International Working Group
on Data Protection
in Telecommunications

675.38.15 13. März 2009

Bericht und Empfehlungen zu Mautsystemen

-"Sofia Memorandum"-

45. Treffen, 12.-13. März, Sofia (Bulgarien)

-Übersetzung-

Empfehlungen:

Die Arbeitsgruppe empfiehlt, dass die Hersteller von großangelegten Mautsystemen, die persönliche Daten verarbeiten, die folgenden Empfehlungen zum Schutz der Privatsphäre der Fahrer und der Fahrzeugeigentümer einhalten:

- Die Anonymität der Fahrer kann und sollte durch die Verwendung der sogenannten "Smart-Clients" oder anonymen Proxies gewahrt werden, die die persönlichen Daten der Fahrer unter deren alleiniger Kontrolle halten und keine Speicherung der Daten außerhalb des Fahrzeugs erfordern.
- Mautsysteme können und sollten so entworfen werden, dass die detaillierten Routendaten gänzlich und dauerhaft aus dem System gelöscht werden, nachdem die Gebühren festgesetzt wurden, um zu vermeiden, dass Bewegungsprofile erstellt oder die Daten zweckentfremdet werden.
- Die Verarbeitung von persönlichen Daten zu anderen Zwecken (z.B. "pay-as-you-drive“-Versicherungen oder verhaltensbasierte Werbung) sollte nur mit der eindeutigen und ausdrücklichen Einwilligung des Betroffenen möglich sein.
- Im Hinblick auf die Durchsetzung sollte das System die Identität der Fahrer oder Fahrzeugbesitzer nicht feststellen, solange nicht der Verdacht besteht, dass der Fahrer eine Zuwiderhandlung begangen hat, die als Verstoß gegen das Mautsystem definiert wird.

Hintergrund:

Großangelegte Mautsysteme, die auf einer "pay as you go"-Basis im fließenden Verkehr angelegt sind, sind keine neue Erfindung. Überlegungen zu elektronischen Mautsystemen kamen in den letzten Jahrzehnten des 20. Jahrhunderts auf[i]. Verschiedene Begriffe werden verwendet, um die Nutzung moderner Informations- und Kommunikationstechnologien für Mautsysteme zu beschreiben; dazu gehören „elektronische Verkehrsgebühr“, „Intelligente Verkehrssysteme“ (IVS), „elektronische Mauterhebung“, "Straßennutzungsgebühr", „Zeit-, Entfernungs-, Ortsgebühren“, „entfernungsbasierte Straßennutzungsgebühr“, "vehicles miles travelled (VMT) charging" und verschiedene weitere.

Bestehende Mautsysteme können Gebühren auf Autobahnen erheben oder eine Abgabe verlangen, wenn eine bestimmte Zone mit dem Fahrzeug befahren wird. Sie sind jedoch nicht in der Lage, Gebühren mittels eines Algorithmus zu errechnen, der an "Zeit, Strecke und Ort" gebunden ist, was für großangelegte Anwendungen erforderlich wäre. Das erwünschte Resultat eines elektronischen Mautsystems ist die Möglichkeit, nach der *tatsächlichen* Nutzung abrechnen zu können (z.B. je mehr man fährt, desto mehr zahlt man), in Abhängigkeit von der Uhrzeit der Fahrt (z.B. weniger in Zeiten außerhalb des Berufsverkehrs) und in einem variierenden Tarif, der sich anhand der gewählten Straße

ermitteln lässt. Der Verkehrsfluss könnte in diesen Systemen dadurch verbessert werden, dass die Fahrer nicht gezwungen wären, an bestimmten Abrechnungsstellen anzuhalten. Prinzipiell wäre dies die gerechteste und ökologisch wünschenswerteste Möglichkeit zu bezahlen - so wie Verbraucher gewöhnlich für ihren Wasser- oder Stromverbrauch zahlen.

Abgesehen von Mautgebühren gibt es zahlreiche andere Dienste, die auf Daten in Bezug auf Zeit, Ort und zurückgelegte Strecke basieren, wie zum Beispiel Parksysteme, "pay-as-you-drive"-Versicherungen, Parkplatzfinder oder -versteigerer, die Rationierung von Straßenraum, Parkplatz-Treue-Programme, Staumelde- und Gebührensysteme, Routenplaner ("Sie könnten 12 € pro Woche sparen, wenn Sie jeden Tag 30 Minuten früher losfahren würden") und intelligente Transportsysteme ("Wenn Sie heute die A2 nutzen statt der A3, sparen Sie 20%"). Während die elektronische Erhebung und Verarbeitung von Daten in Bezug auf den Ort, die Identifikation einer Person sowie die Reisedaten schon heute für verschiedene Zwecke genutzt werden kann und somit auch mehrere sozioökonomische Probleme hervorruft, bezieht sich dieses Dokument vornehmlich auf datenschutzrechtlich relevante Auswirkungen von (großangelegten) elektronischen Mautsystemen.

