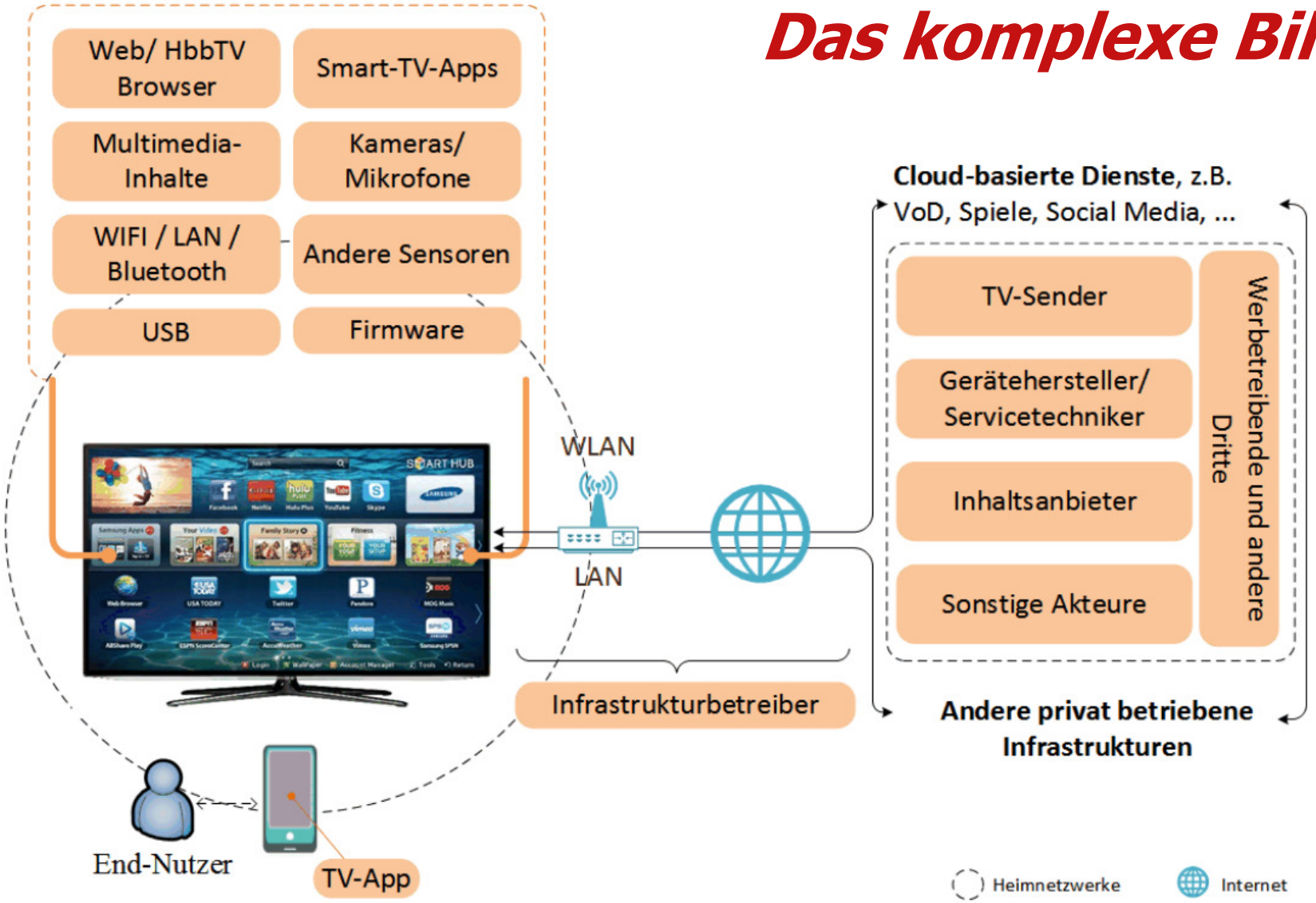


Bild: Forum Privatheit, Das Versteckte Internet, S. 10.

