Erhebung und Nutzbarmachung zusätzlicher Daten – Möglichkeiten und Risiken

24

Kai Rannenberg

Inhaltsverzeichnis

K. Rannenberg (✉)
Goethe-Universität Frankfurt, Deutsche Telekom Chair of Mobile Business and Multilateral Security, Deutschland
Kai.Rannenberg@m-chair.de

M. Maurer et al. (Hrsg.), *Autonomes Fahren*,
DOI 10.1007/978-3-662-45854-9_24,

24.1 Einführung: Autos, Freiheit und Datenschutz

Autos sind seit jeher ein Symbol für die Freiheit und Unabhängigkeit ihrer Benutzerinnen und Benutzer, seien es Fahrer oder Mitfahrer. Fahrer können frei entscheiden, wohin sie fahren, welche Strecke sie wählen und meistens auch, wie schnell sie reisen wollen (oder zumindest, wie oft sie eine Pause machen), ohne jemanden über ihre Entscheidungen informieren oder Rechenschaft darüber ablegen zu müssen. Viele Kunstwerke reflektieren diese Möglichkeit der Freiheit und der Flucht vor (häufig unzulässiger oder unangebrachter) Kontrolle, die Autos ihren Benutzern bieten. Eines der wohl eindrucksvollsten Beispiele hierfür sind die Episoden 3, 4, 6 und 7 des 1947 uraufgeführten Filmes „In jenen Tagen“ [1], die die mehr oder weniger erfolgreichen Autofahrten mehrerer Personen zeigen, die zwischen 1933 und 1945 von den Nationalsozialisten in Deutschland unterdrückt bzw. verfolgt wurden. Weitere Beispiele finden sich in Kap. 3. Gleichzeitig bietet ein Auto seinen Fahrern und Haltern eine geschützte Umgebung: Personen außerhalb können für gewöhnlich nicht hören, was innerhalb des Autos gesprochen wird, und sie können sich auch nicht einfach dazugesellen und der Unterhaltung beiwohnen. Auch wenn „My car is my castle“ nicht so populär ist wie „My home is my castle“, sehen viele Leute dennoch ihr Auto als Erweiterung ihres eigenen Heims. Dementsprechend kann man viele Haushaltsgegenstände in Autos vorfinden, und viele Haushaltsaktivitäten finden dort statt ([2], Paragraf 2).

Davon ausgehend könnten autonome Autos einfach eine Erweiterung der traditionellen Konzepte von Freiheit, Autonomie und Privatsphäre für ihre Fahrer und Benutzer darstellen. Jedoch macht „autonomes Fahren“ in erster Linie das Fahren autonom vom Fahrer. Gleichzeitig baut „autonomes Fahren“ stärker auf Interaktionen mit der Außenwelt als ein Auto, das von einem Menschen gefahren wird. Aus der Forschungswelt bekannte autonome Autos tasten ihre Umgebung ab und kommunizieren sogar häufig mit ihr wie z. B. mit anderen Autos in der Nähe. Über den Austausch mit anderen Entitäten in der näheren Umgebung hinaus gibt es Pläne, Autos durch Verkehrszentralen kontrollieren zu lassen, um ihr Verhalten (z. B. die Routenwahl) zu optimieren. Wie jede andere zentrale Einrichtung, die Daten sammelt, verursachen Verkehrszentralen Bedenken bezüglich der Privatsphäre. Dies motiviert dazu, die Datenflüsse und ihre Auswirkungen auf die Privatsphäre zu analysieren. Wenn man in Betracht zieht, dass Autos nicht nur eine große Menge an Daten über ihre Benutzer und ihre Umgebung sammeln, sondern diese auch für eine lange Zeit speichern und schließlich zu anderen Entitäten kommunizieren können, verstärkt dies noch die Notwendigkeit der Analyse.

Deshalb diskutiert dieses Kapitel fünf Leitfragen zu autonomem Fahren, die entsprechenden Datenflüsse sowie die Auswirkung der Interaktion zwischen Fahrzeugen auf die Privatsphäre:

1. Welche „neuen“ oder zusätzlichen Daten werden zur Realisierung des autonomen Fahrens gesammelt und verarbeitet und welche Konsequenzen ergeben sich daraus (Abschn. 24.2)?

2. Gibt es bestimmte Arten von Daten, die spezielle Hindernisse hervorrufen (s. Abschn. 24.3)?
3. Was ist aus der Perspektive des Datenschutzes zu berücksichtigen (Abschn. 24.4)?
4. Was ist bei der Gestaltung von Architekturen zu berücksichtigen, um schwerwiegende oder gar unlösbare Datenschutzprobleme zu vermeiden (Abschn. 24.5)?
5. Was muss auf lange Sicht hin bedacht werden (Abschn. 24.6)?

Diese Fragen werden, so weit wie möglich, anhand der Use-Cases diskutiert, die in Kap. 2 eingeführt wurden. Abschnitt 24.7 schließt dieses Kapitel ab.

24.2 Zusätzliche durch autonomes Fahren gesammelte und verarbeitete Daten

Zur Beurteilung von Chancen und Risiken, die mit der Sammlung und Verarbeitung zusätzlicher Daten verbunden sind, ist es hilfreich, diese Daten zu identifizieren. Dies geschieht entlang der vier Use-Cases (s. Kap. 2). Zuvor wird jedoch ein kurzer Überblick über die Daten gegeben, die bereits in einem nicht-autonom fahrenden Auto gesammelt oder verarbeitet werden können.

24.2.1 Gesammelte und möglicherweise übermittelte persönliche Daten in heutigen vernetzten Autos

Obwohl sich die Analyse in den übrigen Teilen dieses Abschnitts auf „neue“ oder zusätzlich erhobene Daten konzentriert, muss zunächst erwähnt werden, dass auch heutzutage schon viele Arten sensitiver persönlicher Daten in Autos gesammelt und übertragen werden. Beispiele hierfür sind:

- Alle Arten von Standort- und Navigationsdaten: Typische Beispiele sind Reiseziele, -zeiten und -gewohnheiten („jedes Wochenende nach Stuttgart“) sowie Vorlieben bei der Routenplanung (landschaftlich schön versus schnell versus umweltfreundlich versus am Rande der Legalität). Insbesondere wenn ein Auto durch Systeme zur Einsatzdisposition, Diebstahlvermeidung, Autoversicherung oder Mautberechnung überwacht wird, werden Informationen über Aufenthaltsorte gesammelt und in vielen Fällen an die entsprechenden zentralen Stellen übertragen. Einige dieser Systeme speichern Daten aufgrund ihrer Sensitivität dezentral, andere hingegen jedoch nicht. Ein Beispiel, das kürzlich sehr bekannt wurde, ist das neue europäische eCall-System [3], [4], [5], das automatisch aktiviert wird, wenn Sensoren im Auto einen schweren Unfall feststellen. Einmal ausgelöst wählt das System automatisch die europäische Notfallnummer 112, baut eine telefonische Verbindung zu einer Notfallzentrale auf und sendet detaillierte Informationen über den Unfall an Rettungsdienste. Die

übertragenen Informationen beinhalten die Uhrzeit des Vorfalls, die genaue Position des verunglückten Fahrzeuges sowie die Fahrtrichtung (wichtig bei Autobahnen und in Tunneln). Durch die Betätigung eines Schalters im Auto kann ein eCall auch manuell ausgelöst werden, z. B. durch Zeugen eines schweren Unfalls.

- Daten zur Fahrdynamik: Daten zur Fahrdynamik wie die Beschleunigung liefern Informationen zum Verhalten des Autos, aber auch zum Verhalten des Fahrers, etwa zu seinem Fahrstil (ruhig versus aggressiv versus schnell versus am Rande der Legalität).
- Daten zum Fahrverhalten: Diese Daten können über die Zeit hinweg aus verschiedenen Lokationsdaten abgeleitet werden. So kann aus dem Vergleich der Lokation eines Autos auf der Autobahn mit der Lokation 15 Minuten zuvor die durchschnittliche Geschwindigkeit des Autos bestimmt werden. Hieraus kann geschlossen werden, ob eine Geschwindigkeitsbegrenzung möglicherweise zeitweise überschritten wurde, in einigen Fällen auch, dass sie überschritten wurde.
- Umgebung: Das Auto sammelt Daten aus der Umgebung, um die Fahrt oder spezielle Verkehrssituationen zu dokumentieren, für den Fall, dass eine solche Dokumentation später als hilfreich erachtet würde. Ein Beispiel hierfür sind Kameras auf dem Armaturenbrett, um aufzuzeichnen und möglicherweise zu übertragen, was vor dem Auto passiert. Daten aus der Umgebung können sehr wohl auch persönliche Daten anderer Personen enthalten, wie z. B. Nummernschilder anderer Fahrzeuge oder die Gesichter von Personen.