Um besser nachvollziehen zu können, worin die datenschutzrechtlichen Auswirkungen bestehen, müssen einige der Grundprinzipien dieser Systeme näher betrachtet werden. Großangelegte Maut-Initiativen, die die Verarbeitung persönlicher Daten implizieren (andere als z.B. bei Vignetten, anonymen Aufklebern und Signalen sowie Gebührensysteme mit Mautstationen, die keinen freien Verkehrsfluss ermöglichen) werden weltweit entwickelt, z.B. in den USA (Oregon und der Puget Sound Region), Australien, Neuseeland, Kanada (auf der Schnellstraße 407), das Toll Collect System in Deutschland [2] und die in den Niederlanden[3] und Norwegen bestehenden Mautpläne. In der EG wird darüber hinaus mit der Richtlinie 2004/52/EG das Ziel verfolgt, das "pay as you go"-Prinzip im freien Verkehrsfluss in den zukünftigen Europäischen Elektronischen Mautdienst (European Electronic Toll Service - EETS) einfließen zu lassen. In seiner letzten Stufe der Entwicklung soll dieses europaübergreifende System die Möglichkeit bieten, Verkehrsgebühren für alle Arten von Straßen einschließlich Viadukten, Tunneln und anderen Objekten zu erheben. Mit dem neuen Abrechnungssystem sollen Fahrer die Gebühren zahlen können, ohne anhalten zu müssen und dadurch Verkehrsstauungen zu verursachen. Gleichzeitig ermöglicht es diese Einrichtung auch, Gebühren für alle kostenpflichtigen Autobahnen in Europa zu erheben.

Der Grund, warum die Debatten über Straßennutzungsgebühren so emotional aufgeladen sind, liegt darin, dass ortsbezogene Daten, Daten zur Identifikation und Abrechnungsdaten zusammengeführt werden. Mit anderen Worten, es wird bekannt, wer zu welcher Zeit wo war, um dafür Gebühren abzurechnen. Um das „pay as you go“-Prinzip im freien Verkehrsfluss umzusetzen (und um über ein interoperatives System zu verfügen), können Mautsysteme eine massive Überwachung der Bewegung von Personen (Fahrzeuginhaber und Fahrer) mit sich bringen. Daher müssen die Auswirkungen auf die Privatsphäre der Betroffenen sorgfältig untersucht werden. Es ist nicht schwierig, sich den enormen Wert einer zentralisierten Datenbank über das Bewegungsverhalten von Fahrern und zahlreiche Szenarios für eine Zweckentfremdung der Daten vorzustellen, bei denen Daten für andere Zwecke genutzt werden als die für die sie ursprünglich erhoben wurden (z.B. Mautgebühren). Zahlreiche Datenschutzbeauftragte haben bereits Stellungnahmen und Empfehlungen zum Schutz der Privatsphäre im Zusammenhang mit Mautsystemen erstellt (z.B. Ontario[4], Niederlande[5], Victoria/Australien[6], Norwegen[7] und Slowenien[8]). Fehlwahrnehmungen hinsichtlich der Auswirkungen auf die Privatsphäre werden tatsächlich häufig als eines der größten Hindernisse für die Einführung großangelegter Mautsysteme betrachtet.

Grundsätzlich werden zwei etablierte Technologien für diese Systeme in Erwägung gezogen: short range communications (DSRC[9], das auch als „tag-beacon-System“ bezeichnet wird) und globale Satellitennavigationssysteme (GNSS/SN[10]), welche die Position des Fahrzeugs

bestimmen und die Daten über leistungsstarke drahtlose Kommunikationsnetzwerke übertragen, wobei das letztgenannte oftmals als satellitengestütztes Mautsystem bezeichnet wird.

Jedes dieser Systeme hat seine Vor- und Nachteile: die DSRC-basierten technischen Lösungen sind z.B. weiter verbreitet und wurden häufiger getestet, aber sie sind nicht auf allen Straßen anwendbar.[11] Die Wahl der Technologie hängt hauptsächlich von der Größe der Implementierung ab und unterscheidet sich in der Umsetzung nach relativ kleinen Gebieten (z.B. Großstädte[12]) und großen Gebieten (z.B. landesweit oder sogar international). Im Hinblick auf großangelegte Implementierungen scheint die DSRC-basierte Technologie an Boden zu verlieren. Wegen der enormen Anzahl an abzudeckenden Straßen sind Lösungen, die beträchtliche Infrastrukturen am Straßenrand erfordern, wie bestehende DSRC-basierte Umsetzungen, nicht so sehr geeignet, wenn auf allen Straßen Gebühren erhoben werden sollen.[13] Diese Sichtweise wird auch in einem neuen Bericht der National Surface Transportation Infrastructure Financing Commission der USA wiedergegeben.[14] Der Vorteil eines Satellitensystems besteht in seiner Flexibilität, wobei solche Systeme auf der anderen Seite noch nicht umfassend in der Praxis getestet wurden.