Transparenz bei Smart TV

- Mangelnde Transparenz der Datenschutzerklärungen (z.B. Samsung bei nicht rechtskräftigem Urteil des LG Frankfurt M., 2-03 O 364715, 120 Bildschirmseiten)

- Data Protection by Design und Default (neu in der DSGVO)
  - Geräte sind so zu gestalten, dass Voreinstellungen datenschutzfördernd sind. D.h. keine Datenübermittlung ohne gesonderte Zustimmung. Trennung nach Zwecken: So ist Software-Update vom Hersteller für die meisten Nutzer wohl OK aber das Fernsehverhalten soll nicht zwingend übermittelt werden.

Smart TV

- Forderungen und Ideen für mehr Transparenz
  - Einfach, klar und verständlich (so auch DSGVO!)
  - Sinnvolle Visualisierung – auch für Sehbehinderte
  - Sichtbarmachen der Datenerhebung: z.B. LED je für Internetverbindung, Kamera, Mikrofon
  - Unterrichtung über die aufgebauten Verbindungen
  - Idealerweise ein einfach einsehbares Logfile
  - Verpackung soll bereits informieren, ob Internetverbindung zur vollen Nutzung nötig ist, über Arten der übermittelten Daten und ob diese in Staaten außerhalb der EU gelangen.

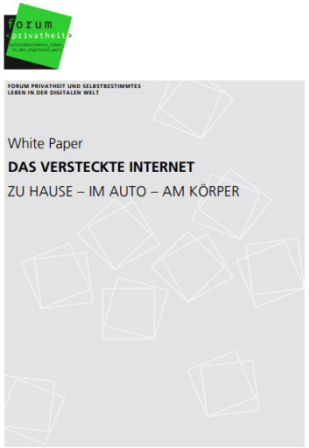
Selbstdatenschutz bei Smart TV

- PC als Empfänger nutzen und via HDMI an TV anschließen. Dann hat man mehr Kontrollmöglichkeiten, Optionen des Browsers und Antivirensoftware
- Auswahl des Geräts
  - Hersteller sollten Voreinstellungen datensparsam wählen
  - Internet, Kamera und Mikrofon sollten erst bewusst durch den Nutzer aktiviert werden
  - Mikrofone und Kameras sollten vom Nutzer deaktiviert werden können
  - Cookies sollten löschbar sein
- DVD-Abend oder ein gutes Buch

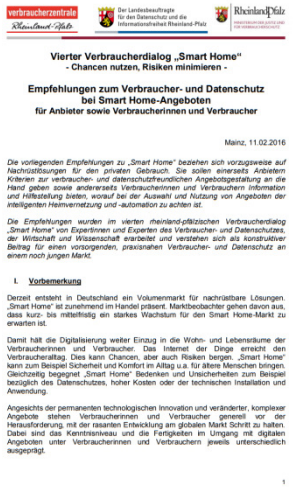
Weitergehende Informationen

- Forum Privatheit, Smart-TV und Privatheit
  https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/Forschungsbericht-Smart-TV-und-Privatheit_Druckfassung.pdf

- Forum Privatheit, Das versteckte Internet
  https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/White-Paper-2-Final_17.07.15-Druckversion.pdf



- LfD R-P, Verbraucherzentrale R-P: Empfehlungen zum Verbraucher- und Datenschutz bei Smart Home-Angeboten für Anbieter sowie Verbraucherinnen und Verbraucher
  https://mjv.rlp.de/fileadmin/mjv/Themen/Verbraucherschutz/Ergebnispapier_mit_Empfehlungen_zum_Verbraucher__und_Datenschutz_bei_Smart_Home_Angeboten_fuer_Anbieter_sowie_Verbraucherinnen_und_Verbraucher_.pdf


Vierter Verbraucherdialog „Smart Home"
- Chancen nutzen, Risiken minimieren -

Empfehlungen zum Verbraucher- und Datenschutz bei Smart Home-Angeboten für Anbieter sowie Verbraucherinnen und Verbraucher

Mainz, 11.02.2016

Die vorliegenden Empfehlungen zu „Smart Home" beziehen sich vorzugsweise auf Nachrüstlösungen für den privaten Gebrauch. Sie sollen einerseits Anbietern Kriterien zur verbraucher- und datenschutzfreundlichen Angebotsgestaltung an die Hand geben sowie andererseits Verbraucherinnen und Verbrauchern Information und Hilfestellung bieten, worauf bei der Auswahl und Nutzung von Angeboten der intelligenten Heimvernetzung und -automation zu achten ist.

