Datenschutzfreundliche Vermessung und Auswertung persönlicher Daten mit Wearables zur Erhöhung der Arbeitssicherheit

Ergebnisbericht D4.1

State-of-the-Art-Bericht zu Privacy-UIs

Version	**1.0**
Datum	29.11.2022
Verfasser	Jannis von Albedyll (Fraunhofer IESE) Reinhard Schwarz (Fraunhofer IESE)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS1511K gefördert.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Ansprechperson

Reinhard Schwarz
Fraunhofer Institut für experimentelles Software Engineering IESE
Fraunhofer-Platz 1
67663 Kaiserslautern

E-Mail: reinhard.schwarz@iese.fraunhofer.de

Inhaltsverzeichnis

Liste der Abkürzungen

BMBF	Bundesministerium für Bildung und Forschung
DSGVO	Datenschutzgrundverordnung
P3P	Platform for Privacy Preferences
PET	Privacy-Enhancing Technology
PIMS	Personal Information Management Systems
TET	Transparency-Enhancing Technology
TTDSG	Telekommunikations-Telemedien-Datenschutzgesetzes
UI	User Interface

1 Bedeutung der Privacy-Nutzerschnittstelle für den Datenschutz

In dem Maße, wie IT-Anwendungen immer mehr persönliche Daten erheben und weiterverarbeiten, gewinnt der Datenschutz an Bedeutung. Anwender müssen nach geltendem Recht über datenschutzrelevante Aspekte eines Dienstes aufgeklärt werden und – sofern es keine andere, übergeordnete Rechtgrundlage für die Datenverarbeitung gibt – in die Verarbeitung einwilligen, und sie möchten oft auch genauer steuern können, in welchem Grade der Dienstleister über personenbezogene Daten verfügen darf. Um dem gerecht zu werden, bieten IT-Anwendungen oft spezielle Nutzerschnittstellen, sogenannte Privacy-UIs, die dem Anwender Einsicht und Kontrolle über die Verarbeitung seiner persönlichen Daten ermöglichen sollen.

1.1 Herausforderungen

Die Herausforderung bei Privacy-UIs besteht darin, eine positive User Experience bei hohem Schutz der Privatsphäre zu erzeugen. Dabei geht es nicht nur um Komfort und eine einfache Bedienbarkeit: Schon 2005 äußerte Zurko [1] die These, dass Probleme bei der Benutzung bestehender IT-Sicherheitsmechanismen deren Effektivität fundamental senken. Eine schlechte User Experience ist also sowohl unangenehm für den Benutzer als auch schädlich für die Sicherheit des Systems, welches er nutzt.

Bei der Konzeption einer Privacy-Nutzerschnittstelle geht es aber nicht nur darum, die Anwender durch eine einladende, bedienfreundliche Oberfläche dazu zu animieren, die verfügbaren Schutzmechanismen auch zu nutzen. Damit sie dies sinnvoll tun können, muss außerdem gewährleistet sein, dass die Bedienoberfläche dem Anwender auch klar signalisiert, wie die Datenschutzeinstellungen des Systems gerade sind, welche Schutzgarantien das System bietet und welche Datenschutzrisiken drohen (Transparenzaspekt). Außerdem sollte die Oberfläche möglichst reichhaltige Funktionen bieten, um Einfluss auf die Datenschutzmechanismen des Systems und damit auf dessen Datenschutzgarantien zu nehmen (Selbstbestimmungsaspekt).

1.2 Gliederung des Berichts

Dieser Bericht gibt einen Überblick über die Arbeiten auf dem Gebiet der Privacy-UIs. Dazu werden in Kapitel 2 zunächst relevante Akteure und Forschungsprojekte auf diesem Gebiet genannt. Anschließend gehen wir auf den spezifischen Kontext im WearPrivate-Projekt ein, das heißt Wearables im Arbeitsschutzkontext. In Kapitel 3 werfen wir einen kurzen Blick auf artverwandte Kontexte, in denen Privacy-UIs relevant sind.

In Kapitel 4 betrachten wir Ansätze, um Transparenz über die Rechtsgrundlage eines Systems – die Datenschutzerklärung des Dienstbetreibers – zu schaffen. Konkret beleuchten wir Arbeiten zu der Fragestellung, wie Datenschutzhinweise benutzerfreundlich gestaltet werden können.

In Kapitel 5 legen wir den Fokus auf die Fragestellung, wie der Anwender einfach und wirkungsvoll Einfluss auf die Datenschutzeinstellungen nehmen kann, um seine informationelle Selbstbestimmung auszuüben.

Kapitel 6 befasst sich mit dem Aspekt der benutzerfreundlichen Gestaltung von Security- und Privacy-Mechanismen. Zunächst werden hier allgemeine Prinzipien zur Entwicklung benutzerfreundlicher

Privacy-UIs genannt. Abschließend erläutern wir sogenannte Privacy Patterns, die konkretere Gestaltungsempfehlungen geben.

2 Player

Spätestens mit der Verabschiedung der Europäischen Datenschutzgrundverordnung ist die Bedeutung von angemessenem Datenschutz ins Bewusstsein der Diensteanbieter gerückt. Nicht nur die Forschung, sondern auch die Industrie hat sich daher in den letzten Jahren verstärkt dem Datenschutzthema zugewandt.

2.1 Forschung

Die Realisierung von Datenschutz und der Schutz der Privatsphäre in informationstechnischen Anwendungen wurde und wird in verschiedenen Forschungsprojekten thematisiert.

Das BMBF-geförderten Projekt TrUSD[1] (Laufzeit 09/2018 – 07/2021) befasste sich mit dem Datenschutz im Arbeitnehmerkontext. Die Zielsetzung war, mehr Transparenz für den Arbeitnehmer bei der Erhebung, Speicherung, Verbreitung und Nutzung persönlicher Daten am Arbeitsplatz zu schaffen und ihm zugleich Möglichkeiten zu bieten, seine Selbst- und Mitbestimmungsrechte wahrzunehmen. Dazu wurden im Projekt Methoden und Prozesse entwickelt, um die Anforderungen an den Arbeitnehmerdatenschutz systematisch zu erheben und ausgehend davon entsprechende Mechanismen zum Schutz der Privatsphäre abzuleiten. Ähnlich wie in WearPrivate sah TrUSD ein Privacy-Dashboard als ein Kernelement einer datenschutzfreundlichen Lösung vor. Das Dashboard soll dem Arbeitnehmer als zentrale Auskunftsinstanz in allen Fragen des Datenschutzes dienen und ist zugleich die universelle Schnittstelle, um in allen Unternehmensanwendungen persönliche Datenschutzpräferenzen vorzugeben. Dazu muss das Dashboard allerdings tief in die Unternehmens-IT integriert werden, um Zugriff auf alle relevanten Einstellungen zu haben.

Anders als im Projekt WearPrivate zielte das TrUSD-Szenario aber vornehmlich auf klassische Personalstammdaten oder Logdaten von Informationssystemen am Arbeitsplatz, nicht jedoch auf Wearable- oder gar dynamisch erhobene Gesundheitsdaten. Im Ergebnis konzipierte TrUSD auch eher Vorgehensmodelle für das Engineering solcher Privacy Dashboards als gebrauchsfertige Systemlösungen. Der Anspruch war eher, ein umfassendes Engineering-Framework für Arbeitnehmerdatenschutz zu entwickeln.

Viele der Ideen aus TrUSD greift das Projekt D'Accord[2] (Laufzeit 9/2021 – 8/2024) auf, das ebenfalls vom BMBF gefördert wird. Der Anwendungskontext sind hier digitale Ökosysteme, das heißt Systemverbünde von mehreren unabhängigen Partnern, die ein gemeinsames, umfassenderes Geschäftsmodell realisieren, in dem jeder Partner seine spezifische Rolle spielt. Gerade kleinere Partnerunternehmen in einem solchen Ökosystem empfinden den Datenschutz oft als Innovationsbremse und Geschäftshindernis. Daher wäre es erstrebenswert, eine Ökosystemplattform mit einem fertigen Werkzeugkasten auszustatten, der für die gängigen Fragen des Datenschutzes vorgefertigte Lösungsbausteine anbietet, die nachweislich den gesetzlichen Anforderungen genügen

[1] https://www.trusd-projekt.de/

[2] https://daccord-projekt.de/

und sich flexibel zu Geschäftsmodell-spezifischen Datenschutzlösungen kombinieren lassen. Wie in TrUSD ist auch hier ein Datenschutz-Cockpit ein wichtiger Lösungsbaustein. Das Cockpit ermöglicht es Geschäftspartnern des Ökosystems, geltende Datenschutzrichtlinien der Plattform schnell zu ermitteln und an geänderte Bedürfnisse anzupassen; zugleich ermöglicht es Endkunden, sich einen benutzerfreundlichen Überblick über die Datenschutzerklärung zu verschaffen und persönliche Privacy-Präferenzen einfach und nachvollziehbar einzustellen.

Die Arbeiten in D'Accord berühren das Vorhaben WearPrivate insoweit, als die Erhebung von Wearable-Daten zumeist an eine Cloud-Lösung geknüpft ist – allein schon, weil einige KI-basierte Analyseverfahren erheblichen Rechen- und Speicherbedarf haben und weil Unternehmen mit entsprechendem Know-how ihre mühsam trainierten Analysemodelle nur ungern aus der Hand geben. Daher könnte ein Datenschutz-Werkzeugkasten, wie ihn D'Accord ins Auge gefasst hat, eine große Hilfe sein, um die Privacy-Ziele in WearPrivate umzusetzen.

Das BMBF-geförderte Projekt InviDas [2] (Laufzeit 05/2020 – 04/2023) zielt auf den Datenschutz beim Einsatz von Smart Watches, Cardio-Sportuhren und Fitness-Trackern zur Erfassung und Analyse von Gesundheitsdaten. Anders als WearPrivate steht hier allerdings die private, individuelle Nutzung solcher Smart Wearables im Vordergrund, nicht der Einsatz im Arbeitsplatzkontext. Da die Daten zunächst nur zwischen Dienstanbieter und Nutzer geteilt werden, stellt sich die Situation hier juristisch etwas einfacher dar als am Arbeitsplatz, wo nicht uneingeschränkt von einer Freiwilligkeit der Dienstnutzung ausgegangen werden kann und wo die Daten – wenn auch nur in aufbereiteter Form – auch dem Arbeitgeber zugänglich gemacht werden sollen.