Die Verwendung elektronischer Mautsysteme ist, - die vielen sozio-ökonomischen Debatten und Probleme außer Acht lassend - oftmals durch zwei gebräuchliche datenschutzrechtliche Fehleinschätzungen gehemmt, die von der allgemeinen Öffentlichkeit und der Presse vertreten werden und denen entschieden entgegengetreten werden muss.

Erstens betont die Arbeitsgruppe, es muss keine Befürchtungen der Art geben, dass GPS-basierte Ansätze bedeuten würden, dass eine allumfassende Datenbank über die Position von Fahrzeugen in einer „Big Brother im Himmel"-Manier aufgebaut würde. Das GPS der USA, das russische GLONASS sowie das zukünftige Satellitensystem Galileo basieren auf passiven Empfängern, die unter Verwendung von Satelliteninformationen den Aufenthaltsort des Fahrzeugs berechnen; diese Empfänger können die Information über den Aufenthaltsort des Fahrzeugs nicht zurück zum Satelliten übermitteln. Daher müssen wir verstehen, wenn die Entscheidung für ein Satellitensystem fallen soll, dass durch Satellitennavigation ein Fahrzeug lediglich die Information über seine Position erhält, während die Ortsangaben an die Kontrollstelle des Mautabrechnungssystems über drahtlose Netzwerke übermittelt werden, so z.B. durch das GSM-Netz. Eine allumfassende Datenbank mit ortsbezogenen Daten und Identifikationsdaten könnte daher nur „vor Ort" in den Kontrollstellen entstehen: Genau davon handelt dieses Dokument.

Zweitens wird häufig der Vergleich zu Mobiltelefonen oder zu Kreditkarten gezogen, wo persönliche Daten nachverfolgt werden oder nachverfolgt werden können. Die Arbeitsgruppe möchte hervorheben, dass vereinfachende Vergleiche dieser Art nicht angemessen sind, vor allem weil Gebührenerfassungsgeräte ununterbrochen in Betrieb sein müssen (zumindest auf kostenpflichtigen Straßen), anders als im Fall von Mobiltelefonen, deren Benutzung völlig freiwillig ist. Die Möglichkeit, das Gerät auf kostenpflichtigen Straßen abzuschalten, würde es einfacher machen, die Gebührenerfassung zu umgehen, und aus diesem Grund werden die Auswirkungen von Mautsystemen auf die Privatsphäre sogar noch relevanter.

Die Verteilung des Abrechnungsprozesses

Der Abrechnungsprozess ist in vier Phasen unterteilt:

1. Bestimmung der Position des Fahrzeugs,
2. Bestimmung des Abschnitts der Straße oder Gebührenelements und des dazugehörigen Tarifs,
3. Berechnung des Betrags, der für diesen Bereich fällig wird,
4. Berechnung des Gesamtbetrages, der für die ganze Fahrt fällig wird.

Ein entscheidender Faktor, wenn man die datenschutzrechtlichen Auswirkungen bestimmen möchte, ist, wie die Phasen des Abrechnungsprozesses zwischen den verschiedenen datenverarbeitenden Stellen verteilt werden. Die vier Phasen des Abrechnungsprozesses können entweder von einer Stelle vorgenommen oder zwischen zwei oder mehreren aufgeteilt werden. Konsequenterweise unterscheiden sich die datenschutzrechtlichen Auswirkungen der verschiedenen Ausführungsmodelle. Einige der Modelle werden im Folgenden vorgestellt, zusammen mit den wichtigsten Kriterien, die beachtet werden müssen, wenn man die datenschutzrechtlichen Auswirkungen ermitteln möchte. Die zwei Hauptmodelle für Mautsysteme werden als **Thin-Client-Ansatz** und **Smart-Client-Ansatz** bezeichnet; allerdings gibt es zwischen diesen beiden Systemen noch andere Modelle**,** so wie der sogenannte Distributed-Role-Ansatz und Proxies. Diese vier Ansätze werden im Folgenden diskutiert.

Der „Thin-Client"-Ansatz

Die im Hinblick auf den Schutz der Privatsphäre am wenigsten favorisierte Variante eines Mautsystems liegt vor, wenn alle Daten über die Reisezeit und die Position der Fahrzeuge an eine einzige Stelle oder Institution, die als Kontrollzentrum agiert, gesendet und dort gespeichert werden. Der sogenannte „Thin-Client" (oder „On-Board-Unit" - OBU) sammelt nur Daten über zurückgelegte Strecken; alle vier Phasen des Abrechnungsprozesses werden durch die Kontrollstelle unter Verwendung einer zentralen Datenbank mit ortsbezogenen Daten, Identifikationsdaten und Abrechnungsdaten verarbeitet.

Die Arbeitsgruppe äußert ihre Bedenken hinsichtlich der Übernahme dieses Ansatzes, denn er bietet offensichtlich den geringsten Schutz für die Privatsphäre der Betroffenen. Im Prinzip ist die Frage, ob man „Thin-Clients" oder „Smart-Clients" bevorzugt, eine Frage von zentralisierter gegenüber dezentralisierter Datenverarbeitung, ein Dilemma, dem der Schutz der Privatsphäre und der Datenschutz oft begegnet.