Die Empfehlungen wurden im vierten rheinland-pfälzischen Verbraucherdialog „Smart Home" von Expertinnen und Experten des Verbraucher- und Datenschutzes, der Wirtschaft und Wissenschaft erarbeitet und verstehen sich als konstruktiver Beitrag für einen vorsorgenden, praxisnahen Verbraucher- und Datenschutz an einem noch jungen Markt.

I. Vorbemerkung

Derzeit entsteht in Deutschland ein Volumenmarkt für nachrüstbare Lösungen. „Smart Home" ist zunehmend im Handel präsent. Marktbeobachter gehen davon aus, dass kurz- bis mittelfristig ein starkes Wachstum für den Smart Home-Markt zu erwarten ist.

Damit hält die Digitalisierung weiter Einzug in die Wohn- und Lebensräume der Verbraucherinnen und Verbraucher. Das Internet der Dinge erreicht den Verbraucheralltag. Dies kann Chancen, aber auch Risiken bergen. „Smart Home" kann zum Beispiel Sicherheit und Komfort im Alltag u.a. für ältere Menschen bringen. Gleichzeitig begegnet „Smart Home" Bedenken und Unsicherheiten zum Beispiel bezüglich des Datenschutzes, hoher Kosten oder der technischen Installation und Anwendung.

Angesichts der permanenten technologischen Innovation und veränderter, komplexer Angebote stehen Verbraucherinnen und Verbraucher generell vor der Herausforderung, mit der rasanten Entwicklung am globalen Markt Schritt zu halten. Dabei sind das Kenntnisniveau und die Fertigkeiten im Umgang mit digitalen Angeboten unter Verbraucherinnen und Verbrauchern jeweils unterschiedlich ausgeprägt.

Datenschutz und Ambient Assisted Living (2011)

- Vergleichbare Fragestellungen im Bereich Gesundheit und Pflege
- Mit steigendem Alter der Bevölkerung werden Assistenzsysteme bedeutsam
- Es gelten mit anderen Smart Home Lösungen vergleichbare Anforderungen, wegen der Verarbeitung von Gesundheitsdaten idR eher strengere Anforderungen
- Patienten sind idR offener für Datenverarbeitung aber auch abhängiger
- Systeme müssen z.B. ausschaltbar sein
- Delegierbare Kontrollmöglichkeiten z.B. an Vertrauensperson

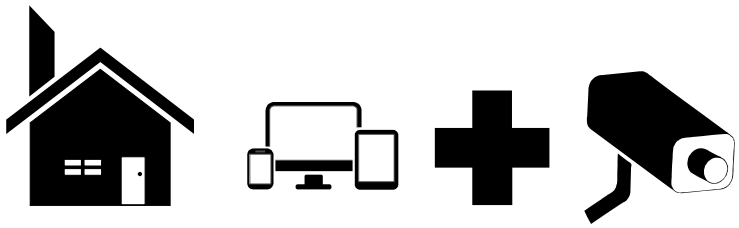
Studie: https://www.datenschutzzentrum.de/projekte/aal/

Weitere Themenbereiche Smart Home

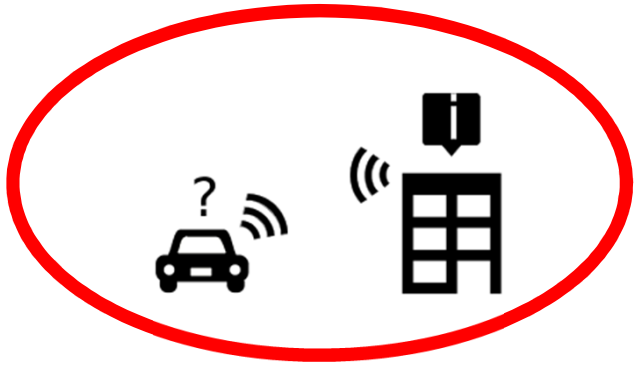
- Stromzähler: Je nach gemessenen Zeitintervallen kann genau auf Elektrogerät und damit auf Verhalten geschlossen werden
- Adere Devices: Vernetzte Lampen, Alarm- & Schließanlagen, Videoüberwachung können einem Angreifer nützliche Informationen bieten
- Darstellungsprobleme: Wie kann ohne Bildschirm oder Eingabemöglichkeit mit dem Gerät kommuniziert werden?
- Vernetzte Kaffeemaschine im Büro? Was erfährt der Arbeitgeber?
- …