Das Hauptanliegen von InviDas ist es, den Anwender über die Übermittlung und Verwendung seiner Daten hinreichend zu informieren, ihm also den Inhalt der Datenschutzerklärung möglichst benutzerfreundlich zu vermitteln. Die Projektergebnisse zielen also vor allem auf Transparenz als *Voraussetzung* für Selbstbestimmungen. Besondere Innovationen zur *Ausübung* der informationellen Selbstbestimmung sind in InviDas hingegen eher zweitrangig; hier geht man offenbar davon aus, dass die Marktkräfte automatisch zu größerer Selbstbestimmung führen werden, sobald die Anwender in die Lage versetzt werden, die Angebote verschiedener Dienstleister besser zu verstehen und miteinander zu vergleichen. Ungenügender Datenschutz sollte dann von den Verbrauchern abgestraft werden, indem sie entsprechende Dienstleister meiden. WearPrivate setzt hier einen etwas anderen Schwerpunkt und zielt gleichermaßen auf Mechanismen für nachvollziehbaren Datenschutz (Transparenz) und für Einflussnahme des Arbeitnehmers (Selbstbestimmung).

Das BMBF-geförderte Projekt PERISCOPE[3] (Laufzeit 07/2021 – 06/2024) verfolgt einen Ansatz, der komplementär zu dem des Projekts D'Accord ist: Anstatt die Datenschutzherausforderungen moderner Online-Plattformen als gegeben hinzunehmen und sie technisch zu lösen, zielt PERSICOPE darauf, möglichst datenschutzfreundliche Geschäftsmodelle zu entwickeln, die nur geringe Anforderungen an den Datenschutz stellen. Zusätzlich zu den technischen Lösungen berücksichtigt das Projekt auch ökonomische Analysen, um privatsphärenfreundliche Geschäftsmodelle effizient zu entwickeln. Ähnlich wie in D'Accord soll auch in PERISCOPE – insbesondere für Start-up- und KMU-betriebene Plattformen – ein benutzerfreundliches und DSGVO-konformes Managementsystem für Betroffenenrechte entwickelt werden, das auf Transparenz und Intervenierbarkeit abzielt. Dazu soll offenbar eine Gesamtlösung konzipiert werden, und nicht wie in D'Accord ein flexibler Werkzeugkasten mit unabhängigen Lösungsbausteinen.

[3] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope

Der von PERISCOPE gewählte Grundansatz hat auch für WearPrivate insofern Bedeutung, als es im Arbeitsplatzkontext nicht nur darum geht, für alle Datenschutzprobleme eine Lösung zu finden; vielmehr kommt es auch darauf an, die betroffenen Arbeitnehmer davon zu überzeugen, dass der gewählte Lösungsansatz auch praktisch funktioniert und die Daten des Nutzers tatsächlich vor unerwünschtem Zugriff schützt. Arbeitnehmer werden einer Wearable-Lösung nur zustimmen, wenn man ihr Vertrauen in die Lösung gewinnen kann. Je privatsphärenfreundlicher sich die Architektur des Systems, seine dynamische Verarbeitungskette und das dahinterliegende Geschäftsmodell darstellen, umso eher werden Arbeitnehmer bereit sein, einen solchen Dienst zu verwenden.

Mit dem Aspekt benutzerfreundlicher Maßnahmen zum Schutz der Privatsphäre befassen sich neben den genannten befristeten Forschungsvorhaben auch verschiedene Forschungsgruppen. Die Forschungsgruppe SECUSO[4] am Karlsruher Institut für Technologie verfolgt den interdisziplinären Ansatz »Human Centered Security and Privacy by Design«, bei dem Informatiker, Mathematiker und Psychologen zusammenarbeiten, um fundierte und zugleich benutzerfreundliche Security- und Privacy-Technologien zu entwickeln. Die Arbeitsgruppe hat sich unter anderem auch mit Privacy Friendly Apps für einen verbesserten Privatsphäreschutz auf dem Smartphone befasst, die sich dadurch auszeichnen, dass sie nur die unbedingt erforderlichen Berechtigungen anfordern und auf jegliches Tracking verzichten. Die Sammlung von Anwendungen wird als Open Source Software bereitgestellt und unterliegt einer gemeinsamen Datenschutzerklärung.

Die Arbeitsgruppe »Sicherheit in Geschäftsprozessen«[5] (Business Process Security) der Universität Freiburg untersucht Architekturen und Mechanismen zur Durchsetzung und Auditierung von Sicherheits- und Datenschutzrichtlinien in verteilten Systemen. Sie hat sich unter anderem mit Transparency-Enhancing Technologies (TETs) befasst [3]. Die dazu konzipierten Dashboards zielen weniger auf Selbstbestimmung und Steuerung, sondern eher auf eine Offenlegung der Privacy-Eigenschaften. In einer anderen Arbeit hat das Forscherteam auch eine Klassifizierung von Privacy-Dashboards vorgeschlagen [4] und die Nutzerakzeptanz von einer Google-Dashboard-Lösung untersucht [5].

Die Forschungsgruppe PRISEC[6] an der Karlstad-Universität in Schweden befasst sich gezielt mit Privacy-Enhancing Technologies (PETs) und deren Usability-Aspekten, um Privacy und Transparenz im Cloud Computing zu verbessern. Forscher der Karlstad-Universität haben unter anderem »Data Track« entwickelt, ein Werkzeug, mit dem Anwender die bei einem Internet-Dienst gespeicherten persönlichen Daten herunterladen und visualisieren können, um sich einen Überblick darüber zu verschaffen, wie tief der Dienst in ihre Privatsphäre eindringt.

2.2 Industrie

Anbieter von Internetdiensten sind im Grundsatz zwar daran interessiert, möglichst viele Informationen über ihre Kunden zu sammeln, um ihre Produkte und ihr Marketing bestmöglich an die Kundenbedürfnisse anzupassen. Allerdings müssen sie sich in Europa auf die Anforderungen der DSGVO einstellen, und eine allzu große »Neugier« ihrer Dienste kann abschreckend auf die Kundschaft wirken. Daher hat auch die Industrie begonnen, sich eingehender mit der Gestaltung von Privacy-UIs

[4] https://secuso.aifb.kit.edu/

[5] https://www.telematik.uni-freiburg.de/forschung

[6] https://www.kau.se/en/cs/research/research-areas/privacy-and-security-prisec/prisec-privacy-and-security

zu beschäftigen. Ein transparenter Umgang mit den persönlichen Daten, eine benutzerfreundliche Schnittstelle für die Wahl der persönlichen Privacy-Präferenzen und ein auf Datensparsamkeit getrimmter Prozess wirken vertrauensbildend und können gegenüber Mitbewerbern einen Wettbewerbsvorteil bieten.

Forscher der Mozilla Corporation, der TU Berlin und der Telekom Innovation Labs konzipierten ein Privacy Dashboard, um Nutzern mobiler Endgeräte mehr Transparenz und informationelle Selbstbestimmung zu bieten [6]. Sie nutzten einen nutzerzentrierten Ansatz, bei dem ausgehend von einer initialen Erhebung der Nutzerbedürfnisse verschiedene technische Lösungsvorschläge erarbeitet wurden, die dann von den Anwendern bewertet wurden. Anhand der Testergebnisse und Nutzerbefragungen wurde das Konzept in mehreren Iterationen verfeinert. Das Dashboard bot vor allem folgende Funktionalitäten: Kontrolle über verlorene oder gestohlene Endgeräte (Lokalisation und Sperren aus der Ferne); Geo-Location Privacy (Ortsdaten verweigern, Genauigkeit verringern, willkürliche Ortsangaben ermöglichen); Datenfluss-Transparenz der mobilen Applikationen (Welche Informationen werden geteilt, wann und warum?); Privatsphäre-freundlicher Gast-Account für verliehene Geräte (eingeschränkter Zugriff auf Apps, Daten und Einstellmöglichkeiten des Endgeräts). In diesem Forschungsprojekt lag der Schwerpunkt weniger auf den Design-Aspekten für maximale Verständlichkeit der Schnittstellenfunktionen und Privacy-Attribute, sondern eher in der Ermittlung grundlegender Privacy-Funktionen, auf die Anwender besonderen Wert legen – wie zum Beispiel das Verschleiern der Geo-Lokation oder die Übersicht über die Datenflüsse der genutzten Apps.

Auch Unternehmen wie Garmin haben erkannt, dass Anwender bessere Transparenz und Selbstbestimmung in Bezug auf ihre persönlichen Daten zu schätzen wissen und langfristig honorieren, wenn Diensteanbieter diesem Wunsch entgegenkommen. Deshalb beteiligt sich Garmin auch aktiv an Forschungsprojekten wie InviDas [2], um den Nutzern von Fitness-Trackern bessere Privacy-Informationen für wohlfundierte Datenschutzentscheidungen zu geben.

Gerade für gefahrenträchtige Tätigkeitsfelder gewinnen tragbare Monitoring- und Tracking-Lösungen an Bedeutung – etwa im Bergbau, in der Seefahrt, auf Großbaustellen oder auf Bohrinseln sowie bei militärischen Einsätzen. Zahlreiche Anbieter liefern Lösungen, um die physische oder auch psychische Verfassung der eingesetzten Kräfte und deren Umweltbedingungen kontinuierlich zu überwachen oder ihren Aufenthaltsort zu bestimmen [7][8].[7] In einigen Bereichen, wie etwa dem Tagebau in den USA, ist es sogar vorgeschrieben, die Beschäftigten mit Standort-Trackern auszustatten, um in Gefahrenbereichen rechtzeitig vor anwesenden Personen zu warnen oder bei Unfällen alle Betroffenen schnell aufspüren zu können. Da der Einsatz dieser Technik oft auf gesetzlichen Anforderungen beruht oder vor allem in Ländern mit geringen Datenschutzauflagen üblich ist, ist die Privacy-Schnittstelle solcher Systeme meist nur schwach ausgeprägt und der Anwender hat kaum Einflussmöglichkeiten, was die Verwendung seiner persönlichen Messdaten betrifft. Als wesentlicher Schutz der Privatsphäre sehen viele Systeme gerade einmal eine verschlüsselte Übertragung zwischen dem Wearable und dem auswertenden Vorgesetzten oder Betriebsarzt vor; auf eine weitergehende, auch innerbetriebliche Datennutzungskontrolle wird in der Regel verzichtet. Umfragen zeigen jedoch, dass Arbeitnehmer durchaus daran interessiert sind, wie ihre Daten genutzt werden, und dass sie gerne mehr Einfluss auf die Erhebung und Nutzung nehmen würden [9].