Die Befürworter einer zentralisierten Datenbank behaupten, wenn die Daten geschützt durch angemessene Maßnahmen zur Datensicherung (z.B. entsprechende Zugangskontrolle, Protokollierung der Verarbeitung persönlicher Daten usw.) zentral gespeichert werden, könne ein höheres Sicherheitslevel gewährleistet werden, als es eine Einzelperson tun könne. Ein Gegenargument ist allerdings, dass dort, wo die Daten unter der Kontrolle eines Einzelnen sind, nur dessen Daten gefährdet sind (z.B. wenn das Fahrzeug oder das im Fahrzeug installierte Gebührenerfassungsgerät gestohlen wurden), wohingegen in dem zentralisierten Verarbeitungssystem persönliche Daten potentiell aller Betroffenen gefährdet sind (trotz eines möglicherweise höheren Grades an Sicherheit). Aus diesem Grund sind aus der Perspektive des Schutzes der Privatsphäre Lösungen zu befürworten, wo persönliche Daten nicht zentralisiert gespeichert werden, sondern im Besitz und unter der Kontrolle des Nutzers bleiben. Darüber hinaus begegnen Datenschützer regelmäßig dem Problem der zweckfremden Nutzung (dem sog. „function creep"-Phänomen) – dabei werden Daten, die ursprünglich für einen bestimmten Zweck erhoben wurden (der völlig legitim und gesetzeskonform sein kann), später für einen völlig anderen Zweck genutzt, ein Zugriff auf die Daten ist vorher unvorhergesehenen Dritten möglich, usw.

Der „Distributed-Role"-Ansatz

Manche Modelle schlagen den sogenannten Distributed-Role-Ansatz vor, der vermutlich einen besseren Schutz der Privatsphäre und der persönlichen Daten bietet. Der Distributed-Role-Ansatz stellt eine Lösung dar, die auf dem Prinzip basiert, die Daten zwischen zwei Stellen oder Parteien zu verteilen, wobei eine Partei die ortsbezogenen Daten und die Abrechnungsdaten hat und die andere nur die Identifikationsdaten der Fahrer.

Die erste Stelle oder Partei verfügt über die Identifikationsnummer des Geräts, das sich im Fahrzeug befindet, und empfängt Informationen über die Strecke, die das Fahrzeug

zurücklegt (Fahrtdauer und Position), weiß aber nicht, wer der Inhaber des Geräts ist. Basierend auf diesen Informationen berechnet diese Partei die fälligen Gebühren. Die Ergebnisse dieser aggregierten Berechnungen (nur die Gebührensumme in einer bestimmten Periode, ohne Informationen über Fahrtzeit und Position) werden zusammen mit der Identifikationsnummer des Geräts an eine andere Partei übermittelt, die den Besitzer des Gerätes identifizieren kann, von dem dann die Gebühr erhoben wird; jedoch sammelt diese zweite Partei keine Informationen über die Reise des Fahrzeugs. Die Befürworter dieses Ansatzes berufen sich häufig darauf, dass durch die Verteilung der Rollen insgesamt keine Verarbeitung personenbezogener Daten stattfindet. Die Arbeitsgruppe stellt eine solche Begründung allerdings in Frage, denn eine große Menge an personenbezogenen Daten wird immer noch von den verschiedenen Parteien verarbeitet.

Diese Lösung schützt die Privatsphäre eines Betroffenen nur scheinbar, auch wenn eine Partei nur die Information über die Position des Fahrzeuges und die Reisedauer sammelt und die Identität des Fahrers nicht kennt und umgekehrt. Innerhalb dieses Ansatzes werden immer noch von einer Stelle große Mengen an Daten gesammelt und verarbeitet; nur die Identifikationsdaten werden einer anderen Stelle oder Partei anvertraut. Die Arbeitsgruppe verweist auf die Stellungnahme der Artikel 29-Datenschutzgruppe, wonach Daten, die auf eine identifizierte oder identifizierbare natürliche Person beziehbar sind, wie personenbezogene Daten behandelt werden müssen und dass die Identifizierbarkeit eines Betroffenen nicht nur durch die Mittel und Ressourcen einer datenverarbeitenden Stelle (in diesem Fall die erste Partei) zu bestimmen ist, sondern in einem generelleren Sinn. Die datenverarbeitende Stelle sollte voraussehen, dass „die Mittel, die wahrscheinlich und vernünftigerweise genutzt werden“, um eine Person zu identifizieren, verfügbar sein werden, wie z.B. durch die angerufenen Gerichte (anders würde das Erheben der Daten keinen Sinn machen) und daher sollten diese Information als personenbezogene Daten behandelt werden. Unabhängig davon, ob die erste Partei einen Betroffenen, auf den sich die Orts- und Zeitangaben beziehen, selbst zu identifizieren vermag oder nicht, verarbeitet diese Partei unzweifelhaft personenbezogene Daten. Um dies zu untermauern: Es ist offensichtlich, dass in Fällen, in denen die Straßennutzungsgebühr nicht gezahlt wurde oder die Person sich geweigert hat, die Gebühr zu zahlen, der Gläubiger einen schnellen und einfachen Weg finden muss, die Kalkulation der Gebühr zu reproduzieren, was es erforderlich macht, die Daten über die Fahrtzeit und Position einer identifizierbaren Person zu verarbeiten. Darüber hinaus ist eine Zweckentfremdung („function creep“) der Daten erneut sehr wahrscheinlich, denn große Mengen von Daten werden zentral gespeichert.