Verstecktes Internet

1. Smart Home, Smart TV, Assisted Living



2. Smart Mobility



3. IoT Lebenszyklus

Datenschutzherausforderung Industrieinteressen

17. November 2016, 07:27 Uhr Digitale Infrastruktur

Dobrindt will Zugriff auf Daten erleichtern

http://www.sueddeutsche.de/wirtschaft/digitale-infrastruktur-dobrindt-will-zugriff-auf-daten-erleichtern-1.3252303

Industrie hat großes Interesse an KFZ-Daten

Wertschöpfung u.a. für Entwicklung aber auch Weitergabe an Unternehmen

Anonymisierung und Pseudonymisierung als Lösung?

Viele Interessierte, viele Beteiligte

- Hersteller
- Händler, Werkstätten
- Lieferanten von Hard- und Software
- Netzwerkanbieter 4G, 5G
- Programmierer
- Halter / Eigentümer
  - Privatperson
  - Mitarbeiter
  - Leasingnehmer
  - Autovermietungen
  - Logistikunternehmen

- Versicherungen
- andere Vertragsparteien, Werbekunden
- Sicherheitsbehörden, Polizei
- andere Behörden

- Betroffene Personen im Sinne des Datenschutzrechts:
  - Eigentümer / Halter
  - Fahrer
  - frühere Fahrer, Halter
  - Mitfahrer, Passagiere
  - sonst. Verkehrsteilnehmer

Vielfältige Anforderungen

- Transparenz
  - Dokumentation muss vorhanden und verständlich sein
  - Zugänglichkeit für alle betroffenen Personen
  - Interfaces sollen Daten im Fahrzeug zugänglich machen

- Intervenierbarkeit / Eingriffsmöglichkeiten
  - Betroffene müssen Einflussmöglichkeiten haben: Abschalten der Erhebung, Löschung bestehender Daten, Rücksetzen auf Werkseinstellungen,…
  - Datenflüsse an Dritte können unterbunden werden

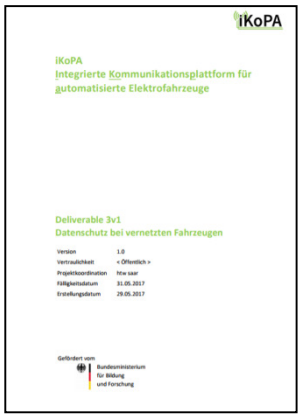
Vielfältige Anforderungen

- Datenminimierung
  - Lokale Datenverarbeitung im Fahrzeug ist gegenüber zentraler Verarbeitung beim Hersteller zu bevorzugen
  - Getrennte Verarbeitung für unterschiedliche Zwecke
  - Anonymisierung und Pseudonymisierung ermöglichen
  - Anonymisierung soll Vorzug haben

- IT-Sicherheit
  - Angemessene Schutzmaßnahmen sind zu ergreifen
  - Datenexport ermöglichen (Portabilität)

Weitergehende Informationen zu Datenschutz und smart cars

- iKoPA-Projekt, Datenschutz bei vernetzten Fahrzeugen
  https://ikopa.de/de/arbeitsergebnisse/


iKoPA

iKoPA
Integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge

Deliverable 3v1
Datenschutz bei vernetzten Fahrzeugen

Version 1.0
Vertraulichkeit < Öffentlich >
Projektkoordination htw saar
Fälligkeitsdatum 31.05.2017
Erstellungsdatum 29.05.2017

Gefördert vom Bundesministerium für Bildung und Forschung

- SeDaFa-Projekt, Selbstdatenschutz im vernetzten Fahrzeug, Publikation aus dem Projekt SeDaFa, DuD 2017,217, online (paywall): https://link.springer.com/article/10.1007/s11623-017-0761-8


Selbstdatenschutz im vernetzten Fahrzeug

Eine Datenschutzlösung unter Berücksichtigung der technischen, rechtlichen und Nutzeranforderungen

Die Vernetzung von Fahrzeugen bringt viele Mehrwerte, aber auch neue Gefahren in Bezug auf Sicherheit und Datenschutz. Dieser Artikel beleuchtet das Thema Datenschutz aus technischer, rechtlicher und Nutzerperspektive und zeigt Ansätze für die Entwicklung einer geeigneten Datenschutzlösung auf, bei welcher der Nutzer selbstbestimmt über den Umgang mit „seinen" Daten entscheiden kann.

