Datenschutzfragestellungen in kontexbezogenen Systemen

Szenariensammlung zur Diskussion von datenschutzrechtlichen Fragestellungen in kontextbezogenen Systemen

SFB 627: Nexus - Umgebungsmodelle für Mobile Kontextbezogene Systeme
Universität Stuttgart
Arbeitsgruppe Allgemeine Sicherheit
Andreas Gutscher
gutscher@ikr.uni-stuttgart.de
18.1.2006

Einleitung

Beim Entwurf von orts- und kontexbezogenen Anwendungen und Systemen werden oft zunächst nur technische Aspekte und Randbedingungen untersucht. Da in diesen Systemen jedoch typischerweise auch personenbezogene Daten wie z. B. die Ortsdaten von Personen erfasst und verarbeitet werden, müssen bei der Entwicklung solcher Systeme schon sehr früh auch rechtliche Randbedingungen, insbesondere die Datenschutzgesetze berücksichtigt werden. Die rasanten technischen Entwicklungen eilen hierbei jedoch der Gesetzgebung voraus, so dass eine rechtliche Beurteilung von neuen Technologien hinsichtlich Datenschutzfragen in vielen Fällen auch für Fachleute sehr schwierig ist.

Von der Arbeitsgruppe Allgemeine Sicherheit des Sonderforschungsbereiches 627 wurden deshalb Nutzungsszenarien von kontextbezogenen Systemen am Beispiel der Nexus-Plattform erarbeitet, welche Fragestellungen im Umfeld des Datenschutzes aufwerfen. Diese Szenarien dienten als Grundlage für das Rechtsgutachten „DamokoS – Datenschutzfragen mobiler kontextbezogener Systeme“, welches von der Projektgruppe für verfassungsverträgliche Technikgestaltung unter der Leitung von Prof. Dr. Alexander Roßnagel (Universität Kassel) erstellt wurde.

Die nachfolgend aufgeführten Szenarien bestehen aus einer Szenarienbeschreibung und einem anschließenden Fragenteil, die Szenarien bauen teilweise auf dem jeweils vorhergehenden auf.

Grundfunktionen kontexbezogener Dienstplattformen

Alice hat über ihren Freund Bob von der Nexus-Plattform erfahren und beschließt, diese auszuprobieren.

Sie entscheidet sich, einen dazu erforderlichen Account bei der Big Brother AG, einem der größten Nexus Service Provider, einrichten zu lassen. Gegen eine geringe monatliche Gebühr erhält sie einen Zugang zu einem Location Server von Big Brother, an den sie Orts-

anfragen richten und auf dem sie die Koordinaten ihres Standortes für andere Benutzer ablegen kann. Alice erhält ein Login-Name und ein Passwort, mit dem sie sich beim Big Brother Location Server einloggen kann. Big Brother speichert in seiner Kunden-Datenbank für Verwaltungs- und Abrechnungszwecke den Vor- und Nachname, Geburtsdatum, die Anschrift, Telefonnummer, eMail-Adresse und die Bankverbindung von Alice.

Alice wird von Big Brother darauf hingewiesen, dass sie in einer sogenannten Zugriffskontroll-Liste festlegen kann, ob und auf welche Benutzer der Zugriff auf ihre Ortskoordinaten beschränkt werden soll.

Erfreulicherweise besitzt Alice bereits einen PDA, der über GPRS oder UMTS Zugang zum Internet hat. Nach der Installation einer geeigneten Nexus-Client-Software ermittelt ihr PDA mit Hilfe des eingebauten GPS-Empfängers in regelmäßigen Abständen seinen augenblicklichen Standort und sendet ihn an den Big Brother Location Server (diesen Vorgang nennt man „Location Updates“). Auf diesem Location Server werden die von Alice übermittelten Koordinaten zusammen mit der Zeit der Übermittlung in einer Datenbank gespeichert. Big Brother gibt an, dass die Daten (Koordinaten, Zeitpunkt) immer nur für eine bestimmte Zeitdauer für Abfragen bereitgehalten werden und dass sie danach gelöscht werden.