[7] Siehe etwa http://www.solepowertech.com/, https://www.optalert.com/industries/mining-transport/ oder https://www.guardhat.com/

3 Datenschutzkontext

3.1 Wearables für den Arbeitsschutz

Eine quantifizierte Arbeitswelt wirft einige Konflikte auf: Auf der einen Seite besteht die Gefahr zunehmender Überwachung im Arbeitskontext, auf der anderen Seite stehen immer mehr Freiheiten der Arbeitnehmer. Arbeitnehmern, die ihre Arbeit mit wachsendem Stress verbinden, stehen jene gegenüber, die personalisiertes Selbstmanagement und Monitoring anstreben [10].

Gerade Wearables ermöglichen dabei ein hohes Maß an möglicher Quantifizierung im Kontext des Arbeitsschutzes: So beschreiben Svertoka et al. [8] 20 Metriken, die zu einer höheren Arbeitsplatzsicherheit beitragen können. Diese Metriken unterteilen sich in solche, die sich auf ein Individuum beziehen (z. B. Blutdruck, Herzfrequenz, Glukosespiegel im Blut) und solche, die sich auf die Umgebung beziehen (z. B. Luftqualitätsindex, Lichtintensität, Temperatur, Lautstärke). Durch diese Metriken können Wearables laut den Autoren folgende vier Kernfunktionen ermöglichen oder unterstützen:

- Monitoring
- Supporting
- Training
- Tracking

Zu diesen Kernfunktionen benennen die Autoren zehn konkretere Subfunktionen, wie etwa die Überwachung und Kontrolle von Vitalparametern der Arbeiter mittels Fitness-Trackern oder ähnlichen Geräten.

Auch offene technische Herausforderungen bei der Nutzung von Wearables werden genannt. Darunter fallen technologische Herausforderungen (z. B. Lokalisierungsprobleme), soziale Herausforderungen (z. B. sozialer Widerstand), ökonomische Herausforderungen (z. B. hohe Kosten eingesetzter Wearables) oder datenbezogene Herausforderungen (z. B. Ort der verarbeitenden Logik). Privatheit und IT-Sicherheit werden als eine querschnittliche Herausforderung genannt.

Maltseva [11] stellt eher die sozialen Herausforderungen in den Vordergrund. So könnten Wearables unter anderem ein stärkeres Ungleichgewicht der Macht im Unternehmen herbeiführen, die Glaubwürdigkeit eines Unternehmens beschädigen und Unternehmen die Menschen noch mehr als Ressource ansehen lassen. Als Lösungsansätze schlägt die Autorin unter anderem vor, einen Ort zum kritischen Reflektieren der Daten zu schaffen. Außerdem sollten Angestellte zumindest einen Teil der genutzten Metriken selbst aussuchen dürfen. Auch eine kritische Diskussion über Wearables und deren Nutzen sollten Unternehmen ermöglichen und den Dialog aktiv fördern.

Etwas konkretere Empfehlungen zum erfolgreichen Einsatz von Wearables am Arbeitsplatz geben Jacobs et al. [12]:

- Es sollten solche Anwendungsfälle zur Verbesserung der Arbeitssicherheit mithilfe von Wearables bevorzugt werden, bei denen Daten nur am Arbeitsplatz gesammelt werden.
- Ein positives Sicherheitsklima sollte im Unternehmen vorangetrieben werden.
- Das Vertrauen der Arbeitnehmer in den Nutzen der Wearables sollte mit ausreichend Evidenz oder konkreten Belegen gestärkt werden.

- Arbeitnehmer sollten in den Prozess der Auswahl und Implementierung der Wearable-Technologie eingebunden und stets darüber informiert werden.

Die bisher genannten Empfehlungen zielen vor allem auf Arbeitgeber ab, um das Vertrauen der Arbeitnehmer in den Einsatz von Wearables am Arbeitsplatz zu stärken. Tindale et al. [9] nehmen hingegen eine breitere Perspektive ein. Sie sehen das Hauptproblem zwar auch beim Vertrauen der Arbeitnehmer in die Technologie und deren vertrauensvolle Verwendung durch den Arbeitgeber, geben aber neben Empfehlungen für den Arbeitgeber auch Empfehlungen für Arbeitnehmer und politische Entscheidungsträger:

- Verantwortlichkeiten der Arbeitgeber (Auszug):
  - Offene und transparente Informationsbereitstellung über die Nutzung der Sensordaten
  - Kommunikation der Intensionen, warum und wie Sensordaten genutzt werden sollen
  - Klare Grundsätze für den Fall, dass Gesundheitsdaten mit Hinweisen auf den Gesundheitszustand des Betroffenen gefunden werden
  - Schutz der Privatsphäre und Privatheit
  - Gewährleisten einer sicheren Datenspeicherung
- Verantwortlichkeiten der Arbeitnehmer (Auszug):
  - Verstehen der Unternehmensgrundsätze zum Sammeln und Nutzen von Sensordaten
  - Verstehen der Prozesse rund um Datenschutz, Datentransfer und Privatsphäre
- Verantwortlichkeiten der politischen Entscheidungsträger (Auszug):
  - Bereitstellung von aktuellen Empfehlungen für den datenschutzkonformen Wearable-Einsatz am Arbeitsplatz
  - Regulatorischen Rahmen zum Nutzen von Fitnessprodukten, die einen Einfluss auf die Gesundheit haben könnten

3.2 Verwandte Kontexte

3.2.1 Industrie 4.0

In Anwendungen der Industrie 4.0 werden umfangreiche Daten über Produktionsprozesse erhoben. Diese verraten mitunter auch sehr viel über die Mitarbeiter, die an diesen Produktionsprozessen beteiligt sind. Daher sollten die Betroffenen Klarheit darüber haben, inwieweit die Produktionsüberwachung auch ihre Privatsphäre betrifft, und im Zweifelsfall sollten sie über die Erhebung und Nutzung der Daten mitentscheiden, um ihren persönlichen Datenschutz zu gewährleisten.

Mannhardt et al. [13] betrachten das Problem, dass bei der Erfassung von Maschinen- und Produktionsdaten auch viele Informationen über die Beschäftigten gewonnen werden können, die in diesem Industrie4.0-Umfeld tätig sind. Dies gefährdet die Privatsphäre der Mitarbeiter, aber andererseits muss auch ein ausgewogener Kompromiss für die Nutzung der Prozessdaten gefunden werden, um die Vorteile einer datengetriebenen, flexiblen Prozesssteuerung heben zu können.

In [13] betrachten die Autoren als Anwendungsfall die Nutzung von Technologien, die die physischen und kognitiven Fähigkeiten der Beschäftigten erweitern, unter anderem, indem sie körperliche und geistige Ermüdung erkennen und entsprechende Gegenmaßnahmen vorschlagen. Um die Daten der

Betroffenen zu schützen, schlagen die Autoren ein Trust & Privacy Framework vor. Technisches Kernstück des Frameworks ist ein Privacy Dashboard, mit dem die Arbeitnehmer die Verwendung ihrer Daten kontrollieren und steuern können.

In mehreren Workshops untersuchte Mannhardt mit seinen Kollegen die Bedürfnisse der Arbeitnehmer. Dabei stellte er fest, dass sich die Dateneigentümer weniger für die subtilen Details der Datenanalyse interessieren, sondern vor allem für den Trade-off zwischen Privacy-Risiken und potenziellem eigenen Nutzen einer Freigabe persönlicher Daten. Dementsprechend vereinfachten die Autoren ihr Framework und reduzierten es auf wenige grundlegende »Touchpoints« (Abbildung 1).

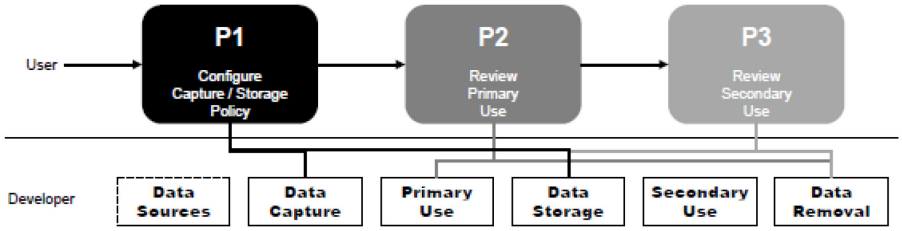

Abbildung 1 Touchpoints für ein Privacy-Dashboard entlang des Datenlebenszyklus' (Quelle: [13])

An den genannten Punkten P1, P2 und P3 sehen die Autoren folgende Kontrollmöglichkeiten im Lebenszyklus der persönlichen Daten vor:

- P1: Configure Capture and Storage Policy
  - Konfigurieren der Policy für die Datenerfassung
  - Konfigurieren der Policy für die Hauptnutzung der Daten
  - Konfigurieren der Policy für die Datenspeicherung
  - Konfigurieren der Policy für die Zweitverwertung der Daten
  - Konfigurieren der Policy für die Datenlöschung
- P2: Review Primary Use
  - Überprüfung und Überwachung der Datenerfassung
  - Überprüfung und Überwachung der Datenhauptnutzung
- P3: Review Secondary Use
  - Überprüfung und Überwachung der Datenspeicherung
  - Überprüfung und Überwachung der Daten-Zweitverwertung

Um die Kontrollmöglichkeiten durchzusetzen, werden jeweils zwischen den Verarbeitungsschritten entlang des Lebenszyklus technische Checkpoints eingefügt, an denen der Nutzer über die Auswahl und Zugriffsrechte der Daten entscheiden kann. Dabei geht es zum einen um die Entscheidung, welche Daten überhaupt erfasst werden sollen und zu welchen Zwecken sie zugreifbar gemacht werden sollen; zum anderen geht es darum, im Nachhinein nachvollziehen zu können, welche Datennutzung tatsächlich stattgefunden hat, um selbst Aufsicht über den bestimmungsgemäßen Gebrauch der Technik zu führen. Die Autoren betonen, wie wichtig es ist, dass das Dashboard den Anwendern ein klares Lagebild vermittelt, damit sie wohlfundierte Privacy-Entscheidungen treffen können. Leider enthält die Veröffentlichung [13] nur das Konzept, aber noch keine konkrete technische Umsetzung des Dashboards. Die vorgesehene Gestalt der Privacy-UI erschließt sich daraus noch nicht.