1 Einleitung

Weitergehende Informationen zu Tracking

Tracking und Identifikation:

- Bewegungsdaten nicht anonym

  Zang, Bolot: Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study, MobiCom 2011


Anonymization of Location Data Does Not Work:
A Large-Scale Measurement Study

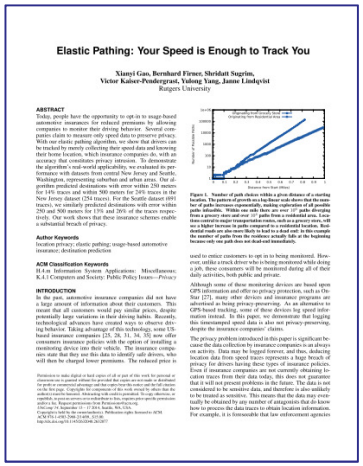
- Ermittlung eines Reiseziels durch Analyse des Fahrverhaltens

  Dewri et al.: Inferring Trip Destinations from Driving Habits Data, WPES 2013


Inferring Trip Destinations From Driving Habits Data

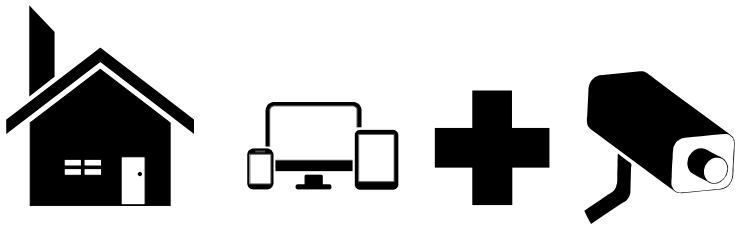
- Tracking bei Kenntnis nur eines Ortes und der Geschwindigkeiten

  Gao et al.: Elastic Pathing: Your Speed is Enough to Track You, UbiComp 2014


Elastic Pathing: Your Speed is Enough to Track You

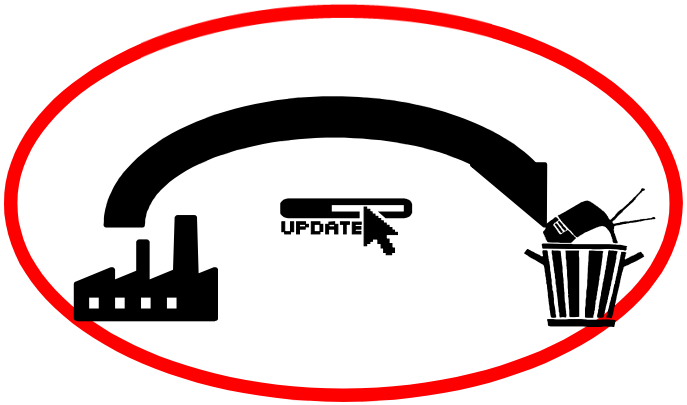
Verstecktes Internet

1. Smart home, Smart TV, Assisted Living,



2. Smart Mobility

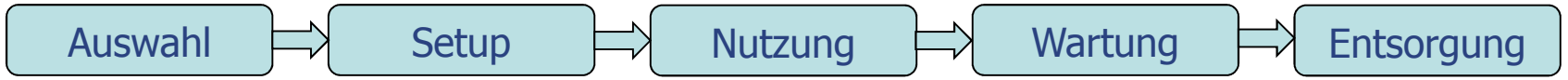
3. **IoT Lebenszyklus**



Projekt Privacy&Us

- Marie Curie Förderprojekt mit 13 Stipendiaten europaweit
- Privacy&Us => Datenschutz und Usability
- Datenschutz soll umsetzbar, anwendbar, einfach werden
- Forschungsschwerpunkt am ULD: Internet of Things

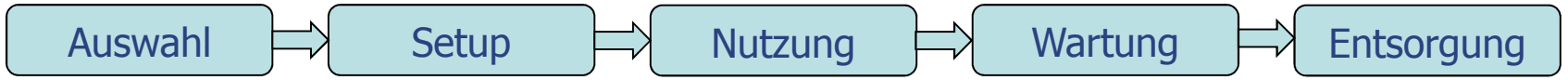
IoT-Lebenszyklus



- Nutzersicht
  - Was tun Anwender?
  - Was glauben Anwender, dass das Device tut?