Bob hat Alice versprochen, ihr bei Gelegenheit ein paar Fragen zur Konfiguration ihrer Nexus Client Software zu beantworten. Auf seinem Heimweg beschließt er deshalb, noch kurz bei Alice vorbeizufahren, sofern sie schon zu Hause (oder zumindest auf dem Heimweg) ist. Um dies herauszufinden, sendet er eine sogenannte Objekt-Anfrage bezüglich Alice an Big Brother („Wo befindet sich Alice gerade?“). Big Brother prüft, ob Bob auf die Koordinaten von Alice zugreifen darf, und übermittelt ihm dann die aktuelle Position, die dann Bob’s PDA in einer Karte darstellt. Auf der Karte kann Bob sehen, dass Alice sich in der Fußgängerzone aufhält und fährt deshalb direkt nach Hause.

Nach dem Einkaufen möchte Alice nachschauen, ob sich jemand von ihren Freunden auch gerade in der Innenstadt befindet. Ihr Nexus Client stellt sendet hierzu eine sogenannte Bereichsanfrage bezüglich des Gebiets der Innenstadt an Big Brother („Welche Personen befinden sich im Gebiet der Innenstadt von Stuttgart?“). Big Brother prüft dann, welche Personen sich momentan im angegebenen Gebiet aufhalten und übermittelt Alice dann eine Liste aller Personen und deren Koordinaten, auf die Alice zugreifen darf. Der Client zeigt Alice mit Hilfe einer Karte an, dass sich ihre Kollegin Carol (die auch Kundin bei Big Brother ist) eine Straße weiter gerade in einer Eisdiele befindet, worauf sie sich noch kurzentschlossen zu einem kleinen Plausch bei einem Eiskaffee zu Carol gesellt.

Bei ihrer Registrierung hat Alice erfahren, dass Big Brother seit wenigen Wochen nun auch einen sogenannten Event Service anbietet. Dieser Event Service kann z. B. beauftragt werden zu überwachen, ob und welche anderen Personen (mit einem Nexus Client) sich in der Nähe befinden und den anfragenden Benutzer mit einem sogenannten Event darüber zu informieren.

Da Alice dies sehr praktisch findet, möchte sie sich in Zukunft von ihrem Nexus Client darüber mit einem Event benachrichtigen lassen. Alice meldet beim Event Service von Big Brother an, dass sie immer dann eine Benachrichtigung erhalten möchte, wenn die Entfernung zwischen ihr und Bob oder Carol kleiner als 200 Meter wird. Big Brother prüft nun bei allen Location Updates von Alice, Bob und Carol, ob diese Bedingung erfüllt ist und sendet Alice gegebenenfalls eine entsprechende Event-Benachrichtigung.

Als sich Bob vor einem Jahr bei Big Brother registriert hatte, war dieser Event Service noch gar nicht vorgesehen. Big Brother hat Bob zwar in einem Newsletter darüber informiert, dass dieser Event Service nun angeboten wird und ihm zur Verfügung stehe, Bob wurde aber nicht explizit darüber informiert, dass auch seine Ortsdaten vom Event Service ausgewertet werden, und Bob wurde auch nicht gefragt, ob er der Auswertung seiner Ortsdaten durch den Event Service zustimme.

Fragestellungen

- Ist es unbedenklich, dass der Location Server Betreiber personenbezogene Daten (insbesondere die Ortsdaten) speichert, ohne dass von vornherein klar ist, für welche Anwendung sie später einmal verwendet werden?
- Ist der Location Server Betreiber verpflichtet, zu speichern, wer wann wessen Ortsdaten abgerufen hat (z. B. um dem betreffenden Benutzer Auskunft darüber zu erteilen)?
- Kann ein Benutzer von seinem Location Server Betreiber Auskunft darüber verlangen, wer wann seine Ortsdaten abgerufen hat? Hängt das davon ab, ob der Location Server Betreiber diese Information überhaupt speichert?
- Muss ein Location Server Betreiber anfragende Benutzer darauf hinweisen, dass ihre Anfrage gespeichert wird und dass diese Information vom angefragten Benutzer eingesehen werden kann?
- Hätte Big Brother Bob über die Einführung des Event Services besser informieren müssen (insbesondere darüber, dass nun andere Benutzer nun Events auf seine Ortsdaten anmelden können) oder hätte der Betreiber sogar eine erneute Zustimmung von Bob einholen müssen?