3.2.2 Automotive

Moderne Fahrzeuge erfassen eine Vielzahl von Messwerten, die Rückschlüsse auf den Betriebs- und Wartungszustand des Fahrzeugs, seinen Aufenthaltsort, die Fahrzeuginsassen und die Fahrweise des Fahrers ermöglichen. Zudem sind Fahrzeuge in zunehmendem Maße mit ihrer Umwelt und mit anderen Fahrzeugen vernetzt; sie geben ihre Telemetriedaten an externe Empfänger weiter. Hinzu kommt, dass Fahrzeuge sich auch mit anderen IT-Geräten der Insassen – insbesondere mit Mobiltelefonen – verbinden und auf diesem Wege zahlreiche persönliche oder personenbeziehbare Daten aufnehmen, etwa Adressverzeichnisse oder persönliche Konfigurationseinstellungen für Sitze, Spiegel oder Infotainment.

Nutzt der Fahrzeuginsasse entsprechende Fahrzeugfunktionen, um zum Beispiel ein persönliches Nutzerprofil einzustellen, zu navigieren, ortsgebundene Dienste zu nutzen, aufgrund defensiver Fahrweise einen vergünstigten Versicherungstarif in Anspruch zu nehmen oder Bezahlvorgänge abzuwickeln, so hinterlässt dies im Fahrzeug Datenspuren, die erhebliche Einblicke in das Verhalten und in die Identität der Person ermöglichen. Leider sind sich die wenigsten Nutzer über die vielfältigen Daten bewusst, die das Fahrzeug erfasst und zum Teil auch an Dritte weiterleitet, und kaum ein Laie macht sich klar, wie tief solche Daten – selbst scheinbar rein technische Messwerte – in die Privatsphäre der Nutzer hineinreichen.

Da das Fahrzeuginnere von den meisten Nutzern als sehr persönlicher Privatbereich empfunden wird, steht die Automobilindustrie also vor einer sehr großen Herausforderung: Zum einen sollte das Fahrzeug die komplexe Datenerfassung für den Fahrzeugnutzer transparent machen, zum anderen sollte es dem Nutzer aber auch eine vollständige Kontrolle darüber zu ermöglichen und die Abwägung, für welche Zwecke er unter welchen Umständen welche Daten in welcher Tiefe wem zur Verfügung stellen möchte.

Im Automobilkontexttreten dabei ähnliche Probleme auf wie bei WearPrivate im Arbeitsplatzkontext:

- Der Fahrzeugnutzer will das Fahrzeug als Fortbewegungsmittel nutzen. Im Allgemeinen hat er weder die Muße noch die Kompetenz, sich intensiv mit Datenschutzangelegenheiten zu befassen, ähnlich wie ein Arbeitnehmer in einem IT-fernen Arbeitsumfeld.
- Obwohl Datenschutzpräferenzen mitunter sehr situationsabhängig sein können, bietet das Steuern eines Fahrzeugs ähnlich wie intensive berufliche Tätigkeiten wenig zeitliche und motorische Spielräume, sich während der Fahrt Datenschutzhinweisen oder Fehlermeldungen des Fahrzeugs auseinanderzusetzen oder komplexe Datenschutzregeln vorzugeben. Die Aufmerksamkeit des Nutzers muss immer überwiegend auf die Haupttätigkeit gerichtet bleiben, dem Steuern des Fahrzeugs. Es bleiben nur geringe Kapazitäten, sich um informationelle Selbstbestimmung zu kümmern.
- Der Druck eines Autokäufers, beim Erwerb des Fahrzeugs schnell einer Reihe von Einverständniserklärungen zuzustimmen, um den Neuerwerb in vollem Umfange erproben und nutzen zu können, ist erheblich. Kaum ein Verkäufer wird sich die Mühe machen, dem Kunden alle Risiken und Nebenwirkungen solcher Entscheidungen darzulegen. Dies ist vergleichbar mit dem sozialen Druck, dem ein Arbeitnehmer in Datenschutzangelegenheiten ausgesetzt ist, und der mangelnden Bereitschaft vieler Führungskräfte, sich auf langwierige Erläuterungen und Diskussionen zu diesem Thema einzulassen.

Die Datenvielfalt bei vernetzten Fahrzeugen ist insgesamt größer als beim Einsatz von Vitaldaten-Wearables im Arbeitsumfeld, so wie im Projekt WearPrivate vorgesehen. Insoweit sind die Anforderungen an entsprechende Privacy-Benutzerschnittstellen im Fahrzeugumfeld in Bezug auf Transparenz und Selbstbestimmung noch höher als in WearPrivate, auch wenn Vitaldaten einen höheren Schutzbedarf haben als Kontakt-, Bewegungs- und Verhaltensdaten, wie sie im Fahrzeug potenziell anfallen.

Im Forschungsprojekt »Selbstdatenschutz im vernetzten Fahrzeug«[8] (SeDaFa), Laufzeit 01/2016 – 12/2017), einem vom BMBF geförderten Verbundprojekt, wurden die Anforderungen an die datenschutzfreundliche Gestaltung einer Fahrzeug-Nutzerschnittstelle untersucht und Lösungen dafür evaluiert. Im Rahmen des Projekts wurden auch verschiedene Studien zu den Bedürfnissen, den Datenschutzvorbehalten und dem technischen Vorwissen der Fahrzeugnutzer ausgewertet. Dabei zeigte sich, wie schwer es ist, für eine heterogene, oft nicht IT- oder Datenschutz-affine Zielgruppe und die harten Usability-Anforderungen des Fahrbetriebs dennoch geeignete Mechanismen bereitzustellen, um für ausreichende Transparenz und Selbstbestimmung zu sorgen. Die Veröffentlichungen von SeDaFa bieten einen guten Überblick über den Stand der Forschung auf diesem Gebiet.

[8] https://sedafa-projekt.de/

4 Transparenz

4.1 Darstellung der Rechtslage

Komplexe rechtliche Sprache sowie lange Texte führen dazu, dass Nutzer Datenschutzerklärungen nicht lesen [14]. Deshalb ist ein gängiger Ansatz vieler Dienstanbieter, die Datenschutzerklärungen in Kurzform zu präsentieren. Im Kontext von Wearables macht dies beispielsweise Polar mit einem eigenen Absatz »Verwendung der Polar Dienste kurz erklärt« [15] innerhalb der Datenschutzerklärung. Hingegen setzt Garmin auf eine eigene Seite mit kurzen Erläuterungen, in denen Nutzer dann auf die vollständigen Datenschutzrichtlinien hingewiesen werden [16]. Diesen Trend bestätigen Gluck et al. [17]. Kurztexte in natürlicher Sprache werden eher gelesen als Langtexte. Eine Möglichkeit, Datenschutzerklärungen zu straffen, ist das Weglassen von gängigen Praktiken und Informationen, die Nutzer ohnehin schon als gegeben annehmen und antizipieren.

Die Frage, wie Datenschutzhinweise präsentiert werden sollen, versuchen Ebert et al. [18] zu beantworten. In ihrem Experiment zeigte sich, dass exklusiv präsentierte Datenschutzhinweise (d. h. auf einer eigenen Seite präsentiert) in Tests zur Erinnerung der Inhalte am besten abschneiden. Verglichen dazu schneiden Informationen, die in die Anwendung integriert sind (z. B. bei einer App an einem Feature, einem Button oder Ähnlichem platziert) etwas schlechter ab. Am schlechtesten schneiden Datenschutzhinweise ab, die erst mit einer Aktion (wie einem Klick) geöffnet werden müssen.

Schließlich gehen Reinhardt et al. [19] der Frage nach, ob eine visuelle Darstellung von Datenschutzhinweisen einer textuellen überlegen ist. Verglichen wurden

a) eine interaktive visuelle Darstellung, also eine Matrix mit Opt-Out-Möglichkeiten
b) ein sog. Privacy Policy Nutrition Label, also eine reine visuelle Darstellung ähnlich einer Matrix oder Tabelle
c) eine textuelle Langfassung

Während die interaktive visuelle Darstellung (a) dazu führte, dass Nutzer mehr Zeit mit der Datenschutzerklärung verbrachten als bei den anderen beiden Darstellungsformen, wies sie bei vielen Werten – etwa wahrgenommener Transparenz, Effizienz oder Attraktivität – keinen Vorteil gegenüber der rein visuellen Darstellung (b) auf. Beide visuelle Darstellungen, egal ob interaktiv oder nicht, schnitten allerdings bei den meisten Messgrößen besser ab als eine textuelle Langfassung der Datenschutzhinweise (c). Offen bleibt hier der Vergleich von Mischformen und der Vergleich mit einer textuellen Kurzfassung.

Das InviDas-Projekt [2] hat sich intensiv mit einer geeigneten Darstellungsform für die Datenschutzerklärung auseinandergesetzt. Im Ergebnis entstanden geraffte Ansichten zu den verschiedenen Datenpunkten und den dafür jeweils geltenden Regeln (Abbildung 2 und Abbildung 3).