Der „Smart-Client“-Ansatz

Um den Schutz der Privatsphäre der Betroffenen sicherzustellen, wäre sicherlich ein System am meisten geeignet, in dem die Daten, die zum Zweck der Mauterhebung erforderlich sind, ausschließlich unter der Kontrolle der Nutzer stehen. In diesem Fall würde die Berechnung der Gebühr durch das Gerät (das sogenannte *intelligent device*) erfolgen, wobei die Kontrollstelle nur die Summe der anfallenden Gebühren empfangen würde. Dies bedeutet, dass alle vier Abrechnungsphasen innerhalb dieses Gerätes erfolgen würden: Bestimmung der Position des Fahrzeugs; Bestimmung des Abschnitts der Straße oder Gebührenelements und des dazugehörigen Tarifs; Berechnung des Betrags, der für diesen Bereich fällig wird und Berechnung des Gesamtbetrages, der für die ganze Fahrt fällig wird.

Die Anonymität des Fahrers würde auf diesem Weg gewahrt, weil alle Daten über Position und Fahrtzeit unter der alleinigen Kontrolle des Nutzers stünden. Die Nutzer sollten sich nur selbst identifizieren, wenn gewisse Unregelmäßigkeiten auftreten, die eine Identifizierung erforderlich machen: z.B. wenn der Nutzer eine richtig berechnete Mautgebühr nicht gezahlt hat, das Fahrzeug gestohlen wurde oder wenn das Gebührenerfassungssystem des Nutzers kaputt ist oder nicht richtig funktioniert (während des Befahrens einer kostenpflichtigen Straße). Die Kontrollstelle muss nur Gewissheit darüber haben, dass das Gerät im Fahrzeug, das die Gebühren berechnet, auf kostenpflichtigen Straßen richtig arbeitet.

In einem solchen System hat die Kontrollstelle keine Daten über die Position des Fahrzeugs; sie kontrolliert nur, ob das Gerät richtig funktioniert. Dieses System erfordert natürlich einige operative Maßnahmen, wie den Schutz der Einrichtungen vor Betrug (dies umfasst die Blockierung, Verfälschung, Abschirmung, Modifikation, absichtliches Herbeiführen einer Fehlfunktion etc.). Ein sehr wichtiger Aspekt sowohl des Thin- als auch des Smart-Clients ist, dass sie nicht durch den Benutzer abgeschaltet werden können, sofern sich das Fahrzeug auf einer kostenpflichtigen Straße befindet, denn das wäre eine Umgehung der Zahlungspflicht. Der Smart-Client-Ansatz ist nicht ohne Herausforderungen, es ist zum Beispiel notwendig, passende Zertifizierungsstandards anzubieten, eine richtige Installation und die Wartung der Geräte zu gewährleisten und außerdem einige andere technische Aspekte zu beachten (z.B. Energieversorgung, Funktionskontrolle, Speicherkapazitäten) und - wahrscheinlich der wichtigste Aspekt - die Kosten.

Während der Smart-Client-Ansatz kostenintensiver erscheint als der sogenannte Thin-Client-Ansatz, hat der Smart-Client-Ansatz auch gewisse ökonomische Vorteile: Das „intelligente“ Gerät ist nicht anfällig für Kommunikationsstörungen (z.B. in Regionen, in denen kein GSM-Signal verfügbar ist) oder wenn die Kontrollstelle temporär nicht betriebsbereit ist, weil der Smart-Client die Gebühr selbst errechnen kann. Auf der anderen Seite kann das Gerät, das permanent Daten an die Kontrollstelle sendet und von der Kalkulation der Kontrollstelle abhängig ist (der Thin-Client) in Gebieten, in denen keine GSM-Abdeckung vorliegt oder wenn die Kontrollstelle nicht arbeitet, die Gebühr nicht allein errechnen. Es ist auch hervorzuheben, dass das „intelligente“ Gerät auch Operationen im Thin-Client-Modus unterstützen kann (metaphorisch gesprochen kann der „dumme“ Client nicht „intelligent“ werden, während das Umgekehrte möglich ist), was eine bedeutende Voraussetzung für die Interoperabilität der Systeme ist (z.B. innerhalb des zukünftigen europäischen elektronischen Mautservices) oder mit anderen zuvor bestehenden städtischen Gebührensystemen oder City-Maut Systemen. Die Geräte in den Fahrzeugen müssen wissen, wie sie auf unterschiedliche Systeme reagieren sollen: Nachdem die Zone eines anderen Betreibers erreicht wurde, wird das Gerät Anweisungen erhalten, wie es zu arbeiten hat. Internationale Standardisierungsorganisationen (ISO und CEN) entwickeln passende technische Standards, während die Industrie bereits funktionierende Lösungen getestet hat. Während ökonomische Faktoren für die Einführung eines bestimmten Systems entscheidend sind, beeinflussen sie die datenschutzrechtlichen Implikationen nicht. Der vermeintliche Nachteil für einen Smart-Client könnte durch Massenproduktionen oder Anreize (z.B. durch die Kombination eines Freisprechmobiltelefons oder eines Satellitennavigationssystems mit dem Gerät) minimiert werden.