Speicher- und Auskunftspflicht über Ortsdatenauskünfte

Big Brother wird darauf hingewiesen, dass er laut BDSG verpflichtet sei zu speichern, welche Benutzer wann welche Ortsinformationen einer Person abgerufen haben (Protokolldaten) und den betroffenen Personen auf Anfrage darüber Auskunft zu erteilen.

Variante 1

Big Brother argumentiert, dass diese Verpflichtung für seinen Dienst nicht gelte, da die Weitergabe der Ortsdaten an andere Benutzer ja eben gerade der primäre Zweck des Dienstes sei, die Weitergabe von den Benutzern also explizit gefordert würde und die Benutzer mit Hilfe der Zugriffskontroll-Liste genau steuern könnten, an wen die Daten weitergegeben werden sollen. Zudem würde die Erfassung und Speicherung aller einzelnen Zugriffe aufgrund der sehr hohen Abfragerate einen unzumutbar hohen technischen Aufwand erfordern. Big Brother schließt deshalb die Aufzeichnung von Protokolldaten in den AGBs aus.

Fragestellungen

- Ist dies zulässig?

Variante 2

Big Brother erfasst die geforderten Protokolldaten und stellt sie den jeweiligen Benutzern online zum Abruf bereit. Da Anfragen nach Protokolldaten jedoch nach kurzer Zeit einen erheblichen Anteil der Anfragen (und somit der Kosten) ausmachen, beschließt Big Brother, Anfragen nach Protokolldaten nun kostenpflichtig zu machen.

Fragestellungen

- Ist dies zulässig?

Variante 3

Big Brother modifiziert seinen Dienst technisch so, daß nun alle Anfragen nach Ortsinformationen anonym gestellt werden können. (D.h., Big Brother kann nun nicht mehr feststellen, wer die Anfragen tatsächlich gestellt hat.)

Fragestellungen

- Müssen auch von anonymisierten Anfragen Protokolldaten aufgezeichnet werden?

Zugriffsschutz und Rechtedelegation

Nach der anfänglichen Begeisterung wird Alice, Bob und Carol bewusst, dass momentan jeder Benutzer ihren Standort abrufen und durch regelmäßige Anfragen sogar ein Bewegungsprofil von ihnen erstellen kann, aus denen sehr viele Schlüsse auf ihre berufliche als auch private Tätigkeiten gezogen werden können.

Glücklicherweise bieten alle Location Server Für jeden Account eine Zugriffskontrolliste (ACL), die festlegt, welche Benutzer auf die Ortsdaten des Accounts zugreifen dürfen. Der Accountinnhaber kann diese ACL nach seinen Wünschen ändern, per default erlaubt sie allen Benutzern, die Ortsinformationen abzufragen.

Alice, Carol und Bob beschließen nun, den Zugriff auf ihre Ortsdaten einzuschränken. Sie autorisieren sich gegenseitig für die Abfrage ihrer Ortsdaten, indem sie sich gegenseitig in ihre ACL eintragen, verbieten aber Unbekannten den Zugriff.

Die bis jetzt recht übersichtliche Situation wird jedoch dadurch komplizierter, dass Doris, eine Freundin von Bob, ebenfalls die Nexus Plattform nutzen möchte. Im Gegensatz zu Bob befürchtet Doris jedoch, dass ihre Ortsdaten bei Big Brother nicht in guten Händen sind und entscheidet sich stattdessen, den Big Sister Server der Universität Stuttgart zu verwenden.

Bob müsste nun seine Anfragen gegebenenfalls an 2 verschiedene Location Server richten und die Ergebnisse zusammenfassen. Um sich dies zu ersparen, beschließt Bob, stattdessen den Föderierungs-Dienst der Supertracer AG in Anspruch zu nehmen, die anbietet, die Anfrage vom Benutzer entgegenzunehmen, an verschiedene Location Server weiterzuleiten, die Ergebnisse zusammenzufassen und an den Benutzer zurückzugeben.