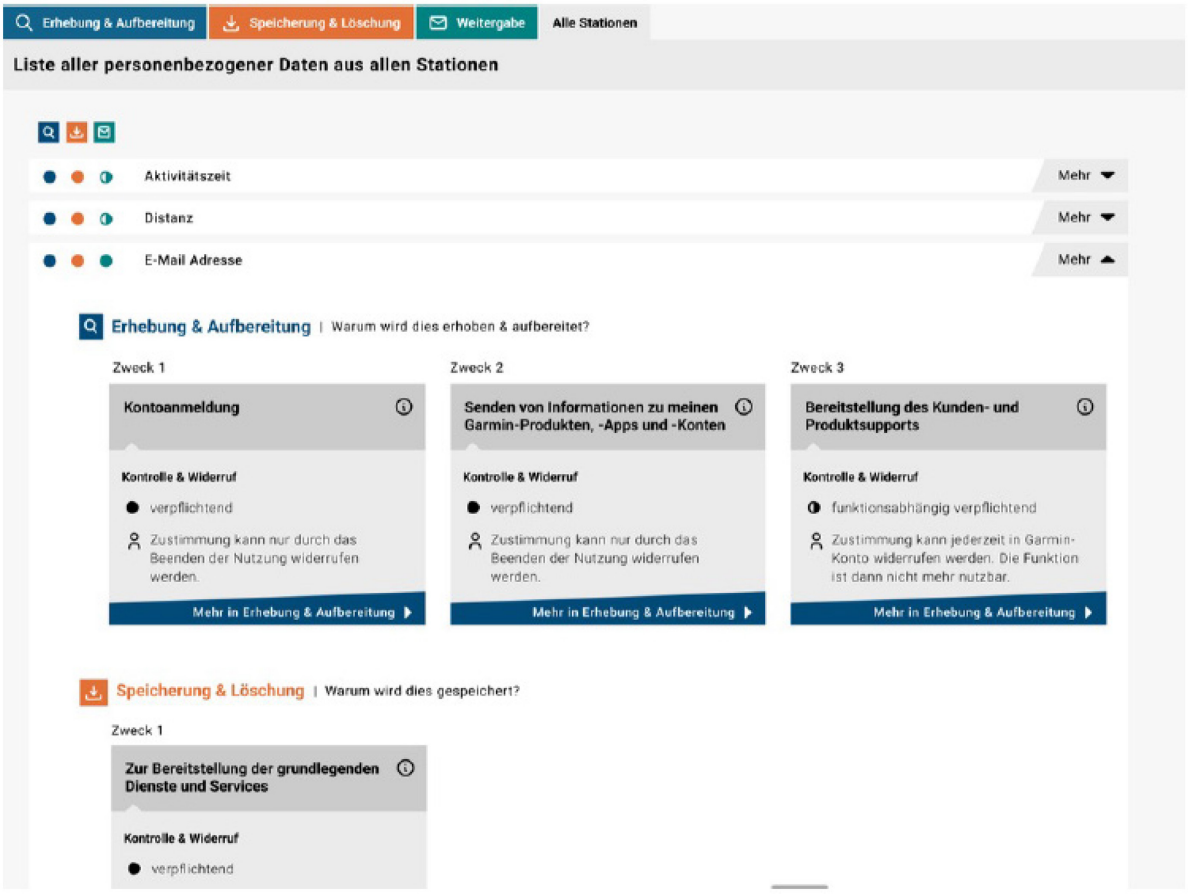

Abbildung 2 Übersicht über die Privacy-relevanten Datenpunkte: Vorschlag des InviDas-Projekts [2]

Das InviDas-Konzept sieht vor, die Informationen aufzuschlüsseln nach

- Erhebung und Aufbereitung
- Speicherung und Löschung
- Weitergabe

der geschützten Daten. Zu jedem Datenpunkt und zu jedem der drei Gesichtspunkte stellt das Dashboard dann kompakte Informationsboxen bereit, die dem Nutzer die grundlegenden Bestimmungen der Datenschutzerklärung zu diesem Datenpunkt in Stichwörtern darlegen.

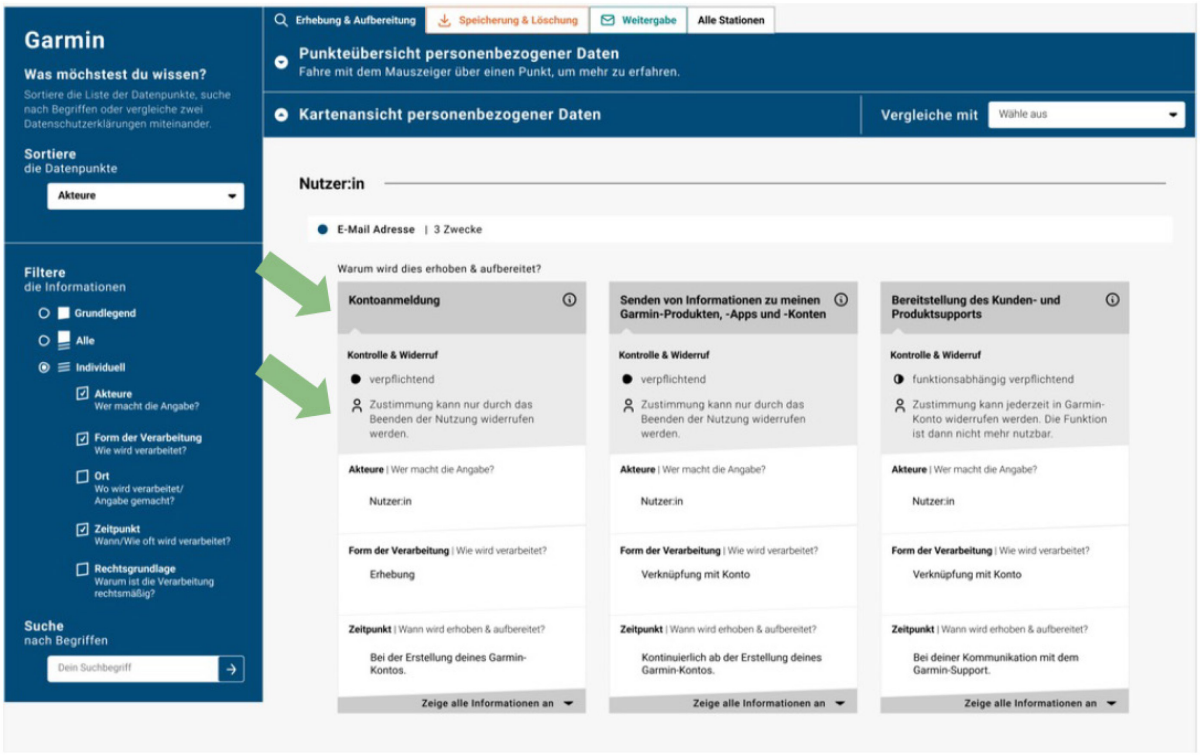

Abbildung 3 Darstellung des Erhebungszwecks: Vorschlag des InviDas-Projekts [2]

4.2 Darstellung der Privacy-Einstellungen

Eine Darstellung wie etwa die Entwürfe des InviDas-Projekts (Abbildung 2 und Abbildung 3) ist nicht darauf beschränkt, eine statische Datenschutzerklärung mit starren Regeln zu visualisieren. Sie lässt sich auch nutzen, um zu jedem Datenpunkt die vom Nutzer wählbaren Policy-Optionen anzubieten und deren Auswirkungen zu erläutern. Die einzelnen Policy-Schalter sind dann allerdings nicht zentral in einer Ansicht versammelt, sondern ihrem jeweiligen Wirkungsbereich zugeordnet. Für Power-User, die sich auskennen und ohne langwieriges Navigieren schnell mehrere Einstellungen ändern wollen, kann man ergänzend zur Datenpunkt-Sicht auch eine Gesamtübersicht aller Policy-Optionseinstellungen anbieten.

Im einfachsten Fall bietet eine solche Schnittstelle nur die gewählten dynamisch konfigurierbaren Privacy-Optionen. Besser ist es, zu jeder Einstellung auch die genauen Konsequenzen zu erläutern

- in Bezug auf die damit einhergehenden (Rest-)Risiken für die Privatsphäre sowie
- in Bezug auf die damit verbundenen Einbußen an Dienstqualität und Benutzerfreundlichkeit.

Vor allem der erste Punkt stellt oft eine Herausforderung dar, weil selbst einem menschlichen Beobachter nicht immer vollständig bewusst ist, welche Auswirkungen die Preisgabe bestimmter Daten haben kann. Die genauen Risiken hängen zum einen vom Anwendungskontext ab, weil viele Daten erst durch zusätzliches Kontextwissen relevante Informationen preisgeben. Zum anderen ist auch der Angreifer zu berücksichtigen: Je kompetenter und entschlossener ein Angreifer ist und je mehr Ressourcen er zur Verfügung hat, umso eher kann er in die Privatsphäre eines Nutzers eindringen. Die Risikoeinschätzung ändert sich daher je nach dem angenommenen Angreifer-Modell. Daher tun sich die meisten IT-Anwendungen schwer damit, den Einfluss ihrer Systemeinstellungen auf die Privatsphäre genau zu deklarieren.

5 Selbstbestimmung

Eine wichtige Voraussetzung für informationelle Selbstbestimmung ist Transparenz. Nur wenn der Anwender sich über die potenziellen Privacy-Risiken im Klaren ist, kann er fundierte Entscheidungen treffen, ob und inwieweit er einen Dienst nutzen will. Allerdings reichen die in Kapitel 4 skizzierten Ansätze nicht aus, denn viele Dienste lassen dem Anwender keinen Spielraum für eine ausgewogene Abwägung von Risiken und Nutzen: Der Anwender muss den Dienst entweder akzeptieren, wie er ist, oder er muss auf die Nutzung vollständig verzichten.

5.1 Privacy-Optionen

Besser ist es, dem Anwender abgestufte Grade von Datenschutz im Austausch für abgestufte Grade von Dienstnutzen anzubieten. Der Anwender kann dann gewisse Datenverarbeitungen einschränken zum Schutz seiner Privatsphäre, muss aber im Gegenzug Einbußen bei den Leistungen und der Benutzerfreundlichkeit des Dienstes hinnehmen. Im einfachsten Fall bietet ein Dienst einfach eine Reihe von Privacy-Optionen an, die der Nutzer wählen oder ausschlagen kann.

Ein Problem solch einfacher Auswahlmenüs besteht darin, dass der Anwender oft nicht versteht, welche genauen Konsequenzen seine Wahl hat und welche genauen Privacy-Risiken sich hinter bestimmten Optionen verbergen. Ein anderes Problem ist die Wahl des Abstraktionsgrades: Eine allzu feingliedrige Auswahl an Optionen überfordert Anwender mit geringem IT- oder Domänenwissen; allzu simple Einstellmöglichkeiten (z. B. »Privacy: low / medium / high«) genügen nicht den Ansprüchen kundiger Power-User.