Dieser grobe Überblick wirft auch die Frage auf, bei welcher Art von Daten man tatsächlich von persönlichen Daten sprechen kann. Ein Teil der beschriebenen Daten scheint auf den ersten Blick nicht „persönlich“ zu sein. Die Erfahrungen aus mittlerweile mehreren Jahrzehnten von Datenschutzbemühungen zeigen jedoch, dass es keine Garantien gibt, dass Daten nicht auf bestimmte Personen zurückgeführt und missbraucht werden können. Eine Konsequenz dieser Lehre ist, dass „personenbezogene Daten“ (englisch „Personally Identifiable Information“ (PII)) heutzutage nicht nur Informationen sind, die eine Person direkt identifizieren, sondern jede Art von Information, die (a) benutzt werden kann, um die (betroffene) Person zu identifizieren, auf die sich die Daten beziehen, oder (b) möglicherweise direkt oder indirekt auf eine Person hinweisen [[8], Clause 2.9].[1] Die Person (oder der PII-Prinzipal, folgend dem englischen „PII Principal“ [[8], Clause 2.11]) ist dann das Individuum, dessen Daten verarbeitet werden. In unserem Fall sind PII-Prinzipale dann nicht nur Fahrer, Mitfahrer oder Autobesitzer, sondern auch Passanten und andere Fahrzeuge, die erfasst und auf irgendeine mögliche Art und Weise identifiziert werden können.

1 Die Beziehung zwischen den Begriffen Daten und Informationen ist zu subtil und zu komplex, um sie hinreichend im Rahmen dieses Kapitels zu erläutern, Gleichzeitig sollte es hier ausreichen, Daten und Informationen als annähernd äquivalent zu betrachten. Würde man sich jedoch auf einen der Begriffe beschränken, tun sich Widersprüche mit der referenzierten Literatur auf.

Es gilt weiterhin, dass die praktische Sensitivität von Daten zu einem Zeitpunkt stark vom Kontext abhängig ist. So können z. B. die Standortdaten eines Autos sensitiver sein, wenn es in der Nähe des Rotlichtviertels einer Stadt geparkt ist. Weitere Beispiele finden sich in der nachfolgenden Diskussion der Use-Cases des autonomen Fahrens und der Interessen der an den Use-Cases Beteiligten. Zudem hilft die Analyse der Cases, neue Situationen und entsprechende Fragestellungen zu illustrieren.

24.2.2 In autonomen Autos gesammelte persönliche Daten

Dieser Abschnitt diskutiert anhand der vier in Kap. 2 vorgestellten Use-Cases die in autonomen Autos gesammelten Daten.

24.2.2.1 Use-Case 1: Autobahnautomat mit Verfügbarkeitsfahrer

Der Fahrroboter übernimmt das Fahren, aber nur auf Autobahnen oder autobahnähnlichen Schnellstraßen. Während der autonomen Fahrt wird der Fahrer zum Passagier, der die Hände vom Lenkrad sowie die Füße von den Pedalen nehmen und anderen Aktivitäten nachgehen kann. Der Fahrroboter koordiniert die sichere Übergabe zum Fahrer und stoppt das Auto an einem möglichst sicheren Ort, wenn nötig.

Neue und zusätzliche Daten, die das Auto in diesem Use-Case sammeln und lernen kann, sind:

- Fähigkeiten des Fahrers, z. B. ob der Fahrer in der Lage ist, die Kontrolle vom Roboter zurück zu übernehmen oder nicht und wie lange die Übergabe dauert. Beide Arten von Daten können von Interesse sein: als aktuelle Daten zur Steuerung von Reaktionen des Autos, aber auch längerfristig als Grundlage für Längsschnittbewertungen.
- Fahrverhalten: Zusätzlich zu Daten über das Fahrverhalten, die bereits heute verfügbar sind, ermöglicht dieser Use-Case auch das Sammeln weiterer Daten, beispielsweise, unter welchen Umständen der Fahrer die Kontrolle abgibt und/oder zurückfordert.
- Umgebung: Es können zusätzliche Daten der Umgebung gesammelt werden, um das autonome Fahren zu ermöglichen. Auch die Dokumentation der Fahrt selbst oder spezifischer Verkehrssituationen kann als hilfreich angesehen werden, um potenzielle Konflikte handhaben zu können. Wie in Abschn. 24.2.1 beschrieben, können Daten der Umgebung auch persönliche Informationen Dritter sein, beispielsweise Nummernschilder oder Gesichter. Daher bestehen Daten der Umgebung aus einer Mischung persönlicher Informationen verschiedener Personen, was sie sehr heikel macht.

Im Rahmen der Diskussion über rechtliche und haftungsbedingte Folgen des autonomen Fahrens (vgl. Teil V dieses Buches, insbesondere die Diskussion durch Gasser Kap. 25) kann angenommen werden, dass ein Interesse darin besteht, Daten zu sammeln, um mögliche Unfälle zu dokumentieren und zu untersuchen, welches Verhalten des Autos, des

Fahrroboters, des Fahrers oder anderer Parteien den Unfall verursacht haben könnte. Dies wäre im Einklang mit anderen Beispielen der Vorgehensweise von Strafverfolgungsbehörden, die ein großes Interesse an Daten haben, die durch die Computerisierung von Aktivitäten zugänglich werden, da computerisierte Aktivitäten meist einfach zu protokollieren sind.

24.2.2.2 Use-Case 2: Autonomes Valet-Parken

Der Fahrroboter stellt das Fahrzeug – nachdem die Insassen es verlassen haben und gegebenenfalls Transportgut ausgeladen wurde – in einer nahen oder auch entfernten Parkposition ab. Anschließend fährt der Fahrroboter das Fahrzeug von der Parkposition wieder zurück bzw. an eine andere gewünschte Adresse oder parkt das Fahrzeug um. Die Fahrer sparen so die Zeit für die Parkplatzsuche, das Abstellen sowie den Fußweg von einem weiter entfernten Parkplatz zum eigentlichen Ziel. Außerdem wird hierdurch der Zugang zum Fahrzeug (räumlich wie zeitlich) erleichtert. Der Parkraum wird durch das autonome Valet-Parken effizienter genutzt und die Parkplatzsuche effizienter gestaltet.

Neue und zusätzliche Daten, die das Auto in diesem Use-Case sammeln und lernen kann, sind:

- Dauer eines Aufenthaltes: Wie viel Zeit verbringen die Nutzer vor Ort?
- Gebiete von Interesse: Wo verbringen Nutzer mehr oder weniger Zeit?
- Fahrt- und Aufenthaltszeiten: Wann verbringen die Nutzer mehr oder weniger Zeit außerhalb ihres Autos?
- Unter welchen Umständen wird das Auto unbeaufsichtigt gelassen?
- Besuchsgewohnheiten: Wie oft begibt sich der Nutzer an einen bestimmten Ort, z. B. „jedes Wochenende zu einem bestimmten Supermarkt, einer Bar oder Diskothek“?
- Umgebung: Diese Daten sind im Prinzip die gleichen wie in Use-Case 1, variieren jedoch in ihrer Abhängigkeit von der Umgebung. Auf einem gefüllten Parkplatz kann das Auto pro Zeiteinheit mehr Nummernschilder erfassen als auf einer Autobahn, aber vermutlich weniger Gesichter, weil die meisten Autos leer sind. Auf dem Weg zum Parkplatz werden allerdings vermutlich oft mehr Gesichter erfasst werden, weil z. B. Fußgänger die Straßen überqueren, als auf dem Parkplatz selbst, vermutlich sogar mehr als auf der Autobahn.

Da es keine direkte Wechselwirkung zwischen Fahrer und Fahrzeug gibt, werden keine Daten über das Fahrverhalten erfasst.

24.2.2.3 Use-Case 3: Vollautomat mit Verfügbarkeitsfahrer

Use-Case 3 ist Use-Case 1 ähnlich, da in beiden Fällen der Fahrroboter die Aufgabe des Fahrens ausführt und der menschliche „Fahrer“ in dieser Situation als Passagier die Hände vom Lenkrad sowie die Füße von den Pedalen nehmen und andere Dinge tun kann. In Use-Case 3 kann der Fahrer jedoch in mehr Situationen die Kontrolle an den Fahrroboter übergeben und ist nicht wie in Use-Case 1 auf Autobahnen beschränkt. Folglich sind die neuen

und zusätzlichen Daten, die das Auto in diesem Use-Case sammeln und lernen kann, grundsätzlich die gleichen wie in Use-Case 1. Allerdings gibt es mehr Optionen für den Fahrer, die Aufgabe des Fahrens zu delegieren und die Kontrolle zurück zu übernehmen. Dies kann dazu führen, dass mehr Daten über das Verhalten des Fahrers erhoben werden können. Hierzu zählen insbesondere Daten über die Umstände, unter denen der Fahrer die Kontrolle delegiert und/oder wieder übernimmt. Ähnlich wie in Use-Case 2 können die Daten der Umgebung umfangreicher und sensitiver sein, als die auf einer Autobahn gesammelten Daten aus Use-Case 1.

24.2.2.4 Use-Case 4: Vehicle-on-Demand

Der Fahrroboter fährt das Fahrzeug in allen Szenerien mit Insassen, mit Fördergut, aber auch komplett ohne Inhalt autonom. Durch den Fahrroboter kann das Fahrzeug überall bereitgestellt werden. Passagiere können die Fahrzeit komplett frei für andere Dinge als für die Bewältigung der Fahraufgabe nutzen. Der Innenraum kann ohne die Einschränkungen eines Fahrersitzes völlig frei gestaltet werden, möglich ist jedoch eine Kamera, die in Richtung des Fahrgastraumes positioniert ist.