Sowohl Alice und Carol als auch Doris lassen den Zugriff auf ihre Ortsdaten auf dem Location Server durch die ACL kontrollieren. Diese erlaubt zwar Bob den Zugriff, jedoch (zunächst) nicht dem Supertracer Dienst. Bob versucht das Problem wie folgt zu lösen:

Alice und Carol erlauben Bob nicht nur den Zugriff, sonder gestatten es ihm auch, das Zugriffsrecht an Dritte weiterzudelegieren. Bob stellt also Supertracer ein Zertifikat aus, welches besagt, dass Supertracer Anfragen im Auftrag von Bob an Big Brother richten darf. Supertracer kann dieses Zertifikat bei Anfragen vorweisen und erhält Zugriff auf die gewünschten Daten.

Doris jedoch hat Bob keine Delegationsberechtigung ausgestellt, so dass Supertracer keinen Zugriff auf Doris' Daten bei Big Sister bekommen wird. Supertracer kennt dieses Problem bereits und schlägt Bob vor, doch einfach sein Login und Passwort an Supertracer zu übergeben, so dass Supertracer im Namen von Bob bei Big Sister anfragen könne. Bob ist zwar nicht ganz wohl bei der Sache (zumal Big Sister die Weitergabe von Zugangsdaten an Dritte verbietet), er willigt dann aber doch ein, da er keine andere Lösung des Problems sieht.

Froh, dass er nun endlich einen Lösung gefunden hat, mit der alles wie gewünscht funktioniert, wirft Bob noch einen flüchtigen Blick auf die AGB von Supertracer, akzeptiert sie, und beginnt, den Föderationsdienst zu nutzen.

Supertracer behält sich mit Hilfe eines unscheinbaren Satzes in den AGB das Recht vor, alle über den Dienst abgewickelten Informationen auch an Dritte weitergeben zu dürfen. Bob hat beim Überfliegen der AGB jedoch nicht erkannt, welches weitreichende Recht sich Supertracer vorbehält und ist auch nicht in der Lage, die Folgen davon zu überblicken.

Fragestellungen

- Muss sich Supertracer das Einverständnis von Alice und Carol für das Abfragen ihrer Ortsinformation einholen?
- Muss sich Supertracer das Einverständnis von Doris für das Abfragen ihrer Ortsinformation einholen?
- Ist die Klausel in den AGB von Supertracer zulässig?

Datensparsamkeit und anonyme Dienstnutzung

Big Brother bietet bisher keine Möglichkeit, seinen Dienst anonym zu nutzen. Findige Forscher haben aber ein Konzept entwickelt und veröffentlicht, wie man einen Location Service mit vernachlässigbarem Mehraufwand und ohne Funktionseinschränkung betreiben kann, so dass er vollständig anonym genutzt werden kann.

Fragestellungen

- Verpflichtet das Gebot zur Datensparsamkeit und -vermeidung Big Brother nun, seinen Dienst so zu gestalten, dass eine anonyme Nutzung möglich ist?

Positionsdatenanbieter

Neben der Positionserfassung durch die Benutzer selbst (z. B. mit einem GPS-Empfänger) besteht auch die Möglichkeit, dass Positionen von Personen und Objekten von Dritten erfasst, verarbeitet und verbreitet werden.

Mobilfunkbetreiber

Mobilfunkbetreiber ermitteln mit Hilfe von Feldstärkemessungen, in welcher Funkzelle sich ein Mobiltelefon befindet. Es ist jedoch möglich, aus diesen Messwerten den aktuellen Aufenthaltsort eines Mobiltelefons mit einer deutlich höheren Genauigkeit zu ermitteln und für ortsbezogene Dienste zu verwenden.

Fragestellungen

- Ist der Ort eines Mobiltelefons eine ‘personenbezogene’ Information und benötigt der Mobilfunkanbieter für die Ermittlung des genauen Aufenthaltsortes folglich die Einwilligung des Mobiltelefon-Besitzers oder des Mobiltelefon-Benutzers?