5.2 Policy-Editor

Um unterschiedlichen Nutzergruppen angemessene Mitgestaltungsmöglichkeiten bei der Auswahl ihrer Privacy-Policy zu geben, empfehlen sich maßgeschneiderte Policy-Editoren. Sie ermöglichen dem Anwender im Idealfall, seine Wünsche auf einer ihm angemessenen, wählbaren Abstraktionsebene auszudrücken, und übersetzen die gewählten Präferenzen in eine Maschinen-verwertbare Spezifikation. Leistungsfähige Editoren unterstützen dabei unterschiedliche Nutzergruppen durch jeweils angepasste Editor-Modes (z. B. »Beginner / Advanced / Expert«).

Ein früher Versuch, dem Nutzer Privacy-Policy-Präferenzen besser zugänglich zu machen, war Privacy Bird von Cranor et al. [20]. Dieses Werkzeug basiert auf dem P3P-Standard (Platform for Privacy Preferences) des World Wide Web Consortiums. Es ermöglicht dem Anwender zum einen, seine Privacy-Präferenzen in verständlicher Form auszudrücken (Abbildung 4) und leitet daraus eine formale P3P-Policy-Spezifikation ab. Zum anderen vergleicht es die Policy-Eigenschaften von Webseiten, die ihre Datenschutzerklärung mittels P3P formalisiert haben, mit den vom Nutzer angegebenen Vorlieben und warnt, wenn die Policy einer Seite mit den eigenen Präferenzen unverträglich ist (Abbildung 5).

Kolter und Pernul [21] greifen die Ideen von Privacy Bird auf. Ihre Kritik an diesem Werkzeug ist die mangelnde Nutzerfreundlichkeit und Verständlichkeit, gerade für unerfahrene Nutzer. Daher schlagen sie ein verbessertes, ebenfalls P3P-basiertes Werkzeug vor, das gegenüber Privacy Bird folgende Vorzüge aufweist:

- Unterschiedliche Menüs für unterschiedliche Nutzergruppen (Anfänger, Fortgeschrittene, Experte)

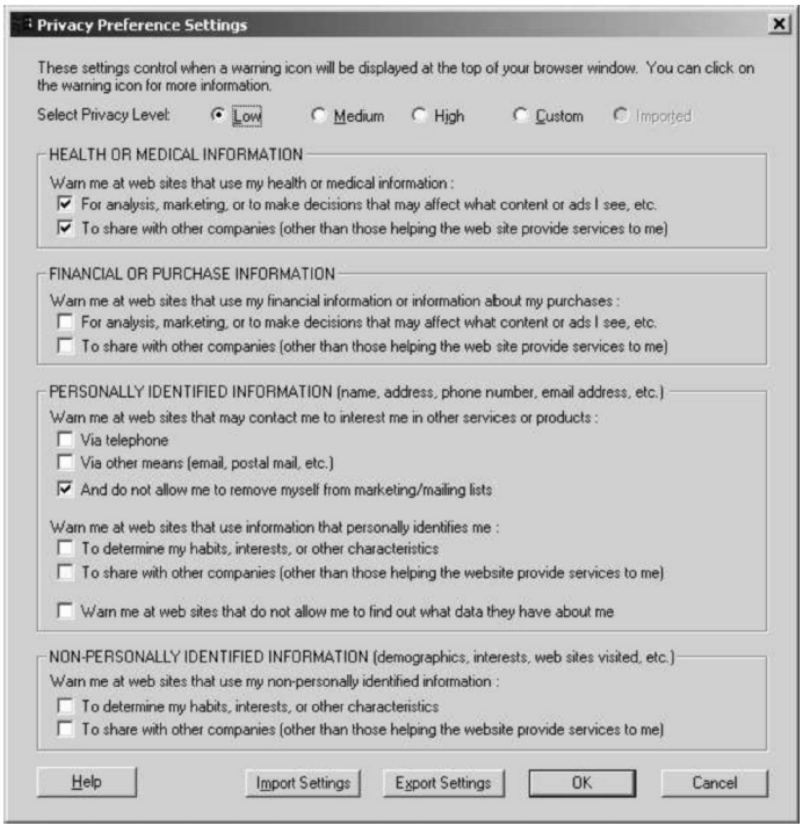

Abbildung 4 Privacy Bird: Panel zum Spezifizieren der eigenen Privacy-Präferenzen (Quelle: [20])

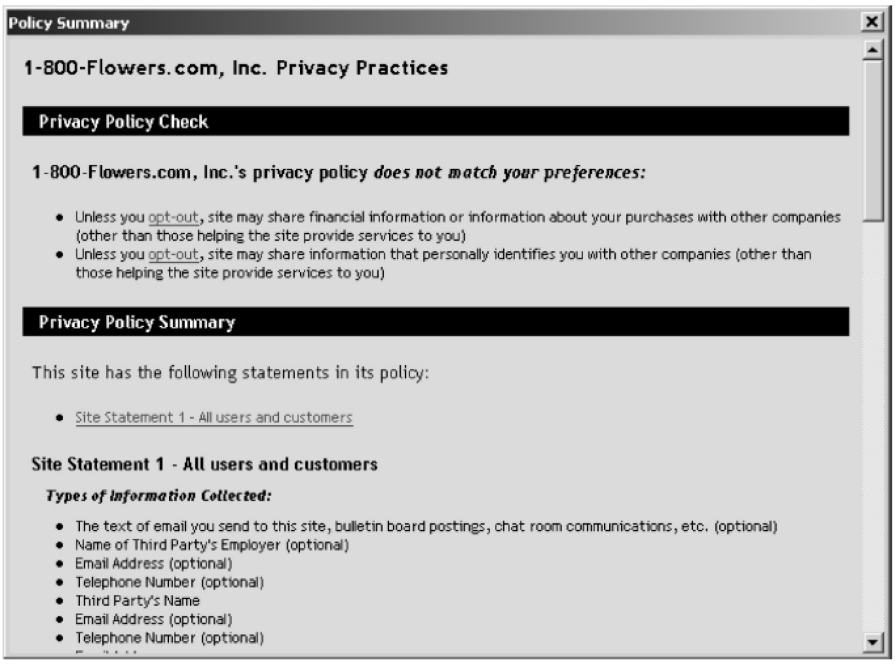

Abbildung 5 Privacy Bird: Inkompatibilitätswarnung bei Unverträglichkeit einer Seiten-Policy mit den eigenen Privacy-Präferenzen (Quelle: [20]).

- Zwölf vorgefertigte Service-Kategorien (z. B. Webmail, Online-Banking, Online-Shopping, Social Networking Portals, eGovernment) mit jeweils Dienst-spezifischer Konfigurationsmöglichkeit
- Vordefinierte Datentypen für häufig genutzte persönliche Informationen (z.B. Login-Daten, E-Mail-Daten, Adressdaten, Finanzdaten), für die voreingestellte Policy-Präferenzen hinterlegt werden können
- Vordefinierte Datennutzungs-Kategorien neben der originären Diensterbringung (z. B. Personalisierung der Webschnittstelle, Kontaktaufnahme mit dem Kunden), für die voreingestellte Policy-Präferenzen hinterlegt werden können
- Policy-Präferenzen für die Offenlegung von Daten gegenüber Dritten

Für einen schnellen Überblick über alle Einstellungen sehen die Autoren ein Policy-Cockpit vor, dass für jede Dienstkategorie und jede Datennutzungskategorie einen Privacy Score berechnet, der als Farbskala (grün bis rot) intuitiv den Grad der Privacy-Bedrohung signalisiert (Abbildung 6).

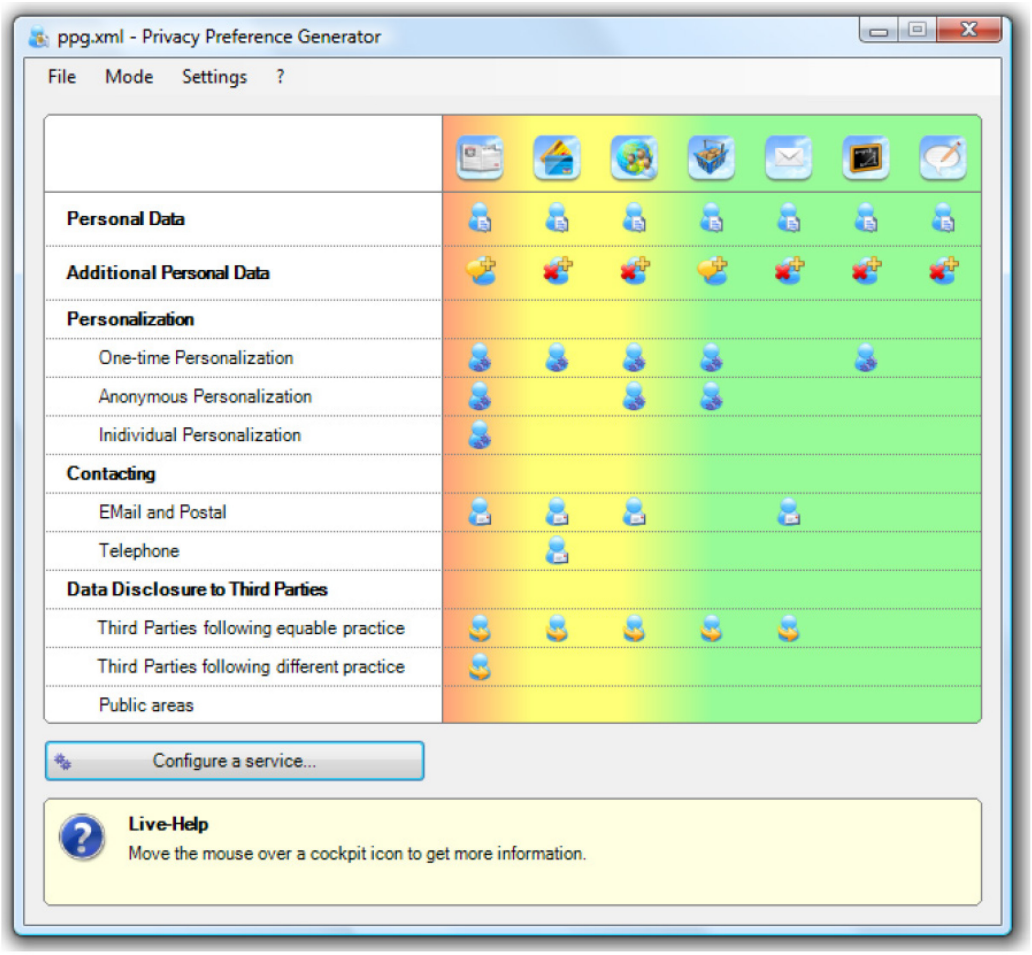

Abbildung 6 Privacy Cockpit – Übersicht über die gewählten Präferenzen und deren Sicherheitsniveau.