Während dieser Use-Case der anspruchsvollste aus der Perspektive des autonomen Fahrens ist, können weniger zusätzliche Daten gesammelt werden als in Use-Case 3. Insbesondere können keine zusätzlichen Daten über das Verhalten eines Fahrers gesammelt werden, da kein Fahrer mehr benötigt wird. Zusätzlich gesammelte Daten sind in diesem Case:

- Reiseverhalten (z. B. wann wollen Passagiere Pausen einlegen?),
- allgemeines Verhalten (oder Fehlverhalten) aller Passagiere im Auto,
- Daten über die Umgebung, beispielsweise, um einen Unfall und dessen Ursache zu dokumentieren (wenn Daten von Passagieren als nützlich für die Unfalldokumentation erachtet werden).

24.2.3 Konsequenzen von Datenspeicherung für die Kontrolle über Daten und Missbrauch

Grundsätzlich eröffnet die Speicherung von Daten die Möglichkeit für jede Art der Verarbeitung dieser Daten. Das mag theoretisch trivial erscheinen; jedoch ergeben sich die praktischen Folgen einer Datenspeicherung daraus, dass die gespeicherten Daten auch später noch gebraucht und missbraucht werden können, möglicherweise auch unter Umständen, die dem Nutzer ursprünglich gar nicht bewusst waren. Dies impliziert eine längerfristige Verantwortung für diese Daten. Diese Verantwortung muss bei der Partei liegen, die die Daten kontrollieren und Entscheidungen über deren Nutzung treffen kann.

Wenn man davon ausgehen kann, dass sich die im Auto gespeicherten Daten unter der alleinigen Kontrolle des Besitzers oder Fahrers des Autos befinden, kann die Frage nach der Verantwortung über die Daten relativ leicht beantwortet werden. Ist dies nicht der Fall,

erweitert sich die Verantwortung für die Speicherung und jede Art von Missbrauch der Daten auf die Parteien, die Speicherung und/oder Transfer der Daten kontrollieren.

Es gibt mindestens zwei Anzeichen dafür, dass einflussreiche Institutionen verlangen werden, die Daten aus dem Auto auch nach außerhalb zu transferieren:

1. Strafverfolgungsbehörden fordern häufig, dass Daten, die für technische oder kommerzielle Zwecke gespeichert werden, auch für Zwecke der Strafverfolgung zur Verfügung gestellt werden sollen. Gesetzgeber folgen dieser Forderung häufig. Das Autos und Ortsdaten ähnlichste Beispiel ist das der Mobilkommunikation. Seit dem Beginn der 1990er-Jahre war der GSM-Standard für zellbasierte Mobilkommunikation implementiert, und Ortsinformationen der Teilnehmer wurden in den Netzen verarbeitet. Schon bald darauf wurden einschlägige Regulierungen eingeführt, um es den „Bedarfsträgern", etwa Strafverfolgungsbehörden, zu ermöglichen, auf alle Arten von Daten (inklusive Ortsdaten) in den GSM-Netzen zuzugreifen: Ein Beispiel hierfür ist die deutsche Fernmeldeüberwachungsverordnung [6], die bereits 1995 eingeführt wurde.
2. Internet-Unternehmen wie Google sind inspiriert und angetrieben durch die Konnektivität beliebiger Systeme und die Übermittlung von Daten. Ein Beispiel ist ein Statement von Jared Cohen, Direktor von Google Ideas, und Eric Schmidt, Executive Chairman von Google, in den Schlussfolgerungen ihres gemeinsamen Buches *The New Digital Age:* „Attempts to contain the spread of connectivity or curtail people's access will always fail over a long enough period of time – information, like water, will always find its way through." ([7], S. 254)

Nicht alles, was einflussreiche Institutionen gefordert haben, ist letztendlich auch so eingetreten, aber die Beispiele geben einen Eindruck von den Herausforderungen, die die Speicherung von Daten mit sich bringt, auch wenn die Daten eigentlich wohlbehalten in abgeschlossener und isolierter Weise gespeichert werden sollten.

24.2.4 Konsequenzen der Weitergabe von Daten an Dritte

Daten, die an Dritte jenseits der Domänen von Autoeignern oder -fahrern transferiert werden, ermöglichen es diesen Dritten, ihre Interessen zu verfolgen. Diese Interessen können mit den Interessen der sogenannten Datensubjekte, die durch die Daten identifiziert werden (in diesem Fall sind das typischerweise Autofahrer oder -eigner) im Konflikt stehen.

In diesem Abschnitt werden Beispiele für die folgenden Drittparteien diskutiert: Fahrzeughersteller, Versicherungsdienstleister, Flottenbetreiber, staatlich autorisierte Parteien, Peer-ad-hoc-Netzwerke, z. B. andere Verkehrsteilnehmer oder andere autonome Fahrzeuge, und Verkehrszentralen. Die Reihenfolge der Unterabschnitte folgt der ansteigenden Komplexität im Setting der Drittparteien.

24.2.4.1 Fahrzeughersteller

Fahrzeughersteller können daran interessiert sein, das Verhalten des Fahrzeugs zu dokumentieren, um Erkenntnisse über das Fahrzeug in Extremsituationen zu sammeln oder die Qualität der (oft sehr komplexen) Software zu testen. Dies ermöglicht ihnen, ihre Systeme zu verbessern und weiterzuentwickeln. Diese Art von Daten ähnelt denen, die Hersteller und Betreiber von Telekommunikationssystemen zum Zwecke der Qualitätssicherung und Wartung sammeln. Gleichzeitig beinhalten diese Daten jedoch sensitive Informationen über die Fahrer, z. B. die typische Fahrgeschwindigkeit, die Anzahl der Notbremsungen oder verpasste Übergaben vom Fahrroboter in den Use-Cases 1 und 3.

24.2.4.2 Versicherungsdienstleister

Versicherungsdienstleister sind häufig an ausführlicheren Informationen über ihre Kunden interessiert, um das Risiko, auf das sie sich einlassen, zu bewerten. Abhängig von der Art der Versicherung können unterschiedliche Informationen von Interesse sein. Für eine Unfallversicherung kann das Risiko beispielsweise vom Fahrverhalten (vorsichtiger oder risikofreudiger Fahrstil) abgeleitet werden, während für eine Diebstahlversicherung insbesondere ortsbezogene Daten (Regionen mit höherem oder niedrigerem Diebstahlrisiko für das jeweilige Fahrzeug) von Bedeutung sind. Alle Use-Cases liefern hier umfängliche Daten. Use-Case 1 und 3 bieten vor allem Daten über das Fahrverhalten, Use-Case 4 ermöglicht das Erheben von Daten über das Verhalten der Insassen und deren Notrufe. Ortsbezogene Daten werden in allen Use-Cases erhoben. Diese Bewertungen ermöglichen vielleicht fairere Beurteilungen der Versicherungskunden, da sie ein kostenreduzierendes Verhalten belohnen. Die Nutzer werden dadurch aber auch einer erhöhten Überwachung ausgesetzt, ohne genaue Erläuterungen der damit verbundenen Risiken und Chancen zu erhalten. Versicherungsdienstleister treffen Entscheidungen oft auf Grundlage von Scoring-Systemen. Von diesen Systemen oder den von ihnen verwendeten Daten und Kriterien wissen Kunden oft nichts, da Versicherungsunternehmen diese Informationen als Geschäftsgeheimnisse betrachten und vor der Konkurrenz geheim halten wollen. Das führt dazu, dass Kunden von den Reaktionen einer Versicherung – wie der Verweigerung einer Vertragsverlängerung oder der Erhöhung einer Prämie – leicht überrascht werden können.

24.2.4.3 Flottenbetreiber

Flottenbetreiber, etwa Autovermietungen, sind in einer ähnlichen Situation wie Versicherungsunternehmen. Um ihren geschäftlichen Erfolg zu steigern, versuchen sie, das Risiko der Autovermietung an die jeweiligen Kunden zu bewerten und das Ergebnis in ihre Preisgestaltung einfließen zu lassen. Daher kann es zu ähnlichen Konsequenzen für die Kunden kommen wie bei Versicherungen (z. B. in Bezug auf (k)eine Verlängerung des Vertrages oder eine Erhöhung der Gebühren). Auch in diesem Szenario könnten in allen Use-Cases Daten erhoben werden. Der wesentliche Unterschied zum Versicherungsszenario ergibt sich aus der Tatsache, dass Flottenbetreiber in der Regel die Besitzer der Autos sind und somit mehr Kontrolle über ihre Autos haben als eine Versicherung über versicherte Autos ihrer Kunden. Dieser Unterschied ist wichtig für jegliches Konzept eines „Private Data

Vault“ zur Speicherung sensitiver Daten von Mietern oder Fahrern (s. Abschnitt 24.5). Ein solches „Private Data Vault“ müsste in diesem Szenario entweder speziell im Auto installiert werden, um es vor dem Zugriff des Flottenbetreibers zu schützen, oder vom Mieter oder Fahrer mitgebracht werden.