KFZ-Kennzeichenerkennung

Ein Betreiber eines Mautsystems hat zum Zweck der Mauterhebung entlang von Autobahnen Kameras installiert, welche die Kennzeichen der Fahrzeuge erfassen. Da der Standort der Kameras, der Straßenverlauf und die durchschnittliche Geschwindigkeit der Fahrzeuge bekannt ist, lässt sich daraus relativ zuverlässig die Position der Fahrzeuge ermitteln bzw. vorhersagen.

Fragestellungen

- Ist der Ort von Kraftfahrzeugen eine ‘personenbezogene’ Information und wird folglich für die Speicherung, Verarbeitung und Weitergabe der Ortsinformation die Einwilligung des Fahrzeughalters oder des Fahrers benötigt?

Pseudonyme Nutzung

Der kommerzielle Location Service Provider „Small Brother“ möchte seinen Dienst so gestalten, dass seine Benutzer bei Nutzung unter einem Pseudonym auftreten können. Um dies umzusetzen, beschließt er, mit PseudonymPay zu kooperieren, welcher die Zahlungsabwicklung übernehmen soll.

Die Benutzer registrieren sich zunächst unter ihrem tatsächlichen Name bei PseudonymPay und geben dort ihre Bankdaten (Bankverbindung, Einzugsermächtigung, Kreditkartennummer, ...) an. Anschließend erzeugt PseudonymPay ein Pseudonym (z. B. eine zufällig gewählter Identifikator) für den Benutzer und bescheinigt ihm mit einem digital signierten Zertifikat, dass PseudonymPay die Abrechnung für dieses Pseudonym für die Nutzung des Dienstes von Small Brother übernimmt.

Der Benutzer tritt nun gegenüber Small Brother unter diesem Pseudonym auf und kann dessen Dienst nutzen, z. B. kann er nun seine Ortsinformationen auf dem Location Server von Small Brother ablegen und somit andern Benutzern zur Verfügung stellen.

Mit dem Zertifikat weist der Benutzer nach, dass PseudonymPay die Abrechnung übernimmt, d.h., Small Brother stellt PseudonymPay die angefallenen Gebühren des Benutzers unter Angabe des Pseudonyms in Rechnung, PseudonymPay wiederum zieht diese dann vom entsprechenden Benutzer ein.

Auf diese Weise hat Small Brother zwar Zugriff auf die Ortsinformationen des Benutzers, kann diese aber lediglich dem Pseudonym, nicht aber einer realen Person zuordnen.

Fragestellungen

- Müssen die Ortsinformationen nun nicht mehr als 'personenbezogen' eingestuft werden und kann Small Brother diese Daten nun ohne Einwilligung der Benutzer und ohne datenschutzrechtliche Einschränkungen verarbeiten und weitergeben? Müssen dafür noch weitere Anforderungen erfüllt sein?

Default-Einstellungen

Die meisten Benutzer belassen die Konfiguration von Geräten, Software und Diensten weitgehend in der vorgegebenen Default-Einstellung. Dienstanbieter können diese Erkenntnis dazu nutzen, Benutzer dazu zu verleiten, dem Dienstanbieter oder Dritten einen weiträumigeren Zugriff auf ihre personenbezogene Daten einzuräumen als eigentlich erforderlich bzw. erwünscht gewesen wäre (beispielsweise bei Zugriffskontrollisten sowie Einstellungen, ob Daten verschlüsselt übertragen werden sollen usw.).

Fragestellungen

- Besteht für Dienstanbieter eine Verpflichtung, die Default-Einstellungen ihres Dienstes sowie der dafür ggf. bereitgestellten Software oder Geräte „datenschutzfreundlich" zu gestalten solange dies keinen unzumutbaren Aufwand verursacht?