5.3 Personal Information Management Systems

Personal Information Management Systems (PIMS) sind Dienste zur Einwilligungsverwaltung. Sie dienen dazu, dem Einzelnen einen Überblick und die Kontrolle über die Nutzung seiner persönlichen

Daten zu verschaffen [22]. PIMS sind zwischengeschaltete Dienste, die in der Regel nicht vom datenschutzrechtlich Verantwortlichen selbst betrieben werden, sondern von einem Treuhänder. Dies hat den Vorteil, dass die vom Nutzer gewählten Präferenzen nur einmal vorgenommen werden müssen und dann bei verschiedenen Dienstnutzungen immer wieder verwendet werden können, ohne sie jedes Mal neu einstellen zu müssen. Dies soll dem sogenannten »Consent Fatigue« vorbeugen, einer zunehmenden Abstumpfung der Anwender vor immer häufigeren Zustimmungsanfragen – etwa im Zusammenhang mit Cookie-Berechtigungen. Ausdrückliche Regelungen zu PIMS wurden auch in § 26 des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) aufgenommen. Der § 26 TTDSG reguliert die sogenannten »anerkannten Dienste« der Einwilligungsverwaltung und in diesem Zuge insbesondere die hierfür zu erfüllenden Anforderungen Es gibt allerdings keine Pflicht der Anbieter, sich nach § 26 TTDSG anerkennen zu lassen.

Grundsätzlich können PIMS so gestaltet werden, dass sie auf dem Endgerät des Nutzers ausgeführt werden, etwa im Browser des Anwenders; dies ist die datenschutzfreundlichste Lösung. Als Alternative können PIMS auch als Cloud-Dienst im Internet realisiert werden. Dann liegen die Einwilligungsdaten jedoch beim PIMS-Betreiber, und der Anwender hat keine unmittelbare Kontrolle mehr darüber, an wen und wann die Daten übermittelt werden; zudem muss der Cloud-Dienst den Nutzer authentisieren, das heißt, der Nutzer benötigt ein PIMS-Nutzerkonto. Dafür können die präferierten Datenschutzeinstellungen unabhängig von einem bestimmten Endgerät genutzt werden.

Übergreifende Einwilligungen für unterschiedliche Dienste zu erteilen ist jedoch nicht unproblematisch:

- Will man die zulässigen Dienste nicht eindeutig mittels einer Positiv-Liste festlegen, so kann die Einwilligung den datenschutzrechtlich Verantwortlichen nicht in die Entscheidung mit einbeziehen, was rechtlich fragwürdig ist, denn eigentlich widerspricht dies den gesetzlichen Anforderungen an eine ausreichende Bestimmtheit der Einwilligung und an die Informationspflichten über die Verantwortlichen.
- Nutzt man andererseits eine zuvor genau definierte Positiv-Liste (»Whitelisting«), dann schränkt dies den Nutzen von PIMS erheblich ein, denn für Dienste, die nicht gelistet sind, erteilt das PIMS keine Einwilligungen.
- In der Praxis ist es auch nicht ganz einfach, alle in Frage kommenden Zwecke der Datenverarbeitung eindeutig und vollständig zu spezifizieren. Da jeder Dienst seine Besonderheiten hat, kann die globale Einwilligung in eine bestimmte Verarbeitungskategorie oder für bestimmte Datenkategorien leicht unvorhergesehene Nebenwirkungen haben.

Inzwischen gibt es kommerzielle Anbieter für PIMS-Lösungen und auch Non-Profit-Konsortien, die solche Lösungen vorantreiben [23]. Allerdings finden sich kaum freie Quellen zu den Gestaltungsdetails der Benutzerschnittstellen dieser Systeme.

6 Usable Privacy

IT-Sicherheit und Datenschutz entfalten nur dann ihre Wirkung, wenn Nutzer die vorhandenen Mechanismen auch einsetzen. Leider sind einige Datenschutzlösungen so hinderlich, dass Anwender dazu neigen, sie zu ignorieren oder sogar aktiv zu umgehen. Daher ist der Aspekt der Usability zentral für den Erfolg von Datenschutzmaßnahmen.

6.1 User Experience im Privacy-Kontext

Laut Zurko [1] ist insbesondere der Abgleich zwischen dem Security-Modell eines Produkts oder Tools mit dem mentalen Security-Modell des Nutzers eine große Herausforderung bei der nutzerzentrierten IT-Sicherheit. Die Lösung dieser Herausforderung sieht Zurko unter anderem in der Anwendung von Design- und Testprinzipien aus dem Human-Computer-Interaction-Bereich auf Sicherheitssysteme. Dies wirft die Frage auf, welche Designprinzipien beim Entwickeln von Lösungen zur IT-Sicherheit oder zum Schutz der Privatsphäre des Nutzers besonders wichtig sind.

Mit dem Design von IT-Sicherheitssystemen beschäftigten sich etwa Reeder et al. [24]. Sie untersuchten eine Anwendung zum Erstellen von Privacy Policies im betrieblichen Kontext und fanden ihrerseits fünf elementare Herausforderungen und resultierende Ratschläge bei der Benutzung und dem Design solcher Software:

- Unterstützung der Gruppierung von Objekten
- Erzwingen konsistenter Terminologie
- Erläuterung von Default-Regeln
- Kommunizieren und Erzwingen von Mindestschutzanforderungen
- Vorbeugen von Regel-Konflikten

Wenngleich diese Punkte wie Empfehlungen für ein sinnvolles Design solcher Anwendungen klingen, so stellen sie vom Standpunkt der Autoren Herausforderungen dar. Welche Technik beim Visualisieren und Gruppieren von Regel-Objekten am sinnvollsten ist oder wie Regel-Konflikte am besten vermieden werden können, wird nämlich nicht eindeutig beantwortet. Dennoch sollten diese Punkte bei der Konzeption von Privacy-Anwendungen betrachtet werden.

Einen etwas anderen Anwendungsfall untersuchten Kuo et al. [25]. Während es hier zwar um die Konfiguration von mobilen Endgeräten und WLANs ging, stand die Anwendbarkeit durch durchschnittlichen Konsumenten ohne Spezialkenntnisse im Vordergrund. Die zentrale Herausforderung aus ihrer Sicht ist, dass Konfigurationen funktionsbasiert arbeiten, während Nutzer eher zielbasiert denken und handeln. Das Ergebnis ihrer Studie waren fünf Designprinzipien zur Entwicklung von benutzerfreundlichen Security-Anwendungen:

- Nimm an, dass Benutzer kein technisches Wissen und keine Expertise besitzen.
- Minimiere menschlichen Aufwand, maximiere die (automatisierte) Arbeit der Anwendung.
- Unterstütze eine positive User-Experience.
- Antizipiere Fehlerfälle.
- Separiere verschiedene Konzepte.

Wenngleich sich diese Prinzipien auf Security-Anwendungen und nicht auf Privacy-Anwendungen beziehen, können sie darauf übertragen werden. So könnte der menschliche Aufwand minimiert werden, indem entweder eine Art Privacy-Wizard eingesetzt oder ein Privacy-First-Ansatz genutzt wird, also maximale Privacy als Default.

Die Idee, mit einem Privacy-Wizard den menschlichen Aufwand für die Konfiguration komplexer Policies zu reduzieren, untersuchten Fang und LeFevre [26]. Hierfür nutzten sie ein Machine-Learning-Modell, welches auf dem Active-Learning-Paradigma basiert. Als Input für das Modell sammelten sie limitierte Nutzerdaten mithilfe eines Wizards. Diese Daten stellten die Trainingsdaten des Modells dar, mit welchem wiederum die detaillierten Privacy-Policies eines sozialen Netzwerks für den entsprechenden Nutzer konfiguriert werden konnten. Sie konnten so feststellen, dass der Active-Learning-Wizard sehr detaillierte Privacy-Einstellungen vornehmen konnte und dafür nur einen sehr limitierten Input brauchte. Somit wurde das oben genannte Prinzip »minimiere menschlichen Aufwand, maximiere die Arbeit der Anwendung« in die Tat umgesetzt.

6.2 Privacy Patterns

Angelehnt an Software-Design-Patterns existieren sogenannte Privacy-Patterns. Die Patterns dienen dazu, eine standardisierte Sprache zu schaffen und ähnliche Problemlösungen zu bündeln. Dadurch wollen die Autoren Entwicklern helfen, Bedenken bezüglich der Privatsphäre zu adressieren und juristische Vorgaben in der Software mit standardisierten Methoden umzusetzen [27].

Bei der Auflistung solcher Privacy-Patterns fällt allerdings auf, dass verschiedene Abstraktionsebenen existieren. Während beispielsweise »Protection against Tracking« [28] ein eher allgemeines Problem adressiert und technisch aufwändig umzusetzen ist, lässt sich »Icons for Privacy Policies« [29] leicht technisch realisieren. Dennoch bieten die Patterns einen guten Anhaltspunkt für Gute Praxis und werden deutlich konkreter als die in der Forschung genannten Prinzipien (siehe Abschnitt 6.1.). Somit könnten sie sich als praxistauglicher erweisen, wenn es um die konkrete Entwicklung von Privacy-UIs geht.

Während sich einige Patterns auf gängigen Plattformen und in üblichen Sammlungen für Design Patterns finden [30], hat sich privacypatterns.org [27] auf eben solche Privacy Patterns spezialisiert. Tabelle 1 zeigt eine Übersicht über gängige Patterns von privacypatterns.org, gruppiert nach Kategorien (Mehrfachnennung von Patterns in unterschiedlichen Kategorien ist möglich).