24.2.4.4 Kommerzielle standortbezogene Dienste

Werbetreibende Unternehmen sind daran interessiert, jeweils passende Werbenachrichten an die jeweilige Zielgruppe zu adressieren. Dies beinhaltet auch die Wahl der richtigen Orte für entsprechende Werbebotschaften. So könnten beispielsweise Pendler, die aktuell im Stau stehen, mit einem Sonderangebot von Geschäften in der Nähe der nächsten Ausfahrt adressiert werden, damit sie aus dem Stau heraus zum Einkaufen fahren. Ebenso können Reisende, die auf dem Weg zu einem großen Flughafen im Stau stehen, von einem besser zu erreichenden Regionalflughafen umworben werden, damit sie ihren nächsten Flug von dort aus buchen: So werden auf der Autobahn von Norden in Richtung Flughafen San Francisco Flüge ab San José beworben. Deshalb interessieren sich werbetreibende Unternehmen für Verkehrsströme (und Staus). Darüber hinaus sind sie immer an weiteren Details über ihre Zielgruppe interessiert, die es ihnen erlauben, Rückschlüsse auf deren Verhalten wie z. B. die Art der Reise (Geschäftsreise, Pendeln, Freizeitausflug) zu ziehen.

24.2.4.5 Staatlich autorisierte Stellen

Staatlich autorisierte Stellen wie Polizeien oder Geheimdienste können die Daten zum Zwecke der Überwachung verwenden, um Verhalten zu erkennen, das sie sanktionieren oder vermeiden wollen. Im Falle der Verkehrspolizei könnte dies jede Art von Verhalten sein, das als unsicher angesehen wird oder gegen Verkehrsregeln verstößt wie z. B. Schwierigkeiten oder auffälliges Verhalten in der Interaktion mit dem Fahrroboter. Polizeikräfte, die Verbrechen untersuchen oder verhindern wollen, sowie Geheimdienste können an Navigations- oder Bewegungsdaten interessiert sein, um Informationen über das soziale Umfeld von Reisenden zu erlangen, etwa, wer wen wo trifft. Mit großer Wahrscheinlichkeit werden interessierte Geheimdienste und Bedarfsträger zudem eine ganz eigene Interpretation davon haben, wozu sie jenseits der Garantien und Zusicherungen von Datenschutzgesetzen autorisiert sind. Dies gilt vor allem für Daten, die Autos von ihrer Umgebung sammeln würden. Mit dem Ansatz, dass Daten von vielen oder sogar allen Autos kombiniert werden, ist eine spezifische Form des *crowd-sourcing* vorstellbar. Einige Gemeinden nutzen bereits heute *crowd-sourcing*, um Daten zur Umweltbelastung zu sammeln. Auch wenn in diesem Fall keine oder nur wenige personenbezogenen Daten gesammelt werden, ist das Beispiel dem Szenario, in dem ein Auto seine Umgebung ausspioniert, konzeptionell nahe.

24.2.4.6 Peer-ad-hoc-Netzwerke

Peer-ad-hoc-Netzwerke (z. B. andere Verkehrseinheiten oder autonome Fahrzeuge) können an jeglichen Daten zur Optimierung der Wegführung und Stabilisierung interessiert sein, die ihnen dabei helfen, die Straßenverhältnisse besser zu bewerten. Dabei können die In-

formationen anderer (etwa entgegenkommender) Fahrzeuge helfen, da diese ja bevorstehende Straßenabschnitte der eigenen Route schon passiert haben. Sofern es sich dabei um anonymisierte Daten handelt, die lediglich unter den beteiligten Peers ausgetauscht werden, sind die Folgen weniger schwerwiegend als bei Datenübertragungen zu einer (zentralen) Einrichtung, die Daten aggregiert (wie andere in diesem Kapitel beschriebene Einrichtungen).

24.2.4.7 Verkehrszentralen

Die Interessen von Verkehrszentralen hängen stark von den Interessen ihrer Betreiber und Eigentümer ab. Verkehrszentralen, die Verkehrsströme effizienter gestalten und die Auswirkungen von Verkehrsunfällen auf den Verkehrsfluss verringern wollen, sind an allen Daten interessiert, die ihnen helfen, die aktuelle und zukünftige Verkehrssituationen besser zu beurteilen: Fahrbedingungen können von Umgebungsdaten oder von Bewertungen des Fahrverhaltens abgeleitet werden, wie sie in allen Use-Cases anfallen; mögliche Staus können aus Reiseplänen und Navigationsdaten abgeleitet werden. Verkehrszentralen können auch an Kooperationen mit anderen Einrichtungen interessiert sein, um ihre Kosten zu refinanzieren oder sogar Gewinne zu erwirtschaften: Dies wird durch die Tatsache gestützt, dass andere Unternehmen, wie in den vorangegangenen Beispielen beschrieben, Nutzen aus den von Verkehrszentralen gesammelten Daten ziehen können.

Das Ausmaß, in dem Verkehrszentralen mit anderen Unternehmen, die an ihren Daten interessiert sind und Geld dafür bieten, kooperieren wollen, hängt von ihrem Status und ihrer finanziellen Ausstattung ab. Eine private gewinnorientierte Verkehrszentrale benötigt eine Finanzierung; eine öffentliche Verkehrszentrale steht eventuell unter geringerem finanziellem Druck. Allerdings gab und gibt es für viele der gegenwärtigen Investitionen in öffentliche Infrastrukturen Überlegungen, sie in öffentlich-privaten Partnerschaften durchzuführen, um sie trotz Geldmangel in den öffentlichen Haushalten durchzuführen. Dies gilt z. B. für die Mauterhebung und war ebenso für das Galileo-Satellitennetz geplant – auch wenn der Plan in diesem Fall mangels privater Interessenten nicht umgesetzt wurde. Auch Rundfunkanstalten werden immer abhängiger von einer privaten Mitfinanzierung, z. B. durch Werbung.

24.3 Gibt es bestimmte Arten von Daten, die spezielle Hindernisse hervorrufen?

Es ist prinzipiell unmöglich, die potenziellen Verwendungen von Daten für legitime oder illegitime Zwecke vorherzusagen. Darüber hinaus hat es sich als unmöglich herausgestellt zu garantieren, dass es auch auf lange Sicht zu keiner Verwendung oder keinem Missbrauch für eine spezielle Art von Daten kommt. Ein Grund hierfür ist, dass die heutige Konnektivität Verknüpfungen von Daten erheblich vereinfacht. Daten über die Fähigkeiten eines Fahrers bei der Übernahme der Kontrolle vom Fahrroboter mögen auf den ersten Blick harmlos erscheinen, setzt man diese jedoch in Bezug zu historischen Daten (Fähigkeiten

vor zehn Jahren) oder zukünftigen Daten (Fähigkeiten in zehn Jahren), kann dies einen Eindruck von steigender oder sinkender Fahrtüchtigkeit verursachen. Dies kann zu ungerechtfertigten Nachteilen für Fahrer führen, etwa bei der Berechnung von Versicherungsprämien. Ähnliche Bewertungsmethoden bei der Beurteilung der Kreditfähigkeit haben sich in der Vergangenheit häufig als falsch erwiesen, wenn es um individuelle Bewertungen ging, auch wenn sie eine statistische Wertigkeit besaßen. Daher gibt es keine expliziten Regeln, bestimmte Arten von Daten als speziell einzuordnen und spezielle Hindernisse für deren Nutzung vorzusehen. Man mag den Eindruck haben, dass Daten, die Rückschlüsse auf die Gesundheit und medizinische Details erlauben, oder Daten zur politischen Meinung von Personen besonders sensibel sind. Es gibt jedoch keinen eindeutigen Beleg dafür, dass diese Daten immer sensibler sind als z. B. Daten über die finanzielle Situation einer Person.

Die rechtliche Konsequenz der beschriebenen Schwierigkeiten ist das Prinzip, für jedes einzelne Datum die Legitimität der Datenverarbeitung zu prüfen, statt eine allgemeine Freigabe vorzusehen (s. auch die Beschreibungen von „Rechtmäßigkeit und genaue Bestimmung des Zwecks der Datenverarbeitung“ und „Beschränkung der Erfassung“ in Abschn. 24.4.1). Somit muss für jede Art von Daten überprüft werden, ob ihre Erfassung notwendig ist, um den Dienst bereitzustellen, dessentwegen sie erhoben wurden. Zusätzlich ist zu überprüfen, ob die Art der Verarbeitung angemessen ist.

24.4 Anforderungen aus der Perspektive des Datenschutzes

Dieser Abschnitt diskutiert die Anforderungen aus der Perspektive des Datenschutzes. Einführend werden international etablierte Grundsätze und ihr Bezug zu den Use-Cases erläutert (s.Abschn. 24.4.1). Anschließend werden in Abschn. 24.4.2 zusätzliche Überwachungsmaßnahmen mit dem Ziel einer „datenschutzverträglichen“ Verwendung der Daten diskutiert, bevor in Abschn. 24.4.3 das Augenmerk auf die Beschränkung von Zugriffsrechten und auf den Einsatz von Datenverschlüsselung gelegt wird.