Einsatz kontextbezogener Systeme in Arbeitsverhältnissen

Carol arbeitet seit einiger Zeit bei der Firma Röhrich Rohre. Carol ist oft dienstlich mit dem Firmenwagen unterwegs, wenn sie spät abends von einem Kundenbesuch zurückkommt und den Wagen am nächsten Tag wieder benötigt, fährt sie oft auch direkt mit dem Firmenwagen nach Hause (dies hat sie selbstverständlich mit ihrem Arbeitgebern so abgesprochen). Der Dienstwagen wird hauptsächlich von Carol verwendet, ab und zu jedoch auch von einem ihrer Mitarbeiter.

Ihr Arbeitgeber, Herr Röhrich, wird von Zeit zu Zeit von Zweifeln geplagt, ob die hohe Kilometerleistung des Dienstwagens tatsächlich nur durch dienstliche Fahrten zustande kommt, insbesondere verdächtigt er heimlich Carol, den Dienstwagen vertragswidrig zu privaten Fahrten am Abend und an Wochenenden zu nutzen. Aus diesem Grund lässt er 'zur Verbesserung der Koordinierung von Dienstfahrten' einen GPS-Empfänger in den Wagen

einbauen, der in regelmäßigen Abständen dessen Standort an einen Location Server meldet, so dass Herr Röhrich jederzeit die genaue Fahrtroute der letzten Tage abrufen kann.

Herr Röhrich informiert seine Angestellten nicht über den eingebauten GPS-Empfänger.

Begeistert von den Möglichkeiten, die diese neue Technik eröffnet, wünscht sich Herr Röhrich nun auch die Möglichkeit einer direkten Überwachung der Angestellten. Er verkündet seinen Angestellten den Start eines Projekts zur 'Optimierung der Koordinierung von internen Abläufen'.

Kernpunkt dieses Projekts ist ein Mobiltelefon mit eingebautem GPS-Empfänger, das jeder Mitarbeiter während der Dienstzeit bei sich tragen soll. Es soll nicht nur sicherstellen, dass jeder Mitarbeiter allzeit erreichbar ist, sondern auch, dass deren momentaner Aufenthaltsort dadurch jederzeit bekannt ist, dass das Mobiltelefon seinen Standort in regelmäßigen Zeitintervallen an einen Location Server meldet.

Der Aufenthaltsort der Mitarbeiter soll dabei nicht nur von ihm, sondern zum Teil auch von den Mitarbeitern abfragbar sein, soweit es für eine besseren Koordinierung der Mitarbeiter untereinander dienlich ist. So soll z. B. das Koordinieren von kurzfristigen Meetings dadurch erleichtert werden, dass alle Teilnehmer sehen können, wer gerade vor Ort ist.

Die Installation und der Betrieb des Location Servers soll dabei aus Kostengründen von einem externen Dienstleister durchgeführt werden.

Die Teilnahme am Projekt sei 'selbstverständlich freiwillig', Herr Röhrich weist jedoch ausdrücklich darauf hin, dass er es sehr begrüßen würde, wenn sich alle Angestellten innovationsfreudig zeigen sollten und niemand versuchen würde, Effizienzverbesserungen in seiner Firma systematisch zu boykottieren, schließlich würde das ja auch zur 'Sicherung der Arbeitsplätze' beitragen.

Herr Röhrich merkt ferner an, dass es im Übrigen nicht erforderlich sei, das Mobiltelefon nach Feierabend auszuschalten, vielmehr sollte es besser durchgehend an bleiben, zum einen, damit niemand 'vergisst', es morgens wieder einzuschalten und zum andern, damit man 'in Notfällen' auch nach Feierabend erreichbar ist. Auf die Frage, ob man denn nicht zumindest den GPS-Empfänger ausschalten könne, antwortet Herr Röhrich, dass dies leider aus 'technischen Gründen' nicht möglich sei.

Fragestellungen

- Darf Herr Röhrich den Ort des Dienstwagens überwachen, wenn er von Angestellten benutzt wird?
- Muss Herr Röhrich seine Angestellten über die Überwachung des Dienstwagens informieren?
- Darf Herr Röhrich den Aufenthaltsort seiner Angestellten während der Arbeitszeit überwachen, sofern deren Einverständnis vorliegt?
- Darf Herr Röhrich seine Angestellten mit mehr oder weniger offensiven Maßnahmen dazu zwingen, einer Überwachung während der Arbeitszeit zuzustimmen?
- Darf Herr Röhrich den Aufenthaltsort seiner Angestellten während ihrer Freizeit überwachen, sofern deren Einverständnis vorliegt?