- Datensicht
  - Was passiert mit den Daten?
  - Was tut das Device?

IoT-Lebenszyklus



- Hypothesen der Umfrage
  - Nutzer sehen IoT Geräte in ihrem bisherigen Kontext als Sachen, nicht als Computer.
  - Nutzer behalten IoT Geräte auch wenn diese in Ihre Privatsphäre eingreifen
    - wenn diese besonders teuer waren.
    - wenn sie eine emotionale Bindung an das Gerät haben.

Umfrageteilnehmer

Geschlecht	
männlich	57%
weiblich	38%
ohne Angabe	5%

Alter	
21..30	52%
31..40	28%
41..50	8%

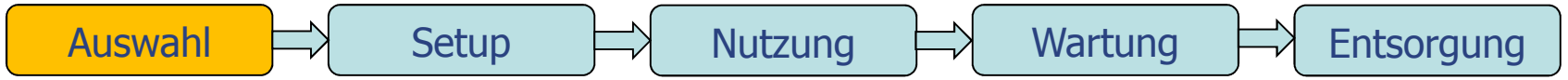
Herkunft	
Osteuropa	45%
Westeuropa	31%
Nordamerika	14%

Computererfahrung	
Experte	55%
Mit Erfahrung	37%
Anfänger	7%

Bildungsabschluss	
Bachelor	45%
Master	33%
Hochschulreife	8%
ohne Angabe	5%
Promotion	3%

IoT Besitz	
Kein Gerät	41%
Smart TV	38%
Smart watch	23%
Fitnessarmband	18%
Thermostat	12%
Stimmassistent	12%

Käuferwünsche

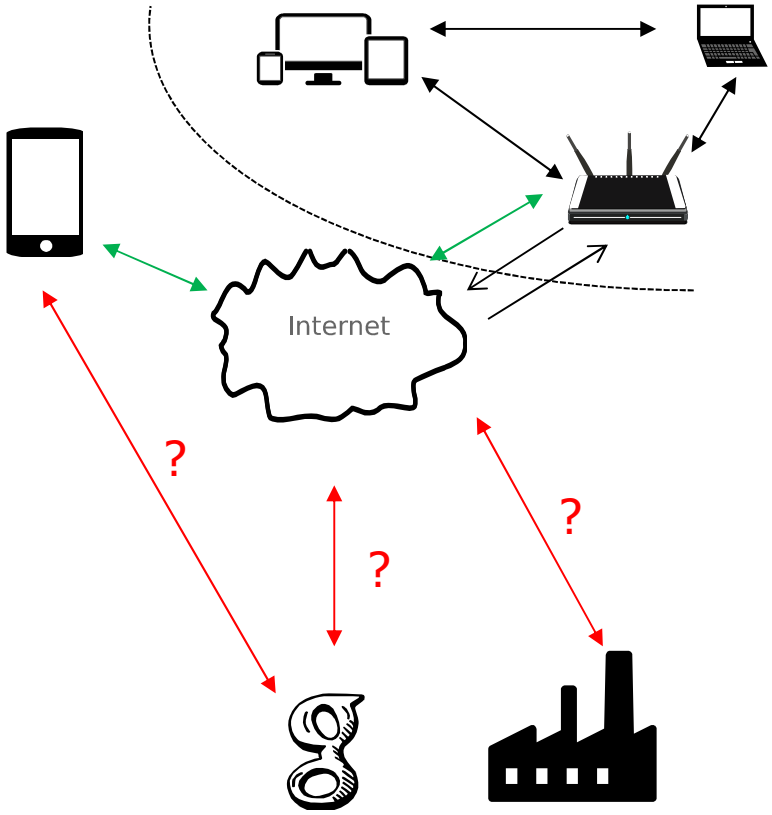


Käuferwünsche (Mehrfachantworten)	%
einfache Anwendbarkeit	72
Kompatibilität mit vorhandenen Geräten	66
guter Ruf der Marke	48
geringer Preis	47
klare Datenschutzerklärung	46
Empfehlung durch Bekannte	39
Design, Aussehen	35
Verfügbarkeit einer techn. Dokumentation	35
Zertifizierung, Gütesiegel	20
andere	8