24.4.1 Grundsätze

Für jegliche Art persönlicher Daten, die erhoben oder erfasst und aus dem Einflussbereich der betroffenen Person heraus übermittelt werden, muss es eine klare Begründung geben, die die einschlägigen Datenschutzgrundsätze und -anforderungen berücksichtigt. Die Datenschutzgrundsätze und -anforderungen hängen von der jeweiligen nationalen, regionalen und gelegentlich auch branchenspezifischen Gesetzgebung ab, sodass eine vollständige Analyse hier unmöglich wäre. Erfreulicherweise existiert seit 2011 die internationale Norm ISO/IEC 29100 „Privacy Framework“ [8], die elf Datenschutzgrundsätze enthält. Diese Grundsätze wurden aus Datenschutzgrundsätzen abgeleitet, die in den Jahren und Jahrzehnten zuvor von Staaten, Ländern und internationalen Organisationen (z. B. der OECD und der EU) in ihren jeweiligen Regulierungen entwickelt worden waren. Die Editoren der

Norm kamen aus Deutschland und den USA, und Experten aus vielen weiteren Ländern beteiligten sich an dem Normprojekt. Ein Schwerpunkt der ISO/IEC 29100 „Privacy Framework“ ist die Implementierung der Datenschutzgrundsätze in IKT (Informations- und Kommunikationstechnologie)-Systemen. Ein weiterer Schwerpunkt ist die Entwicklung von Datenschutzmanagement-Systemen, die in die IKT-Systeme von Organisationen integriert sind. Die Datenschutzgrundsätze zielen darauf, die Gestaltung, Entwicklung und Implementierung von Datenschutzrichtlinien und -kontrollen anzuleiten. Ein Entwurf verwandter Anforderungen findet sich auch in den jüngsten Empfehlungen des Deutschen Verkehrsgerichtstages [9]. Die elf Grundsätze lauten:

1. Einwilligung und Wahlfreiheit,
2. Rechtmäßigkeit und genaue Bestimmung des Zwecks der Datenverarbeitung,
3. Beschränkung der Erfassung,
4. Datenminimierung,
5. Beschränkung der Verwendung, Speicherung und Weitergabe,
6. Richtigkeit und Qualität,
7. Offenheit, Transparenz und Auskunft,
8. Individuelle Beteiligung und Zugriff,
9. Rechenschaftspflicht,
10. Informationssicherheit,
11. Erfüllung der Datenschutzanforderungen.

Dieser Abschnitt konzentriert sich auf die Erläuterung der wichtigsten Grundsätze und gibt Beispiele basierend auf den Use-Cases.[2]

1. Einwilligung und Wahlfreiheit
   Das Prinzip der Einwilligung wurde im Laufe der Zeit eingeführt, um sicherzustellen, dass eine von der Verarbeitung ihrer PII betroffene Person kontrollieren kann, ob ihre PII verarbeitet wird oder nicht. Eine Ausnahme von diesem Prinzip bilden Gesetze, die explizit eine Verarbeitung von PII ohne Einwilligung erlauben. Es wird aufgrund einschlägiger Erfahrungen ausdrücklich erwähnt, dass die Einwilligung eine informierte Einwilligung sein muss, damit Betroffene erklärt bekommen, wozu sie einwilligen und nicht „über den Tisch gezogen“ werden. Die Einwilligung muss außerdem in Form einer expliziten Einwilligungserklärung (*opt-in*) erfolgen. Es hat sich herausgestellt, dass die Forderung nach Wahlfreiheit wichtig ist, um zu vermeiden, dass Benutzer faktisch gezwungen werden einzuwilligen, weil sie keine Alternative zu dem jeweiligen Dienst haben. In den Use-Cases 1, 2 und 3 wird die Einwilligung des Besitzers, des Fahrers und jedes identifizierten Mitfahrers benötigt. Im vierten Use-Case wird die Einwilligung der Mitfahrer und gegebenenfalls des Fahrers benötigt. Die kritischste Frage entsteht jedoch bei der Einwilligung zur Verarbeitung der Daten

2 ISO/IEC 29100 erläutert die Grundsätze ausführlicher.

der untersuchten Umgebung. Zum Beispiel sind private Überwachungskameras üblicherweise nicht rechtens, wenn sie öffentliche Flächen mit einbeziehen und dort Daten von Personen erfassen können. Für Daten von öffentlichen Überwachungskameras gibt es strikte Regeln entlang der folgenden Grundsätze.

2. Rechtmäßigkeit und genaue Bestimmung des Zwecks der Datenverarbeitung
   Sich an diesen Grundsatz zu halten bedeutet: Sicherstellung, dass der Zweck der Datenverarbeitung vollständig geltendem Recht entspricht und sich auf eine zulässige Grundlage stützt; Kommunikation des Zwecks an den Betroffenen, bevor die Information erfasst oder für einen neuen Zweck benutzt wird; Verwendung einer Sprache für die Spezifikation, die klar und den jeweiligen Umständen angemessen ist; und, wenn zutreffend, die Bereitstellung von hinreichenden Erläuterungen für die Notwendigkeit der Verarbeitung sensitiver PII. Ein Zweck kann eine gesetzliche Grundlage oder eine spezifische Autorisierung seitens einer autorisierten Datenschutz- oder Regierungsbehörde erfordern. Wenn der Zweck der Verarbeitung der PII nicht den einschlägigen Gesetzen entspricht, darf keine Verarbeitung stattfinden. Für die Use-Cases bedeutet dies, dass die Zwecke der Datenverarbeitung auf eine klare Art und Weise spezifiziert werden müssen. Dies wird eine besondere Herausforderung im Fall des Erfassens von Umgebungsdaten darstellen.
3. Beschränkung der Erfassung
   Die Erfassung von PII muss im Rahmen der jeweiligen gesetzlichen Vorschriften bleiben und ist auf solche Daten zu begrenzen, die für den beschriebenen Zweck notwendig sind: In unserem Fall trifft dies auf alle Daten über das Verhalten des Fahrers und der identifizierten Mitfahrer zu. Wenn der Zweck das autonome Fahren ist, werden jegliche gesammelten Daten mit dem Zweck des autonomen Fahrens gerechtfertigt werden müssen (und nicht mit einer anderen Verwendung, auch wenn diese beispielsweise kommerziell attraktiv erscheint).
4. Datenminimierung
   Das Prinzip der Datenminimierung ist eng mit dem Prinzip der Beschränkung der Erfassung verknüpft, bezieht sich aber auf eine strikte Minimierung der *Verarbeitung* von PII. Datenverarbeitungsprozeduren und IKT-Systeme sollen die PII minimieren, die verarbeitet wird, und den Zugriff darauf begrenzen; Default-Optionen sollen, wenn immer möglich, betroffene Personen nicht identifizieren, die Möglichkeit ihrer Überwachung reduzieren und die Verknüpfbarkeit der erfassten PII mit anderer PII begrenzen (und so auch die Verfolgbarkeit der betroffenen Personen); außerdem ist PII zu löschen und zu beseitigen, sobald der Zweck der PII-Verarbeitung entfallen ist, oder, falls es keine rechtliche Anforderung gibt, die PII aufzubewahren oder wann immer Löschen und Beseitigen zweckmäßig sind. Bei allen vier Use-Cases beschränkt dieser Grundsatz die Übertragung jeglicher Daten an zentrale Einheiten wie etwa Verkehrszentralen; PII, die nur benötigt wird, um die Situation im und um das Auto zu bewältigen, darf ohne Erlaubnis der betroffenen Personen nicht das Auto verlassen. Datenminimierung erfordert auch die Begrenzung der Speicherung erfasster Daten, insbesondere, wenn diese Daten einfach erneut erfasst werden können, sobald sie

wieder benötigt werden. Um die Verknüpfbarkeit gesammelter PII zu beschränken, wird zudem die Anonymisierung und Aggregation jeglicher Daten verlangt, die nicht individuell benötigt werden.

5. Informationssicherheit
   Informationssicherheit bezieht sich auf den Schutz von PII mit entsprechenden Maßnahmen auf der operationellen, funktionalen und strategischen Ebene, um die Integrität, Vertraulichkeit und Verfügbarkeit der PII zu gewährleisten und sie über den gesamten Lebenszyklus hinweg gegen Risiken wie nicht autorisierten Zugriff, nicht autorisierte Vernichtung, nicht autorisierte Modifizierung, nicht autorisierte Veröffentlichung oder Verlust zu schützen. Informationssicherheit umfasst gegebenenfalls die Auswahl eines geeigneten Auftragsverarbeiters, um den Zugriff auf die PII auf diejenigen zu beschränken, die zur Ausübung ihrer Pflichten zugreifen müssen. Abschnitte 24.4.2 und 24.4.3 beschreiben entsprechende Maßnahmen.

Die Verwendung von Daten jenseits dessen, was für die Zurverfügungstellung eines Dienstes (für die die Daten erfasst wurden) nötig ist, erfordert eine explizite Einwilligung. Daher bedarf es für jegliche PII, die den Einflussbereich des PII-Prinzipals verlässt, einer klaren und aussagekräftigen Begründung unter Berücksichtigung der einschlägigen Datenschutzgrundsätze. Die Begründung muss den PII-Prinzipal darüber informieren, was er gewinnt und was er dafür aufgibt. Praktisch muss die Begründung also überzeugend, aber nicht tendenziös sein. Davon muss auch die Aufsichtsbehörde überzeugt sein, wenn sie prüft, ob der PII-Prinzipal getäuscht wurde, z. B. durch die Behauptung der Notwendigkeit einer Datenverarbeitung, die nicht notwendig war, wenn nach dem Prinzip der Datenminimierung eine alternative Methode oder Technologie hätte gewählt werden können. Die Aufsichtsbehörde wird auch überprüfen, ob Grundrechte durch die Verarbeitung der Daten gefährdet würden. Grundrechte können nicht einfach durch die Einwilligung der Benutzer aufgegeben werden, da die Benutzer möglicherweise nicht die damit verbundenen Konsequenzen erkennen. Ein verwandtes Beispiel wäre, Benutzer einer Wahlmaschine zu bitten, ihr Wahlverhalten speichern und verarbeiten zu dürfen.