Der Smart-Client könnte auch eine anonyme Nutzung erleichtern, wenn Pre-Paid-Lösungen wie beim Mobiltelefon angeboten würden. Ein Fahrer sollte die Möglichkeit haben, ein Gebührenguthaben zu kaufen, das mit der On-Board-Einheit verwendet werden könnte, die dann die Kontrollstelle informieren könnte, dass die Gebühren für den Straßenabschnitt bereits vorab gezahlt wurden.

Proxies

Es sind auch weitere gemischte Ansätze bekannt und schon jetzt auf dem Markt erhältlich. Die Abrechnungsstelle kann zum Beispiel ausschließlich als technisches Zentrum agieren, als eine Art Zwischenstelle oder Proxy, der ausgewählt wird, um Berechnungen vorzunehmen. Diese Proxies (gewöhnlich als anonyme weiterleitende Proxies oder anonyme „loop-back“-Proxies bezeichnet) können im Fahrzeug oder außerhalb installiert werden und die Funktion haben, die Daten an Bord des Fahrzeugs oder an einer anderen Stelle zu speichern. Die datenschutzrechtlichen Auswirkungen eines solchen Ansatzes zu bewerten ist im Prinzip eine Frage des Vertrauens (z.B. ob dem Gerät vertraut werden kann und ob Dritte wirklich nicht in der Lage sind, auf die Daten zuzugreifen).

Die Arbeitsgruppe befürwortet generell solche Proxy-Ansätze, sofern deren Schutz der Privatsphäre unabhängig überprüft werden kann und sie den Grad an Schutz der Privatsphäre garantieren, der bei einem reinen Smart-Client-Ansatz erreicht wird.

Durchsetzung

Die Durchsetzung ist ein anderes entscheidendes Element, das in einer datenschutzfreundlichen Art und Weise gestaltet werden muss, wenn man anstrebt, die Anonymität der Fahrer in elektronischen pay-as-you-go-Mautsystemen zu wahren.

Der Bereich, in dem ein möglicher Missbrauch der persönlichen Daten stattfinden könnte und der besondere Aufmerksamkeit erfordert, ist die Überwachung und das Aufspüren von Zuwiderhandelnden. Die Identität der Fahrer muss nicht festgestellt werden, bis der Fahrer etwas getan hat, das als Verletzung der Nutzungsbedingungen des Mautsystems definiert ist oder als sonstiges Vergehen. Der Grundsatz der Verhältnismäßigkeit sollte in vollem Umfang beachtet werden, z.B. muss zunächst festgestellt werden, dass sich das Gebührensystem in dem Fahrzeug befindet und ob es fehlerfrei funktioniert. Wenn die Kontrolleinheit keine Verletzung hinsichtlich des Vorhandenseins oder der ordentlichen Funktionsweise des Gebührenerhebungsgeräts feststellt, sollte sie keine weiteren Schritte zur Ermittlung der Identität des Geräts oder des Fahrers einleiten. Nur wenn die Aufsichtsstelle feststellt, dass ein Gerät nicht vorhanden ist, dass das Gerät nicht ordentlich funktioniert oder dass die Einstellungen missbräuchlich verändert worden sein könnten, sollte eine autorisierte Stelle - im Einklang mit dem Verhältnismäßigkeitsgrundsatz - mit der Identifizierung des Fahrers fortfahren. Laut Berichten von Expertengruppen stellt die Erfassung des Nummernschilds und somit die Identifizierung des einzelnen Fahrers oder Fahrzeuginhabers eine zufriedenstellende Kontrollmöglichkeit in dieser Hinsicht dar.

Das oben Gesagte bedenkend sollten die persönlichen Daten der Fahrer, die dem System nicht zuwidergehandelt haben, auf keine Art und Weise, außer durch den Fahrer selbst, verarbeitet werden. Diesem Ansatz folgend würde die Kontrollstelle lediglich überprüfen, ob das Gerät im Fahrzeug richtig funktioniert, und nur eine autorisierte Person (für den Zweck, für den dieser Person die Berechtigung zum Zugriff auf personenbezogene Daten erteilt wurde) darf die Identität der Betroffenen erfragen oder Informationen über die Position des Fahrzeugs erhalten. Dies darf nur unter bestimmten Umständen erlaubt sein, die im Vorhinein bestimmt und aufgelistet sein müssen (z.B. wenn an dem elektronischen Mautgerät in dem Fahrzeug unerlaubte Änderungen vorgenommen wurden, wenn das Gerät auf kostenpflichtigen Straßen nicht funktioniert oder wenn das Auto gestohlen wurde). Jeder Zugriff zum Zweck der Durchsetzung auf Informationen über die Position des Fahrzeugs, die Reisezeit und Gebühren muss entsprechend dokumentiert werden, so dass eine vollständige Nachüberprüfung möglich ist. Es wäre unzulässig, einen nicht autorisierten und nicht registrierten Zugang zu den Daten in dem Gerät zu erlauben.