Tabelle 1 Exemplarische Privacy Patterns, vorgeschlagen von privacypatterns.org [27]

Kategorie	Gängige Patterns
Control	Encryption with user-managed keys, Discouraging blanket strategies, Reciprocity, Incentivized participation, Outsourcing [with consent], Personal data store, Sign an agreement to solve lack of trust on the use of private data context, Single point of contact, Enable/Disable functions, Obtaining explicit consent, Decoupling [content] and location information visibility, Selective access control, Pay back, Negotiation of privacy policy, Reasonable level of control, Masquerade, Buddy list, Lawful consent, Informed consent for web-based transactions, [Support] Selective disclosure, Private link, Active broadcast of presence
Abstract	Location granularity
Separate	Personal data store, User data confinement pattern, Anonymous reputation-based blacklisting

Kategorie	Gängige Patterns
Hide	Encryption with user-managed keys, Use of dummies, Pseudonymous messaging, Onion routing, Pseudonymous identity, Aggregation gateway, Anonymous reputation-based blacklisting, Added-noise measurement obfuscation, Attribute based credentials, Trustworthy privacy plug-in, Anonymity set
Minimize	Protection against tracking, Strip invisible metadata, Added-noise measurement obfuscation, Attribute based credentials
Inform	Minimal Information asymmetry, Informed secure passwords, Awareness feed, Who's listening, Privacy policy display, Layered policy design, Asynchronous notice, Abridged terms and conditions, Policy matching display, Ambient notice, Dynamic privacy policy display, Privacy labels, Data breach notification pattern, Trust evaluation of services sides, Privacy icons, Privacy-aware network client, Informed implicit consent, Privacy color coding, Appropriate privacy icons, Icons for privacy policies, Privacy mirrors, Appropriate privacy feedback, Impactful information and feedback, Platform for privacy preferences, Privacy dashboard, Preventing mistakes or reducing their impact, Informed credential selection, Privacy awareness panel, Privacy aware wording, Personal data table, Informed consent for web-based transactions, Increasing awareness of information aggregation, Unusual activities
Enforce	Federated privacy impact assessment, Identity federation, Do not track pattern, Obligation management, Sticky policies

Leider beschreiben die genannten Patterns nur das prinzipielle Vorgehen, zeigen aber keine konkrete Umsetzung in einer Nutzerschnittstelle. Zudem ist der Abstraktionsgrad bei vielen Patterns recht hoch, oft zu hoch für eine direkte Umsetzung. So besagt etwa das Pattern »Awareness Feed«, dass man den Nutzer über die möglichen Schlussfolgerungen, die aus seinen Daten gezogen werden können, informieren soll. Es ist aber im Allgemeinen sehr schwer, diese Konsequenzen genau zu ermitteln; ebenso schwer kann es sein, die gezogenen Schlussfolgerungen einem unerfahrenen Anwender verständlich darzulegen.

7 Fazit

Mit der wachsenden Bedeutung von IT-Sicherheit und Datenschutz wächst der Bedarf für nutzerfreundliche Bedienschnittstellen, die auch einem unerfahrenen, IT-fernen Anwender Transparenz in Bezug auf seine Sicherheitsrisiken und informationelle Selbstbestimmung bieten. In den letzten Jahren gab es zahlreiche Forschungsarbeiten und Systemlösungen, die sich mit diesem Problem auseinandergesetzt haben.

Trotz vieler Vorschläge, hilfreichen Designprinzipien und Entwurfsmustern erfüllt der Stand der Technik die Erwartungen bisher nur unzureichend. Noch immer erhält der Anwender nur lückenhafte, oft schwer verständliche Einsichten in die Verarbeitung seiner persönlichen Daten und die damit verbundenen Privacy-Risiken. Und noch immer sind die Möglichkeiten des Anwenders, Einfluss auf die Privacy-Eigenschaften von IT-Systemen zu nehmen, ziemlich begrenzt, oft mit starken Komforteinbußen verbunden und in vielen Fällen eher Technik- als Nutzer-zentriert. Zudem konzentrieren sich viele Forschungsbeiträge eher nur auf Konzepte und Prinzipien, ohne eine konkrete Realisierung ihrer Ideen vorzulegen, die man mit Nutzern in der Praxis evaluieren könnte.

Quellenverzeichnis

[1] Zurko, Mary Ellen (2005): User-Centered Security: Stepping Up to the Grand Challenge. Proceedings 21st Annual Computer Security Applications Conference (ACSAC'05), 187–202. DOI: 10.1109/CSAC.2005.60

[2] InviDas Projekt-Home Page (2022): Gesellschaft für Informatik e.V. https://invidas.gi.de/

[3] Zimmermann, Christian & Accorsi, Rafael (2013):Transparenz durch Privacy Dashboards: Ein Process Mining Ansatz. INFORMATIK 2013 – Informatik angepasst an Mensch, Organisation und Umwelt. Bonn: Gesellschaft für Informatik e.V. 2087–2101. https://dl.gi.de/handle/20.500.12116/20641

[4] Zimmermann, Christian & Accorsi, Rafael & Müller, Günter (2014): Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy. Proceedings - 9th International Conference on Availability, Reliability and Security (ARES 2014), 152-157. DOI: 10.1109/ARES.2014.27

[5] Johana Cabinakova, Johana & Zimmermann, Christian & Müller, Günter (2016): An Empirical Analysis of Privacydashboard Acceptance: The Google Case. Proceedings European Conference on Information Systems (ECIS 2016), Research Papers, 114. http://aisel.aisnet.org/ecis2016_rp/114

[6] Piekarska, Marta & Zhou, Yun & Strohmeier, Dominik & Raake, Alexander (2015): Because we care: Privacy Dashboard on FirefoxOS. Proceedings of the 9th Workshop on Web 2.0 Security and Privacy (W2SP 2015), arxiv.org/abs/1506.04105

[7] Pantelopoulos, Alexandros & Bourbakis, Nikolaos G. (2010): A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis. IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews 40(1), 1–12. 10.1109/TSMCC.2009.2032660

[8] Svertoka, Ekaterina & Saafi, Salwa & Rusu, Alexandru & Burget, Radim & Ion, Marghescu & Hosek, Jiri & Ometov, Aleksandr (2021). Wearables for Industrial Work Safety: A Survey. Sensors 21(11). DOI: 10.3390/s21113844

[9] Tindale, Lauren & Chiu, Derek & Minielly, Nicole & Hrincu, Viorica & Talhouk, Aline & Illes, Judy (2022): Wearable Biosensors in the Workplace: Perceptions and Perspectives. Frontiers in Digital Health 4. DOI: 10.3389/fdgth.2022.800367

[10] Moore, Phoebe & Piwek, Lukasz (2017): Regulating wellbeing in the brave new quantified workplace. Employee Relations 39(3), 308–316. 10.1108/ER-06-2016-0126

[11] Maltseva Reiby, Kateryna (2020): Wearables in the workplace: The brave new world of employee engagement. Business Horizons 63(4), 493–505. DOI: 10.1016/j.bushor.2020.03.007

[12] Jacobs, Jesse & Hettinger, Larry & Huang, Yueng-Hsiang & Jeffries, Susan & Lesch, Mary & Simmons, Lucinda & Verma, Santosh & Willetts, Joanna (2019): Employee acceptance of wearable technology in the workplace. Applied Ergonomics 78, 148–156. DOI: 10.1016/j.apergo.2019.03.003

[13] Mannhardt, F. & Oliveira, M. & Petersen, S.A. (2020): Designing a Privacy Dashboard for a Smart Manufacturing Environment. In: I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, and M. Mäntymäki (Eds.): Digital Transformation for a Sustainable Society in the 21st Century, IFIP Advances in Information and Communication Technology 573, Springer, 79–85. DOI: 10.1007/978-3-030-39634-3_8

[14] Milne, George & Culnan, Mary (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices. Journal of Interactive Marketing 18(3), 15–29. DOI: 10.1002/dir.20009

[15] Siehe https://www.polar.com/de/legal/privacy-notice#toc1

[16] Siehe https://www.garmin.com/de-DE/privacy/global/, Abruf am 21.09.2022.

[17] Gluck, Joshua & Schaub, Florian & Friedman, Amy & Habib, Hana & Sadeh, Norman & Cranor, Lorrie Faith & Agarwal, Yuvraj (2016). How short is too short? Implications of length and framing on the effectiveness of privacy notices. Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security (SOUPS '16), 321–340.

[18] Ebert, Nico & Ackermann, Kurt & Scheppler, Björn (2021). Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–12. 10.1145/3411764.3445516

[19] Reinhardt, Daniel & Borchard, Johannes & Hurtienne, Jörn (2021). Visual Interactive Privacy Policy: The Better Choice? Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–12. 10.1145/3411764.3445465

[20] Cranor, Lorrie Faith & Guduru, Praveen & Arjula, Manjula (2006): User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction 13(2), 135–178. 10.1145/1165734.1165735

[21] Kolter, J. & Pernul, G. (2009): Generating User-Understandable Privacy Preferences. International Conference on Availability, Reliability and Security (ARES 2009), 299–306. 10.1109/ARES.2009.89

[22] Salemi, Simone (2022): Chancen und Risiken von PIMS nach §26 TTDSG. Datenschutz und Datensicherheit (DuD) 46, 505–510. 0.1007/s11623-022-1648-x

[23] European Data Protection Supervisor, Attoresi, M. & Moraes, T., EDPS TechDispatch (2020): Personal Information Management Systems. Issue 3, 2020. 10.2804/11274

[24] Reeder, Robert & Karat, Clare-Marie & Karat, John & Brodie, Carolyn (2007). Usability Challenges in Security and Privacy Policy-Authoring Interfaces. Human-Computer Interaction – INTERACT 2007. Lecture Notes in Computer Science 4663, 141–155. 10.1007/978-3-540-74800-7_11

[25] Kuo, Cynthia & Goh, Vincent & Tang, Adrian & Perrig, Adrian & Walker, Jesse (2005). Empowering Ordinary Consumers to Securely Configure their Mobile Devices and Wireless Networks. Report CMU-CyLab-05-005, Carnegie Mellon University, Pittsburg PA

[26] Fang, Lujun & LeFevre, Kristen (2010). Privacy Wizards for Social Networking Sites. Proceedings of the 19th International Conference on World Wide Web, 351–360. 10.1145/1772690.1772727

[27] Siehe https://privacypatterns.org, abgerufen am 11.11.2022.

[28] Siehe https://privacypatterns.org/patterns/Protection-against-tracking, Abruf am 11.11.2022.

[29] Siehe https://privacypatterns.org/patterns/Icons-for-Privacy-Policies, Abruf am 11.11.2022.

[30] Siehe http://www.welie.com/patterns/ oder https://ui-patterns.com/patterns/, Abruf am 11.11.2022.