Jede PII, die eine Diskriminierung von Personen aufgrund ihrer Gesinnung ermöglicht, ist in vielen praktischen Fällen besonders kritisch zu betrachten. Einschlägige Beispiele sind die Interessengebiete und entsprechenden Orte und Fahrtrichtungen, etwa zu einer politischen Demonstration und auch in Verbindung zu Aufenthaltsorten und Fahrtrichtungen anderer Personen, etwa in Bürgerinitiativen. Ein Beispiel für eine Begründung steht in der Grundsatzentscheidung des Deutschen Bundesverfassungsgerichtes von 1983 [10], die für Deutschland das Grundrecht auf „informationelle Selbstbestimmung“ etabliert hat und fordert, einen *Chilling Effect* bei der Bürgerbeteiligung in demokratischen Prozessen zu vermeiden:

> Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann

> in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.
>
> Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insofern die Befugnis des Einzelnen, grundsätzlich selbst über die Verwendung seiner persönlichen Daten zu bestimmen.

Ähnliche Überlegungen sind besonders in Ländern mit instabilen politischen Verhältnissen relevant, wo Bürger befürchten müssen, dass zukünftige Machthaber ihr Verhalten, das gegenwärtig völlig legal ist, im Rückblick nicht tolerieren. Dies kann auch die Reise zu politischen Treffen einschließen.

Hinzu kommt, dass die Veröffentlichungen von Edward Snowden [11] ernstzunehmende Schwächen im Datensicherheitsregime vieler PII-Verarbeiter aufgezeigt haben. Dies gilt insbesondere für Daten und PII, die für Geheimdienste interessant sind. Man kann erwarten, dass diese Entwicklung in zukünftige Risikoanalysen und Überlegungen mit einbezogen wird.

24.4.2 Weitere Überwachungsmaßnahmen für eine datenschutzverträgliche Verwendung der zusätzlichen Daten

Weitere Überwachungsmaßnahmen für eine datenschutzverträgliche Verwendung der zusätzlichen Daten sind zu erwarten. Sie sind z. B. durch den Grundsatz der Rechenschaftspflicht in der Norm ISO/IEC 29100 [8] motiviert.

Der Grundsatz der Rechenschaftspflicht beabsichtigt, dass die Verarbeitung von PII die Pflicht zur Sorgfalt und zur Aneignung konkreter und praktischer Maßnahmen zum Schutz der PII mit sich bringt. Dies gilt für alle, die PII verarbeiten. Diese Maßnahmen sind nicht nur dazu vorgesehen, die Verarbeitung abzusichern, sondern auch die Aufsicht durch die zuständigen Behörden (z. B. Datenschutzbeauftragte) zu ermöglichen und zu vereinfachen.

Der Grundsatz der Informationssicherheit (s. auch Abschn. 24.4.1) erfordert z. B. Kontrollen auf der operationalen, funktionalen und strategischen Ebene, um die Integrität, Vertraulichkeit und Verfügbarkeit der PII sicherzustellen und sie über den gesamten Lebenszyklus hinweg gegen Risiken wie nicht autorisierten Zugriff, nicht autorisierte Vernichtung, nicht autorisierte Modifizierung, nicht autorisierte Veröffentlichung oder Verlust zu schützen.

Typischerweise ist es wichtig zu überprüfen, wer Zugriff auf die PII hatte oder hat und wer mit ihr auf welche Art und Weise arbeitete oder arbeitet. Daher werden für jede zusätzliche Entität, die möglicherweise einen Zugriff auf die PII hat, zusätzliche Überwachungsmaßnahmen anfallen. Erfahrungen mit Audit-Maßnahmen zeigten, dass diese zu zusätzlichen Datenschutzproblemen führen können, da Audit-Aufzeichnungen noch kritischer und diskriminierender als die PII selbst sein können. Ein Beispiel hierfür wäre ein Eintrag in der Audit-Aufzeichnung einer Verkehrszentrale, dass die PII zu den Reaktionszeiten eines bestimmten Fahrers in der Interaktion mit dem Fahrroboter durch eine Arbeitsgruppe eingesehen wurde, die gefährliches Fahrverhalten analysieren soll.

Darüber hinaus sollten zusätzliche Überwachungsmaßnahmen nicht zu übermäßiger Überwachung der Individuen führen, die mit dem System arbeiten, zumindest in den Rechtssystemen, die Arbeitnehmerdatenschutz vorsehen. Hier ist der Grat zwischen Kundendatenschutz und Arbeiternehmerdatenschutz besonders schmal und komplex.

24.4.3 Beschränkung von Zugriffsrechten und Einsatz von Verschlüsselung

Beschränkung von Zugriffsrechten und Einsatz von Verschlüsselung sind typische Instrumente der Informationssicherheit. Die Beschränkung von Zugriffsrechten folgt dem Grundsatz „Informationssicherheit“ in ISO/IEC 29100: Der Zugriff auf PII ist auf diejenigen zu begrenzen, die den Zugriff benötigen, um ihre Aufgaben zu erfüllen, und auf genau die PII, die sie für diese Aufgaben benötigen. Zugriffskontrollen können genau festlegen, wer auf welche PII zugreifen darf. Dies setzt eine detaillierte Spezifikation des Systems voraus und kann am besten erreicht werden, wenn Datenschutz schon in der Entwurfsphase berücksichtigt wurde, beispielsweise, wenn festgelegt wird, welche Daten durch das Fahrzeug gesammelt werden und für welche Anwendung sie benötigt werden.

Ein anderer Weg, Zugriffsrechte zu beschränken, ist festzulegen, dass Gruppen von Entitäten nur gemeinsam Zugriff auf bestimmte Daten erhalten (z. B. auf jegliche Art von Audit-Aufzeichnungen). Dieses Vier-Augen-Prinzip (oder n-Augen-Prinzip) schützt zu einem gewissen Grad vor unerlaubter Nutzung von Daten und kann insbesondere bei Audit-Aufzeichnungen zur Kontrolle des Systemverhaltens angewendet werden, wenn diese Aufzeichnungen auch PII beinhalten. Es kann beispielsweise festgelegt werden, dass diese Arten von Daten nur verfügbar gemacht werden, um einen genau beschriebenen Systemfehler zu adressieren, und dass PII-Prinzipal und die interessierte Partei (beispielsweise eine autorisierte Werkstatt) sich über den Zugriff einigen müssen. Das n-Augen-Prinzip

kann auch durch Verschlüsselung realisiert werden, indem Teile des Schlüssels unter den jeweiligen Stakeholdern verteilt werden.

Verschlüsselung wird in der ISO/IEC 29100 nicht direkt erwähnt, und ihr Nutzen wird in einigen ISO/IEC-Mitgliedsstaaten manchmal kontrovers diskutiert. Wohl aber wird Verschlüsselung als Beispiel für eine Anforderung an die Übermittlung medizinischer PII über öffentliche Netzwerke erwähnt ([8], Clause 4.4.7). Verschlüsselung wird auch mehr und mehr von Datenschutzbeauftragten gefordert, die ihren Mehrwert verstanden haben, insbesondere wenn es darum geht, die Speicherung und Übertragung von PII zu schützen, auch ohne sich auf diejenigen, die die PII physikalisch speichern oder transportieren, verlassen zu müssen. Wenn Verschlüsselung verwendet wird, ist es wichtig, klar festzulegen, wer die Schlüssel für die Ver- und Entschlüsselung besitzt. Es kann sich anbieten, PII, die Rückschlüsse auf das Verhalten und die Fähigkeiten eines PII-Prinzipals erlaubt, durch die Verwendung eines asymmetrischen Verschlüsselungssystems zu schützen. Die PII wird dann mittels des öffentlichen Schlüssels des jeweiligen PII-Prinzipals verschlüsselt. Dies stellt dann sicher, dass die PII nur durch den dazugehörigen privaten Schlüssel des PII-Prinzipals entschlüsselt werden kann.

24.5 Architekturüberlegungen

Architekturen zur Datenverarbeitung müssen Interessen der Stakeholder des Systems berücksichtigen. Die in diesem Beitrag bisher erwähnten PII-Stakeholder sind Fahrer, Mitfahrer und Besitzer der Autos. Weitere Stakeholder sind möglicherweise Individuen, die mit den PII arbeiten müssen, eventuell auch eigentlich Unbeteiligte oder andere Verkehrsteilnehmer, wenn sie vom System identifiziert werden können.[3] Es ist sinnvoll, insbesondere nicht professionelle Benutzer des Systems zu betrachten, da diese normalerweise weniger Möglichkeiten besitzen, sich selbst zu schützen [12]. Sie sind üblicherweise auch diejenigen, um die sich Datenschutzbeauftragte kümmern.

Im Allgemeinen können Architektureigenschaften von den in Abschn. 24.4.1 diskutierten Grundsätzen abgeleitet werden. Insbesondere die Grundsätze der Beschränkung der Erfassung, der Datenminimierung und der Informationssicherheit sind für Architekturen relevant. Eine Architektur, die die jeweiligen Dienste unter weniger Erfassung, Verwendung und Verbreitung von PII bereitstellt, mindert nicht nur die schädlichen Folgen eines Missbrauchs, sondern erleichtert auch die Sicherung der Informationen.