Die Frage der optionalen oder zwangsweisen Verwendung

Wenn die Nutzung der On-Board-Einheit optional wäre, könnten die Fahrer entweder die On-Board-Einheit oder eine andere Methode wählen, die Gebühren zu erheben und abzurechnen (z.B. Anmeldung und Zahlung an einer automatischen Station). Hervorgehoben werden muss, dass der Nutzer weder in dem optionalen noch in dem freiwilligen Schema das Gerät abschalten kann, während er auf einer kostenpflichtigen Straße fährt. Die Frage nach einer optionalen oder freiwilligen Nutzung des Mautgeräts und den Auswirkungen auf die Privatsphäre ist zu einem großen Maß eng mit der Frage der Überwachung verbunden. Im Prinzip ist die optionale Verwendung benutzerfreundlicher, weil die Betroffenen ihre vorherige Einstimmung in die Verarbeitung ihrer persönlichen Daten erteilen können; allerdings sind auch die Durchsetzungsprobleme eng mit dieser Frage verbunden und sollten insofern auch bewertet werden.

Ein Beispiel aus der deutschen Erfahrung mit Lastkraftwagen (Toll Collect System) zeigt, dass 90 % der LKW-Fahrer sich für die Installation eines Satellitensystems entschieden haben; weniger als 10 % bevorzugen andere Systeme. Die Zuverlässigkeit und Genauigkeit des installierten Systems liegt bei 99,75 %, was bedeutet, dass gewissermaßen alle Probleme in Bezug auf die Durchsetzung und Unregelmäßigkeiten bei denen auftreten, die kein Gerät installiert haben und sich bei Mautstationen anmelden und dort manuell bezahlen. Wenn man diese Erfahrungen mit LKW auf ein Mautsystem für private Fahrzeuge überträgt (insbesondere wenn dies schlussendlich auf allen Straßen eingesetzt werden soll), scheint eine optionale Verwendung wenig realistisch. Ein optionales Mautsystem im freien Verkehr würde die Installation sehr komplexer und teurer Kontrollsysteme auf allen kostenpflichtigen Straßen erfordern (Videoüberwachung, Identifizierung der Nummernschilder etc.), was im Ergebnis zu einem höheren Grad an Überwachung und einem größeren Eingriff in die Privatsphäre führen würde als ein verbindliches System. Die Entscheidung, ob man eine optionale Verwendung erlaubt oder eine verbindliche Nutzung durchsetzt, hängt wesentlich von der Größe der Implementierung und den für die Durchsetzung verfügbaren Ressourcen ab und kann daher im kleinräumigen und großräumigen Ansatz (national oder sogar international) unterschiedlich sein.[15]

Die Rechte der Betroffenen

Eine besondere Aufmerksamkeit sollte der Frage von umstrittenen Gebühren gewidmet werden. Wenn man sicherstellen will, dass personenbezogene Daten unter der alleinigen Kontrolle des Nutzers verbleiben, sollte ein Zugriff zu den Daten nur ermöglicht werden, wenn der Nutzer es ausdrücklich verlangt. Mautsysteme können und sollten so gestaltet sein, dass die detaillierten Reisedaten vollständig und dauerhaft aus dem System gelöscht werden, nachdem die Gebühren festgesetzt wurden und jede Frist, innerhalb derer die Gebühr angefochten werden kann, abgelaufen ist (wie es z.B. im Londoner City-Maut System geschieht).

Ein Fernzugriff auf die Rohdaten durch die Kontrollstelle oder durch Dritte zu anderen als Durchsetzungszwecken, unabhängig davon, ob die Daten in dem Gerät gespeichert sind oder nicht, sollte nur mit Einwilligung des Betroffenen erfolgen. Ebenso sollte die Verarbeitung zu anderen Zwecken (z.B. „pay-as-you-go“-Kfz-Versicherung oder verhaltensbasierte Werbung) nur möglich sein, wenn der Fahrzeughalter seine eindeutige und ausdrückliche Einwilligung erteilt hat.