- Darf Herr Röhrich seine Angestellten mit mehr oder weniger offensiven Maßnahmen dazu zwingen, einer Überwachung während ihrer Freizeit zuzustimmen?

Telekommunikations-Überwachung

Zur verstärkten 'Bekämpfung des internationalen Terrorismus und der Kinderpornographie' und unter Berufung auf die Telekommunikations-Überwachungsverordnung (gegebenenfalls nach einer entsprechenden Erweiterung) fordern die Strafverfolgungsbehörden von allen Location-Server-Betreibern, dass diese die persönlichen Daten der Nutzer, die Verbindungsdaten von Zugriffen auf die Ortsdaten (Location Updates und Anfragen) sowie die Ortsdaten selbst für mindestens 3 Jahre speichern und eine Überwachungsschnittstelle einrichten, welche allen Strafverfolgungsbehörden Zugriff auf diese Daten gibt. Die Kosten haben die Betreiber zu tragen.

Diese Überwachungsauflage bereitet insbesondere allen nicht-kommerziellen Betreiber von Location Servern finanzielle Schwierigkeiten. Der Big Sister Location Server zum Beispiel wird von einer Forschergruppe an der Universität Stuttgart betrieben und stellt seinen Benutzern seinen Dienst kostenlos zur Verfügung. Durch die Überwachungsauflagen entstünden erhebliche Kosten, die die Universität nicht decken könnte. Um den Überwachungsauflagen zu entgehen, modifiziert die Forschergruppe die Spezifikation der Plattform und der Protokolle derart, dass Ortsdaten nur noch verschlüsselt auf dem Location Server abgelegt werden, so dass die Betreiber des Servers keinerlei Möglichkeit mehr haben, auf die Ortsdaten im Klartext zuzugreifen. Private Benutzerdaten fallen nicht an, da der Server eine anonyme Registrierung und Nutzung zulässt. Mit einem Hinweis auf diesen Umstand weist die Universität die Forderungen nach Überwachungsauflagen zurück. Die Strafverfolgungsbehörden untersuchen derzeit, ob eine Überwachungsverpflichtung weiterhin besteht oder nicht sowie ob die Universität damit gegen ihre Pflicht zur Kooperation bei der Strafverfolgung verstößt.

Fragestellungen

- Gibt die gegenwärtige Telekommunikations-Überwachungsverordnung Strafverfolgungsbehörden (oder andere Gesetze) die Möglichkeit, Location Server Betreibern diese Überwachungsauflagen inklusive deren Kosten aufzuerlegen?
- Wenn nicht, ist es realistisch, dass die Telekommunikations-Überwachungsverordnung (oder andere Gesetze) in den nächsten Jahren dementsprechend geändert werden könnten?
- Verstößt die Universität Stuttgart durch die Modifizierung der Plattform und der Protokolle (so dass sie die Ortsdaten selbst nicht mehr lesen kann) gegen die Telekommunikations-Überwachungsverordnung (oder andere Gesetze)?

Nutzung von Ortsinformationen für KFZ-Versicherungen

Auch die KFZ-Versicherung Heilig's Blechle weiß das Potential von Ortsinformationen zu schätzen. Sie erklärt ihrem Kunden Bob, dass sie als Versicherung gerne Zugriff auf die Ortsdaten seines Fahrzeuges hätten. Fast alle Neuwagen würden ja schließlich sowieso mit GPS-Empfänger und mobilem Internetzugang ausgeliefert, so dass ihm dadurch keine nen-