Drei Eigenschaften und Elemente von Architekturen sind besonders zu empfehlen:

1. Dezentrale Ansätze
   Wenn PII nicht zu zentralen Entitäten, wie Verkehrszentralen, transferiert wird, ist das Risiko des Missbrauchs reduziert. Beispiele hierfür sind:

3 Dies mag eine Motivation sein, das System so zu gestalten, dass Unbeteiligte und andere Verkehrsteilnehmer nicht identifiziert werden können.

- Wenn in einem der Use-Cases eine Situation direkt zwischen zwei Fahrzeugen geklärt werden kann, ist dies besser, als die Verkehrszentrale oder andere externe Entitäten einzubeziehen. Manchmal wird das Thema der Vertrauenswürdigkeit der durch andere Fahrzeuge bereitgestellten Informationen zur Sprache gebracht. Eine einfache Lösung hierfür scheint die individuelle Identifikation von Fahrzeugen und der Abgleich mit einer zentralen Registrierungsdatenbank zu sein, ähnlich wie ein Polizeiauto Kennzeichen von Autos überprüft. Dieses Szenario mag ein schönes Vermarktungsszenario für den Vertrieb von Verzeichnisdiensten sein, es aber als Gewinn für Datenschutz oder Sicherheit zu betrachten, wäre zu kurzsichtig. Das Szenario würde eine im Ausnahmefall stattfindende Polizeiaktivität zu einer regelmäßigen Aktivität machen, die möglicherweise von jedem Fahrzeug ausgeführt werden kann und so eine umfangreiche Massenüberwachungsinfrastruktur etablieren würde. Zudem gibt die Möglichkeit, Autos präzise zu identifizieren, keinerlei Garantie für die Informationen, die von diesem Fahrzeug bereitgestellt werden. Diese Informationen können auch dann manipuliert oder irreführend sein, wenn das Fahrzeug, das die Informationen bereitstellt, einen gültigen Identifikator vorweist.
- Das Konzept eines benutzereigenen „Private Data Vault“ (PDV) zur Speicherung von PII sollte näher untersucht werden, um die Speicherung sensitiver Daten unter Kontrolle der Nutzer zu ermöglichen. Ein PDV könnte die PII des jeweiligen Nutzers speichern und gegen ungewollten Zugriff schützen, sodass kein Zugriff ohne die Einwilligung des Nutzers möglich ist. Insbesondere für Fahrer, die sich ein Auto mit anderen Fahrern teilen, oder Kunden von Autovermietungen wäre dies sehr hilfreich. Ein PDV kann im Fahrzeug installiert werden (im speziellen Fall, dass das Fahrzeug nur von einem Fahrer verwendet wird) oder idealerweise vom jeweiligen Fahrer in das verwendete Auto mitgebracht werden. Das PDV sollte Hardware verwenden, die die gespeicherten Daten gut schützen kann und könnte die erste Version eines vertrauenswürdigen Datenspeichers sein. Eine Kombination mit anderen persönlichen Geräten wie Mobiltelefonen wäre eventuell in Zukunft möglich; zunächst aber müssen diese Geräte sicherer werden und besser in der Lage sein, sich selbst zu schützen, insbesondere gegen Angriffe, um Daten von außen auszulesen. Verwandte Konzepte existieren für die Berechnung von Straßenmaut, beispielsweise [13] und Pay-as-you drive-Versicherungen wie beispielsweise [14].
- Wenn nicht „nur“ PII des Benutzers des Autos, sondern auch Daten von anderen Parteien wie z. B. der Umgebung gespeichert werden, sollte das Vier- oder n-Augen-Prinzip zur Zugriffskontrolle angewendet werden.
- In Use-Case 2 sind Verkehrszentralen oder andere Entitäten in die Auswahl von Parkplätzen involviert. Diese Entitäten sollten Fahrer oder Mitfahrer nicht nach allen möglichen Prioritäten zu Parkplätzen und Routen ausfragen, sondern stattdessen Optionen anbieten, aus denen die Benutzer oder ein lokales Assistenzsystem wählen können. Dies reduziert das Risiko einer zentralen Verarbeitung von Einstellungen der Benutzer in Bezug auf Preise und ortsbezogene Präferenzen.

2. Anonymisierung
   Informationen, die zu einem gerechtfertigten Zweck erfasst werden, müssen nicht zwingenderweise so erfasst werden, dass das entsprechende Individuum identifizierbar ist. Selbst wenn die Informationen so erfasst werden, dass Individuen identifiziert werden können, müssen sie nicht auf diese Art und Weise weiterverarbeitet werden. Dies gilt insbesondere für jegliche Informationen, die nur in aggregierter Form benötigt werden:
   – Verkehrs- und Stauanalysen müssen keine individuellen Autos oder gar Fahrer identifizieren.
   – Die Interaktion zwischen Peers, etwa mit anderen Fahrzeugen Daten zur Verkehrssicherheit auszutauschen, benötigt keine Identifikation (s. die Diskussion unter 1. „Dezentrale Ansätze“ weiter oben).
   – Nicht einmal die Zugriffskontrolle für Autos (z. B. die Entscheidung über den Zugriff auf Parkplätze) benötigt eine individuelle Identifizierung der Autos. Die Konzepte Partieller Identitäten (ISO/IEC 24760-1, [15]) und Privatsphärenfreundlicher Attribute Based Credentials [16] erlauben eine Beschränkung der Informationen auf das, was wirklich benötigt wird, beispielsweise in Use-Case 2 auf die zertifizierte Information, dass ein Parkplatz für das autonome Valet-Parken von einem Fahrzeug gebucht wurde. Das Fahrzeug muss sich gegenüber der Zugriffskontrolle des Parkplatzes nicht individuell identifizieren. Die Übertragung eines Tokens, das das Fahrzeug nur dann identifiziert, wenn das Token missbräuchlich mehrfach verwendet wird, ist ausreichend.
3. Systematische Löschung von PII
   Die Löschung von Daten wird häufig in Konzepten und Lebenszyklusmodellen von IKT-Systemen vernachlässigt. Insbesondere im Fall von PII kann dies zu gefährlichem Missbrauch und entsprechenden Haftungsrisiken führen. Aus diesem Grund sollten bereits Architekturentwürfe in jedem Fall Konzepte zur systematischen Löschung von Daten beinhalten. Dies erfordert eine sorgfältige Überlegung, wie lange welche Daten zu welchem Zweck vorgehalten werden müssen. Beim Deutschen Institut für Normung (DIN) und auch in der ISO/IEC-Normung wurden Projekte zur Löschung von Daten diskutiert und teilweise gestartet (s. [17]). Diese Initiativen basieren zu einem großen Teil auf dem Konzept der Datenlöschung im Mautsystem Toll Collect für Lkw.

24.6 Was muss auf lange Sicht hin bedacht werden?

Es sieht danach aus, dass die Infrastrukturen für autonomes Fahren sehr groß und komplex werden und daher ein größerer Zeitraum für jede Planung zur Einführung, Verwendung und Wartung zu berücksichtigen ist. Daher sollten Anmerkungen zur längerfristigen Erfahrung im Bereich ICT und Datenschutz hilfreich sein:

1. Schleichende Erweiterungen des Anwendungsbereiches
   Hat sich eine technische Infrastruktur erst einmal für einige Anwendungen etabliert, können neue zusätzliche Anwendungen recht einfach auf derselben Technologie und Infrastruktur aufbauen. Damit können sich neue Datenschutzrisiken schnell einschleichen, speziell wenn die neuen zusätzlichen Anwendungen weitere PII verarbeiten. Dies hat sich z. B. beim Mobilkommunikationsnetz GSM gezeigt, das viele mächtige Funktionalitäten (z. B. Lokalisierung) besitzt, deren De-facto-Einführung und -Nutzung in manchen Ländern aber in einer Grauzone stattfand. Ähnliche Ängste bestehen für Mautsysteme und deren Überwachungsinfrastrukturen, die in mehreren Fällen nur für Lkw oder andere überwiegend beruflich genutzte Fahrzeuge etabliert wurden. Eine Erweiterung auf privat genutzte Fahrzeuge ist dann oft sehr einfach zu realisieren.
2. Schleichende Übergänge von Test-Systemen zu Wirksystemen
   Erfahrungen der internetorientierten Softwareentwicklung zeigen, dass der Schritt von einem Test-System oder gar einem experimentellen Prototypen mit reduzierten oder gar keinen Datenschutz- und Datensicherheitsvorkehrungen zu einem Wirksystem heutzutage sehr einfach ist, etwa durch das Ändern eines Weblinks in einem öffentlichen Portal, damit der Link auf ein neues Backend-System zeigt. Eine solche Änderung kann dazu führen, dass Testsysteme zu Wirksystemen werden, obwohl sie noch lange nicht angemessen geschützt sind. Insbesondere Projekte, die unter Ressourcenknappheit leiden und einen schnellen Erfolg benötigen, können dieser Versuchung erliegen.
3. Verbindliche pseudo-eindeutige Identifizierung
   Mehr und mehr Computer speichern und verteilen Identifikatoren, die diese Geräte als mehr oder weniger einmalig und vertrauenswürdig identifizieren. Ein Beispiel hierfür ist die GSM International Mobile Station Equipment Identity (IMEI). Theoretisch ist die IMEI ein eindeutiger Identifikator für jedes Mobilkommunikationsgerät. Praktisch gesehen kann diese IMEI aber manipuliert werden. Ähnlich ist es in internetorientierten Netzen bei der Media Access Control Address (MAC-Adresse), die jeder Netzwerkschnittstelle als theoretisch eindeutiger Identifikator zugeteilt ist. Beide Identifikatoren sind auch für Fahrzeuge, die mit entsprechenden Kommunikationstechnologien ausgestattet sind, einschlägig. Während diese Identifikatoren zur Identifizierung von Angreifern sehr wenig nutzen, weil sie recht einfach manipuliert werden können, machen sie (inoffizielle) Datensammlungen sehr einfach und schaffen dadurch ein erhebliches Datenschutzproblem. Ferner wecken sie einen wiederkehrenden „Appetit“ interessierter Parteien auf mehr Identifikation von Benutzern in Kommunikationsnetzwerken oder bei Internetdiensten. Im Interesse eines effektiven Datenschutzes muss dieser Trend erkannt, berücksichtigt und überwunden werden [18].