Ergebnis

Die Arbeitsgruppe ist der Ansicht, dass die zentralisierte Verarbeitung persönlicher Daten für Mautsysteme im freien Verkehrsfluss nicht erforderlich und daher gemäß dem Verhältnismäßigkeitsgrundsatz nicht gerechtfertigt ist, angesichts der nachweisbaren Existenz technischer Lösungen, die eine zentralisierte Verarbeitung der Daten nicht erfordern. Ein starker Schutz der Privatsphäre kann und sollte von Beginn an so gestaltet sein, dass Informationen, die an die Kontrollstelle übermittelt werden, sich lediglich auf die Höhe der Gebühren beziehen und nicht auf Ort und den Zeitpunkt der Reise. Wie es in dem Bericht der National Surface Transportation Infrastructure Financing Commission der USA dargestellt wurde, würde ein solches System einen wesentlich höheren Grad an Privatsphäre bieten als andere Informationssysteme in unserer Gesellschaft, wie z.B. Kreditkarten und Mobiltelefonsysteme, bei denen der Anbieter nicht weiß, wie viel eine Person schuldet, aber wo Personen einkaufen und welche Nummern sie angerufen haben (mehr oder weniger präzise sogar den Ort). Mautsysteme können und sollten so gestaltet sein, dass detaillierte Reisedaten vollständig und dauerhaft aus dem System gelöscht werden, sobald die Gebühren festgesetzt wurden, um zu vermeiden, dass Bewegungsprofile erstellt oder die Daten zweckentfremdet werden.

Die Anonymität des Fahrers sollte innerhalb des Systems durchgängig gewährleistet bleiben. Im Hinblick auf die Durchsetzung sollte das System die Identität des Fahrers nicht feststellen, es sei denn, der Fahrer hat etwas getan, das als Verletzung der Nutzungsbedingungen des Mautsystems definiert ist. Die Verarbeitung der Daten zu anderen Zwecken (z.B. „pay-as-you-go"-Kfz-Versicherung oder verhaltensbasierte Werbung) sollte nur möglich sein, soweit der Betroffene seine eindeutige und ausdrückliche Einwilligung erteilt hat.

Im Prinzip ist die Frage nach der Privatsphäre in elektronischen Mautsystemen relativ einfach: Wesen und Zweck jedes groß angelegten Mautsystems erfordern die Verarbeitung persönlicher Daten, setzen aber nicht eine zentralisierte Verarbeitung der personenbezogenen Daten (solange keine Zuwiderhandlung begangen wurde), die unverhältnismäßige Verarbeitung der Daten, den Zugang zu persönlichen Daten oder eine allgegenwärtige Überwachung voraus. Die fundamentalen Grundsätze des Schutzes persönlicher Daten streben danach, die Anonymität zu bewahren; die Technologie kann und sollte in einer Weise eingesetzt werden, die es ermöglicht, die Anonymität der Fahrer zu erhalten. Jede Abweichung von diesem Grundsatz würde einen zusätzlichen Eingriff in die bereits erodierte Privatsphäre in der Informationsgesellschaft bedeuten.

---

[i] Electronic Road Charging: http://www.parliament.uk/post/pn112.pdf.

[2] Es muss darauf hingewiesen werden, dass das deutsche System nur für Lastkraftwagen gilt: http://www.toll-collect.de.

[3] Ministerium für Verkehr, Öffentliche Arbeit und Wassermanagement: Implementierung des Maut-Systems: http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/roadpricing/index.aspx

[4] 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner Ontario: http://www.ipc.on.ca/images/Resources/407-e.pdf.

[5] http://www.curacaoproject.eu/documents/newsletter-issue3.pdf.

[6] Eine ausführliche Studie von Mautsystemen und eine vollständige Liste an Quellen wurde durch Victoria Transport Policy Institut vorbereitet: Road Pricing, Congestion Pricing, Value Pricing, Toll Roads and HOT Lanes; http://www.vtpi.org/tdm/tdm35.htm.

[7] Road Reform and Privacy: Which Way Forward? Submission by the Privacy Commissioner to the Ministry of Transport in relation to the final report of the Roading Advisory Group: http://www.privacy.org.nz/road-reformand-privacy-which-way-forward/?highlight=impact.

[8] http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=568.

[9] DSRC - Dedicated Short Range Communications.

[10] GNSS/CN - Global Navigation Satellite System/Cellular Networks.

[11] Privacy-Sensitive Congestion Charging. Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle: http://www.cl.cam.ac.uk/~arb33/papers/BeresfordDaviesHarle-PrivacyAwareCongestion-SPW2006.pdf.

[12] Singapore, Melbourne, Trondheim, Toronto sind Beispiele für Systeme in Großstädten.

[13] Stefan Eisses, Wiebren de Jonge und Vincent Habers: Privacy And Distance Based Charging For All Vehicles On All Roads.Sh: http://www.tipsystems.nl/files/Privacy_and_RUC_ITSLondon-doc.pdf.

[14] National Surface Transportation Infrastructure Financing Commission: Paying Our Way, a New Framework for Transportation Finance, February 24, 2009 http://www.itif.org/index.php?id=227.

[15] In den Niederlanden werden zum Beispiel alle registrierten Fahrzeuge im Land von dem Mautsystem erfasst. Es gibt allerdings Ausnahmen innerhalb dieser Gruppe: Motorräder und bestimmte Fahrzeuge wie Rettungswagen. Ausgenommene Fahrzeuge werden nicht mit einem On-Board-Gerät ausgestattet.