nenswerten Kosten entstehen würden. Mit Zugriff auf die Ortsdaten seines Fahrzeuges könne aber z. B. sein Fahrzeug nach einem Diebstahl schneller wieder gefunden werden und nicht zuletzt würde das der Versicherung die Möglichkeit geben, günstigere Versicherungstarife für die Fahrer anzubieten, die sich freiwillig zur Einhaltung bestimmter (nun überprüfbarer) Regeln verpflichten, z. B. die Einhaltung der jeweils zulässigen Höchstgeschwindigkeit oder die Meidung von Gegenden mit hoher Kriminalitätsrate beim Parken. Selbstverständlich müsse Bob der Versicherung keinen Zugriff auf die Ortsdaten geben wenn er nicht möchte, aber er müsse dann wohl mit erheblich teureren Tarifen rechnen. Bob merkt an, dass er mittelmäßig entsetzt über dieses Vorgehen ist, nach einem Vergleich der Tarife begleitet von der offen gestellten Frage, ob er denn etwas zu verbergen habe, willigt Bob dann doch widerwillig ein, der Versicherung Zugriff auf die Ortsdaten seines Fahrzeuges zu geben.

Fragestellungen

- Darf die Versicherungen von Kunden den Zugriff auf die Ortsdaten des Fahrzeugs fordern?

Handel mit Kontextdaten

Doris arbeitet in einer Apotheke in Stuttgart und fährt täglich mit der U-Bahn zur Arbeit. In vielen U-Bahn-Stationen wurden in letzter Zeit Werbeprojektoren installiert, die durchgehend eine Mischung aus Anzeigen, Werbespots und Nachrichten auf großformatige Leinwände projizieren. Da Doris diese Werbung immer beim Warten auf die U-Bahn im Blick hat, fällt ihr mit der Zeit auf, dass der Anteil von Werbespots für Medikamente erstaunlich hoch ist. Konkreten Verdacht schöpft Doris aber erst, nachdem sie samstags in einem Einrichtungshaus nach einem neuen Kleiderschrank gesucht hatte und die Werbespots in den nächsten Tagen auffällig von Möbeln dominiert wurden. An dem Tag, an dem Doris völlig unerwartet von einer freundlich lächelnden Dame auf der Werbeleinwand mit ihrem Vornamen angesprochen wird, wird ihr die Sache zu bunt. Sie versucht herauszubekommen, wie die personalisierte Werbung zustandekommt, findet aber lediglich heraus, dass die Werbespots von dem Unternehmen Adds4You zusammengestellt werden, das sich aber über die Quelle der offensichtlich verwendeten Ortsinformationen in Schweigen hüllt. Doris ist sich sicher, dass Bob ihr Bewegungsprofil nicht an eine Werbefirma weitergeben würde und verdächtig die Betreiber ihres Location Servers. Diese weisen jedoch die Schuld von sich und versichern, dass sie Doris' Ortsdaten nur an die Benutzer herausgeben, die Doris in die Zugriffskontrolliste eingetragen hat; in der steht derzeit nur Bob.

Tatsächlich hat Bobs Föderations-Provider Supertracer Bobs Zugangsdaten an Spyglass verkauft. Die Firma Spyglass hat ihren offiziellen Sitz auf einer einsamen Südseeinsel und ist in wenigen Monaten zu einem der größten Wiederverkäufer von personenbezogenen Ortsdaten und Bewegungsprofilen im derzeit boomenden Ortsdatenhandel geworden. Spyglass extrahiert systematisch Informationen aus den Bewegungsprofilen von Personen (z. B. den Wohnort und Arbeitsplatz, Freizeitaktivitäten, wer kauft wo ein, wer isst gerne italienisch, wer geht zu welchen Fußballspielen, ...) und vertreibt an andere Unternehmen (vornehmlich Werbefirmen wie z. B. Adds4You) zum einen den Zugriff auf die extrahierten Informationen und zum andern auch auf die die Ortsdaten selbst.

Fragestellungen

- Muss Adds4You Doris Auskunft darüber geben, woher sie Doris' Ortsdaten beziehen?
- Benötigt Adds4You Doris' Einwilligung oder kann sich Adds4You auf die Einwilligung von Bob berufen, welche Supertracer über Spyglass an ihn weitergereicht hat?
- Darf Spyglass Profile aus den Ortsdaten der beobachteten Personen erstellen und an Dritte weitergeben?