24.7 Fazit

Man könnte annehmen, dass ein höheres Maß an Autonomie beim Fahren zu mehr Datenverarbeitung und dadurch auch zu mehr Überwachung führen würde. Tatsächlich ist dies aber nicht notwendigerweise der Fall. Die hauptsächlichen Faktoren, die zur Erfassung und Verbreitung zusätzlicher Daten beim autonomen Fahren führen, sind:

1. Die Interaktion zwischen Fahrzeug und Fahrer(n), Passagier(en) und gegebenenfalls Eigentümer(n) wird intensiver, was zur Speicherung und Verarbeitung zusätzlicher Daten führt.
2. Die Interaktion des Fahrzeugs mit anderen Entitäten, insbesondere Verkehrszentralen, wird intensiver, was zu zusätzlichen Übermittlungen potenziell sensitiver Daten aus dem Fahrzeug heraus führt.

Ein autonom fahrendes Fahrzeug, das so autonom fährt, dass es nicht mit dem Fahrer zu interagieren braucht, muss nicht mehr Daten von einem Fahrer erfassen als ein herkömmliches Auto. Auch wenn das Fahrzeug in der Lage ist, autonom durch den Verkehr zu navigieren, würde es nicht mehr Daten kommunizieren als irgendein anderes Auto. Gegebenenfalls würde es sogar weniger Daten kommunizieren als ein herkömmliches Auto, das ein zentralisiertes Navigationssystem einsetzt und unter Überwachung steht, beispielsweise durch ein System, das fortwährend die Geokoordinaten des Fahrzeugs sammelt.

Natürlich können einige der realitätsnahen Zwischenszenarien, wie z. B. der Kontrollübergang an den Fahrer in kritischen Situationen (s. z. B. Use-Case 1) in Kombination mit einer zentralisierten Überwachung in solchen kritischen Situationen zu mehr Überwachung und dann auch zu mehr Datenschutzproblemen führen. Während also autonomes Fahren theoretisch nicht zu mehr Datenschutzproblemen führen muss, gibt es eine realistische Bedrohung, dass in der Praxis genau das passiert, wenn Entwurf und Architektur der Systeme Datenschutzprobleme nicht sorgfältig verhindern.

Daher ist ein Privacy-by-Design-Ansatz für autonomes Fahren und die einschlägigen Szenarien nötig. Zumindest die folgenden Fragen müssen gründlich geprüft werden:

- Ist die Erfassung, Verarbeitung und Übermittlung von Daten wirklich notwendig, um eine tatsächliche Verbesserung der Fahrsituation zu erreichen?
- Ist dieser Vorteil die zusätzlichen Datenschutzrisiken wert?
- Können die PII-Stakeholder (häufig Fahrer, Fahrgäste, Eigentümer) ertüchtigt werden, in einem möglichen Dilemma zwischen mehr Funktionalität oder mehr Verkehrssicherheit auf der einen Seite und weniger Privatsphäre auf der anderen Seite informiert und selbstständig zu entscheiden?
- Bleiben die Daten unter Kontrolle der PII-Stakeholder, oder verlassen sie deren Einflussbereich?

Es gibt eine klare Herausforderung, die Freiheit, die seit langer Zeit mit dem Automobil verbunden wird und ein Grund für seinen Erfolg ist, zu schützen.

Ein mögliches Alleinstellungsmerkmal für die etablierte Automobilindustrie und vor allem für Premium-Hersteller und -Marken ist es, nicht einfach dem Trend der Internetunternehmen zu folgen und Informationen überallhin fließen zu lassen, bis man vom Regulator oder empörten Kunden gestoppt wird, sondern einen hinreichenden Privatsphärenschutz für ihre Kunden zu ermöglichen. Gerade die Automobilindustrie hat in anderen Bereichen wie der Reduktion des Energieverbrauchs gezeigt, dass man primitive Lösungen nicht akzeptieren muss, sondern negative Auswirkungen überwinden und Ressourcen schonen kann, indem man sorgfältig plant und entwickelt. Über kurz oder lang wird dieser Ansatz in jedem Fall angeregt oder gefordert werden.

Danksagung

Dank gebührt Tim Schiller, Jetzabel Serna-Olvera und Markus Tschersich für hilfreiche Hinweise und Kommentare und Marvin Hegen und Markus Tschersich für die Hilfe bei der Übersetzung ins Deutsche.

Literatur

1. Helmut Käutner, Ernst Schnabel: In jenen Tagen; Camera-Filmproduktion 1947; mehr Information unter http://de.wikipedia.org/wiki/In_jenen_Tagen_%281947%29; zuletzt aufgerufen 2014-08-15
2. Angelina Göb: “Nimm Zwei – Carpool Lanes”; 2013-08-06; www.urbanfreak.de/carpool-lanes/, zuletzt aufgerufen 2014-08-15
3. Telematics News: eCall in German privacy debate; veröffentlicht: 01 February 2012; http://telematicsnews.info/2012/02/01/ecall-in-german-privacy-debate_f3011/; zuletzt aufgerufen 2014-08-15
4. Jan Philipp Albrecht: eCall – Überwachung aller Autofahrten muss gestoppt werden; www.greens-efa.eu/ecall-11553.html; zuletzt aufgerufen 2014-08-15
5. European Parliament: Decision of the European Parliament and of the Council on the deployment of the interoperable EU wide eCall service; P7_TA-PROV(2014)0359; http://www.europarl.europa.eu/RegistreWeb; zuletzt aufgerufen 2014-08-15
6. Deutsche Bundesregierung: Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (18. Mai 1995, BGBl. I S. 722)
7. Eric Schmidt, Jared Cohen: The New Digital Age: Reshaping the Future of People, Nations and Business; Alfred A. Knopf 2013, ISBN-10: 0307957136
8. ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework, First edition, 2011-12-15, kostenlos via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
9. 52. Deutscher Verkehrsgerichtstag 2014, 29. bis 31. Januar 2014 in Goslar, Arbeitskreis VII: Wem gehören die Fahrzeugdaten? www.deutscher-verkehrsgerichtstag.de/images/pdf/empfehlungen_52_vgt.pdf; zuletzt aufgerufen 2014-08-29

10. Bundesverfassungsgericht: Volkszählungsurteil: Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83; www.servat.unibe.ch/dfr/bv065001.html und Mitglieder des Bundesverfassungsgerichts (Hrsg.): Entscheidungen des Bundesverfassungsgerichts. 65, Mohr, Tübingen, S. 1–71, ISSN 0433-7646
11. Wikipedia: Global surveillance disclosures (2013–present); http://en.wikipedia.org/wiki/Global_surveillance_disclosure; zuletzt aufgerufen 2014-08-14
12. Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151–162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19–21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3
13. Josep Balasch, Alfredo Rial, Carmela Troncoso, Christophe Geuens, Bart Preneel, and Ingrid Verbauwhede: PrETP: Privacy-Preserving Electronic Toll Pricing. Pp. 63–78 in Proceedings of the 19th USENIX Security Symposium, USENIX, 2010
14. Carmela Troncoso, George Danezis, Eleni Kosta, Josep Balasch, and Bart Preneel: PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance. Pages 742–755 in IEEE Transactions on Dependable and Secure Computing – IEEE TDSC 8(5), IEEE, 2011
15. ISO/IEC 24760-1:2011 Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts, First edition, 2011-12-15, kostenlos via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
16. Ahmad Sabouri, Ioannis Krontiris, Kai Rannenberg: Attribute-based credentials for Trust (ABC4Trust); Pp. 218–219 in Simone Fischer-Hübner, Sokratis K. Katsikas, Gerald Quirchmayr (Eds.): Trust, Privacy and Security in Digital Business – 9th International Conference, TrustBus 2012, Vienna, Austria, September 3–7, 2012; Springer Lecture Notes in Computer Science ISBN 978-3-642-32286-0; siehe auch www.abc4trust.eu
17. Volker Hammer, Karin Schuler: „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“, Version 1.0.2, Stand 25. Oktober 2013; www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/DINLoeschkonzeptLeitlinie.pdf
18. Kai Rannenberg: Where Security Research Should Go in the Next Decade. Pp. 28–32 in Willem Jonker, Milan Petkovic (Eds.): Secure Data Management – 10th VLDB Workshop, SDM 2013, Trento, Italy, August 30, 2013, Post-Proceedings; 2014; Springer Lecture Notes in Computer Science 8425, ISBN 978-3-319-06810-7