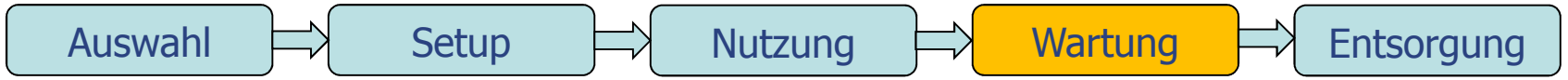
Auswahl: Datenschutzperspektive

Auswahl → Setup → Nutzung → Wartung → Entsorgung

- Packung sollte Datenflüsse und Risiken beschreiben
- Kann Gerät lokal betrieben werden?
- Welche Funktionalitäten bedürfen der Cloud?
- Datenflüsse in Drittstaaten



Wartung, Updates



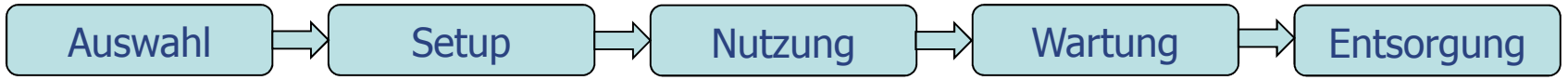
- Denken Sie, dass IoT Geräte Updates benötigen?

Option	%
Ja	92
Ich weiß nicht	5
Nein	3

- Wer sollte für die Updates verantwortlich sein?

Option	%
Hersteller	60
Eigentümer	44
Verkäufer	15
Eine Behörde	1
Ich weiß nicht	1

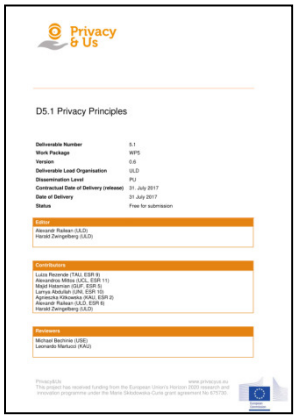
IoT Lifecycle



- Hypothesen der Umfrage
  - Nutzer sehen IoT Geräte in ihrem bisherigen Kontext als Sachen, nicht als Computer. falsifiziert
  - Nutzer behalten IoT Geräte auch wenn diese in Ihre Privatsphäre eingreifen
    - wenn diese besonders teuer waren. bestätigt
    - wenn sie eine emotionale Bindung an das Gerät haben. teilweise bestätigt, mehrheitlich weibliche Teilnehmerinnen

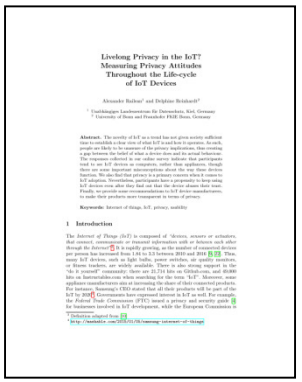
Weitergehende Informationen

- Privacy&Us D5.1 – Privacy Principles
  Veröffentlichung ausstehend
  https://privacyus.eu/publications/deliverables/


Privacy & Us

D5.1 Privacy Principles

- Railean, Reinhard,
  Livelong Privacy in the IoT?
  IFIP Summer School 2017, Ispra
  Veröffentlichung folgt
  https://www.datenschutzzentrum.de/projekte/privacy-us/


Livelong Privacy in the IoT?
Measuring Privacy Attitudes
Throughout the Life-cycle
of IoT Devices

Förderhinweise

Die Darstellung beruht auf Ergebnissen der Projekte

Forum Privatheit I & II

integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge

Privacy & Us

Selbstdatenschutz im vernetzten Fahrzeug

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Gefördert unter
MSCA-ITN-2015-ETN –
Marie Skłodowska-Curie
Innovative Training Networks
Projektnummer: 675730

www.forum-privatheit.de/
www.sedafa.de

https://fgvt.htwsaar.de/public/index.php/ikopa-2015-2018/

www.privacyus.eu

Zeit für Fragen und Diskussion

Kontakt:
Harald Zwingelberg
uld6@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1222

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein