Schutz der Privatsphäre bei Geo-Services

Privacy Protection in Geo-Services

Gerhard Navratil

Department für Geodäsie und Geoinformation, TU Wien · gerhard.navratil@geo.tuwien.ac.at

Zusammenfassung: Der Schutz der Privatsphäre wird in einer hoch technisierten und stark vernetzten Gesellschaft immer schwieriger. Ohne es zu wollen, hinterlassen wir ständig digitale Spuren, die stark mit unseren persönlichen Daten korrelieren. Im Artikel wird gezeigt, dass die lokale Verarbeitung persönlicher Daten durch heruntergeladene Scripts dieses Problem teilweise lösen würde. Trotzdem bleiben offene Fragen bezüglich einzuholender Zusatzinformationen, da auch hier Rückschlüsse auf persönliche Daten möglich sein könnten.

Schlüsselwörter: Datenschutz, Privatsphäre, Geo-Service, Servicekonzept

Abstract: *Protection of privacy is getting more complex in our highly technical age and strongly linked society. Accidentally, we continuously leave digital traces which correlate strongly with our personal data. The paper shows that local analysis of personal data using downloaded scripts can partially deal with the problem. However, open questions concerning required additional information, because they may provide an insight into the personal data.*

Keywords: *Data protection, privacy, geo-service, service concept*

1 Einleitung

Immer mehr Daten liegen digital vor und Transaktionen werden auf digitalem Wege durchgeführt. Damit wird der Schutz der Privatsphäre immer schwieriger. Was früher mit Observierungen oder Abhöranlagen ermittelt wurde, kann man heute durch Verfolgen der digitalen Spuren erfahren. Daraus resultiert beispielsweise die umfassende Diskussion zum Thema Vorratsdatenspeicherung. Im Zuge dieser Diskussion hat etwa das deutsche Bundesverfassungsgericht 2010 festgestellt, dass Vorratsdatenspeicherung nicht grundsätzlich gegen das Postgeheimnis verstoße (BVerfG, 2010). Dabei ist aber zu beachten, dass digital gespeicherte Daten Analysen ermöglichen, die bei analogen Spuren gar nicht, nicht lange oder nur mit großem Aufwand durchgeführt werden konnten. Vor der Einführung von Computern war es jedoch auch nicht möglich nachträglich festzustellen, ob es zwischen zwei Personen einen Briefwechsel gab. Vorratsdatenspeicherung ermöglicht das und noch viel mehr. Generell hat sich nach Moser-Knierim das Spannungsverhältnis zwischen Freiheit des Einzelnen und Sicherheit der Allgemeinheit vor allem auch durch die Technisierung verschärft (Moser-Knierim, 2014, p. 1). Es ist aber für den Einzelnen auch nicht zielführend, die Nutzung von technischen Möglichkeiten vollständig einzustellen, nur um die Privatsphäre zu schützen. Daher stellt sich die Frage, wie die Technik genutzt werden sollte, um gleichzeitig die Privatsphäre zu wahren. Vollständig kann die Sicherung der Privatsphäre natürlich nicht gelingen, weil bestimmte Spuren immer hinterlassen werden. Kostenpflichtige Services brauchen etwa eine Rechnungsadresse. Als Nutzer von Services kann man jedoch zumindest solche bevorzugen, welche mit möglichst wenigen Daten auskommen bzw. welche die Privatsphäre respektieren.

AGIT – Journal für Angewandte Geoinformatik, 3-2017, S. 24-32. © Wichmann Verlag, VDE VERLAG GMBH · Berlin · Offenbach. ISBN 978-3-87907-633-8, ISSN 2364-9283, eISSN 2509-713X, doi:10.14627/537633003.
Dieser Beitrag ist ein Open-Access-Beitrag, der unter den Bedingungen und unter den Auflagen der Creative Commons Attribution Lizenz verbreitet wird (http://creativecommons.org/licenses/by-nd/4.0/).

Im folgenden Beitrag wird nach einigen theoretischen Betrachtungen anhand eines praktischen Beispiels gezeigt, wie ein solches Service gestaltet werden könnte. Als beispielhaftes Service wird die Plausibilitätsprüfung der Eintragungen in einem Kontoauszug beschrieben. Dabei richtet sich der Beitrag weniger an die Nutzer von Geo-Diensten als vielmehr an die Entwickler und soll das Bewusstsein hinsichtlich des Schutzes der Privatsphäre stärken.

2 Datenschutz und das Recht auf Privatsphäre

Der Schutz privater Daten ist in der Jurisdiktion vieler Staaten ein wichtiger Eckpfeiler der persönlichen Freiheit. In Österreich ist der Anspruch auf Geheimhaltung der personenbezogenen Daten verfassungsrechtlich als Grundrecht verankert:

„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. […]“ (DSG, 2000, § 1).

Ebenso besteht ein Recht auf Privatsphäre. § 1328a Z.1 ABGB schützt dieses Recht. Eine kurze Diskussion der relevanten österreichischen Gesetze vor allem in Hinblick auf Medienfreiheit und Informationsinteressen der Öffentlichkeit findet man bei Fichtinger (2006). Allerdings fehlt hier eine Diskussion von Möglichkeiten, um seine Privatsphäre im Internet zu schützen. Generell liefert die moderne Informationstechnologie erst die Voraussetzungen, um die Privatsphäre umfassend zu verletzen. Wagner hat gezeigt, wie umfassend Personen mittels Smartphone ausgespäht werden können (Wagner, 2014). Ein einfaches räumliches Profil (wann war man wo) kann schon viel über einen Menschen verraten. Ein regelmäßiger Besuch in einem bestimmten Gotteshaus beispielsweise lässt einen Rückschluss auf die Konfession zu. Sich als Laie gegen ein solches Ausspähen zu schützen ist nahezu unmöglich und es kann mitunter auch für Experten schwierig nachzuvollziehen sein, was genau erfasst und übertragen wurde.

Der Schutz privater Daten ist aber auch in der Charta der Grundrechte der Europäischen Union verankert (EU, 2000). Dieser Schutz kann nur dann vom Staat gewährleistet werden, wenn dieser auch die volle Kontrolle über sämtliche von den Daten durchlaufenen Transport- und Verarbeitungskanäle hat. Das ist im Allgemeinen nicht (mehr) gegeben. Bei Verletzung der Privatsphäre besteht zwar Anspruch auf Wiedergutmachung, ein bereits entstandener Schaden kann aber oftmals nicht durch finanzielle Zuwendungen bereinigt werden. Wie sollte man etwa den Schaden beziffern, der durch die eventuell nicht mehr rückgängig zu machende Verbreitung eines Fotos aus dem privaten Bereich entstanden ist?

Die einfachste Möglichkeit zum Schutz persönlicher Daten wäre daher, solche Daten prinzipiell nicht an Dritte weiterzugeben. Diese Forderung ist zwar leicht zu stellen, kann aber bei der Umsetzung Probleme beinhalten. Einkaufen bei Online-Shops, Bewerbungen per E-Mail oder Informationsgewinnung im Internet wären dann nur mehr bedingt möglich.

3 Prozessablauf bei Web-/Geo-Services

Ein Web-Service ist ein Softwaresystem entworfen um die Interaktion zwischen Maschinen über ein Computernetzwerk zu ermöglichen (W3C, 2004)[1]. Ein Beispiel für die Nutzung von Web-Services sind Online-Shops. Eine solche Seite ermöglicht den Einkauf im Internet. Anders als bei traditionellen Geschäften ist die Ware aber nicht im Web-Shop lagernd, sondern die Seite stellt oftmals nur einen Kontakt zwischen Lieferanten und Kunden her. Dabei gilt es, eine Reihe an Informationen abzuklären:

- Welche Artikel bietet der Lieferant an und zu welchen Konditionen?
- Stimmt die angegebene Lieferadresse?
- Wann ist der voraussichtliche Liefertermin?
- Stimmen die Kreditkartendaten?
- …

Bei jeder dieser Frage muss der Web-Shop Daten von Dritten nutzen. Das geschieht im Allgemeinen durch Web-Services. Beispielsweise werden die Lieferdaten durch ein Service des Lieferanten an den Web-Shop weitergegeben, der sie dann an den Kunden weiterleitet. Dabei müssen klarerweise die Daten zur Bestellung an das Service übermittelt werden.

Geo-Services sind spezialisierte Web-Services. Sie dienen zur Verarbeitung räumlicher Informationen. Das Spektrum reicht von einfachen Geocoding-Abfragen oder Datumswechseln bis zu komplexen Analysen unter Verwendung umfangreicher Zusatzinformationen wie der Suche nach einer optimalen Flugverbindung. Die Programmierschnittstelle (API) ist dabei vom Anbieter des Dienstes vorgegeben. Für das Geocoding stellt Google Maps JavaScript das Objekt *google.maps.Geocoder* mit der Methode *Geocoder.geocode()* zur Verfügung. Dabei wird die Adresse als Parameter übergeben und man erhält (unter anderem) die Koordinaten als Ergebnis (Google, 2016). Hier zeigt sich natürlich bereits ein Datenschutzproblem. Im privaten Bereich wird man vornehmlich solche Orte abfragen, an denen man Interesse hat. Dieses Interesse gehört jedoch bei Privatpersonen zur Privatsphäre, weil es sich um religiöse Einrichtungen, Ärzte oder die Wohnadressen persönlicher Kontakte handeln kann. Erfolgt ein solcher Aufruf nicht anonymisiert, so kann der Betreiber des Services (im obigen Fall Google) ein geographisches Profil des Nutzers erstellen.

Bei der Nutzung eines Geo-Service von einem privaten Rechner aus stellt sich der prinzipielle Ablauf der Nutzung wie in Abbildung 1 gezeigt dar. Der Computer des Nutzers sendet eine Anfrage an das Geo-Service. Diese Anfrage wird über das Internet an den Adressaten weitergeleitet. Auf diesem Server wird die Anfrage bearbeitet und das Ergebnis bestimmt. Dieses wird dann wieder über das Internet an den aufrufenden Rechner zurückgeschickt. Der Rechner des Nutzers empfängt die Ergebnisse.

[1] Orig. “A web service is a software system designed to support interoperable machine-to-machine interaction over a network.”

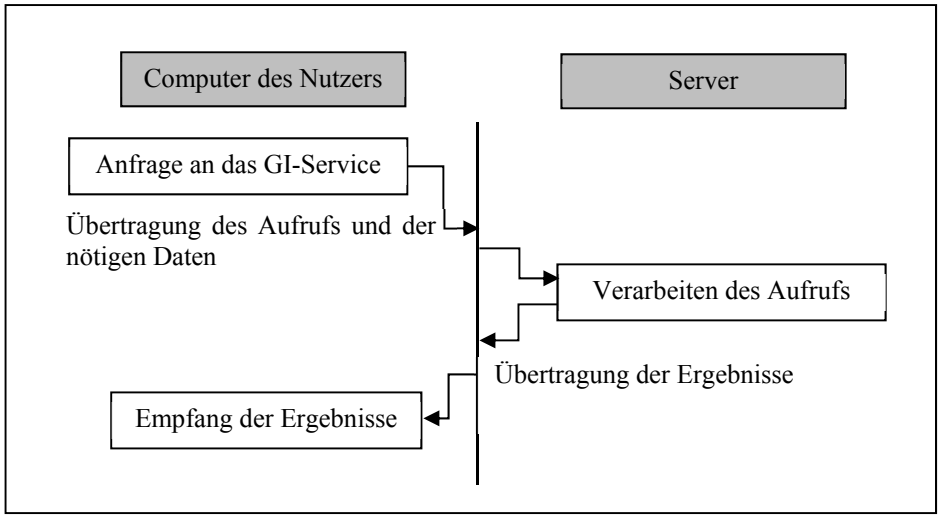

Abb. 1: Schematische Darstellung des Aufrufs eins Geo-Service

4 Prozessablauf unter Berücksichtigung des Datenschutzes

In diesem Ablauf gibt es zwei problematische Bereiche: Der Server auf dem das Service läuft und die Verbindung dorthin. Die Verbindung zum Server ist nicht vorherbestimmt, sondern die Pakete werden von Knoten zu Knoten weitergeleitet. Somit ist es möglich, dass die Datenströme auf dem Weg zum Empfänger dupliziert und analysiert werden. Abhilfe schaffen verschlüsselte Kommunikationen, aber gerade staatliche Stellen drängen massiv darauf, Zugang zu den Verschlüsselungsalgorithmen und -Codes zu bekommen (vgl. ORF, 2013; Pany, 2016). Die zweite Schwachstelle ist der Server des Betreibers. Einerseits kann der Server gehackt werde, was in der Vergangenheit bereits öfter passiert ist um Zugang zu Kreditkartendaten zu erhalten, andererseits kann auch der Service-Betreiber selbst die Daten anderweitig nutzen oder an Dritte weitergeben.

Prinzipiell sollten sich Service-Anbieter an die von Duckham und Kulik beschriebenen Kriterien halten (Duckham & Kulik, 2006):

- Bekanntmachung und Transparenz: Es muss den Nutzern klar sein, ob persönliche Informationen gespeichert werden, welche persönlichen Informationen und warum.
- Zustimmung und Nutzungsbeschränkung: Der Nutzer muss der Speicherung für bestimmte Zwecke zustimmen und die Nutzung der persönlichen Informationen ist dann auf diese Zwecke beschränkt.
- Zugang und Mitwirkung: Die Nutzer müssen Zugang zu den gespeicherten persönlichen Informationen und Fehlerkorrekturen beantragen können
- Integrität und Sicherheit: Die Service-Betreiber müssen darauf achten, dass persönliche Informationen korrekt und aktuell sind und sie gegen unbefugte Zugriffe, Offenlegung und Nutzung schützen
- Vollstreckung und Verantwortung: Die Service-Betreiber sind verantwortlich bei Nichteinhaltung der Kriterien.

Diese Kriterien sind zwar gut durchdacht, haben aber zwei Schwachstellen: Man kann nur gegen Datensammlungen vorgehen, wenn bekannt ist, dass diese Daten gesammelt werden (vgl. McKenzie & Janowicz, K., 2014), und es kann schwer sein, den Verstoß gegen die Kriterien zweifelsfrei nachzuweisen. Dazu kommt, dass Services oft auf ausländischen Servern laufen und eventuell andere Regeln gelten als in der Heimat des Nutzers.

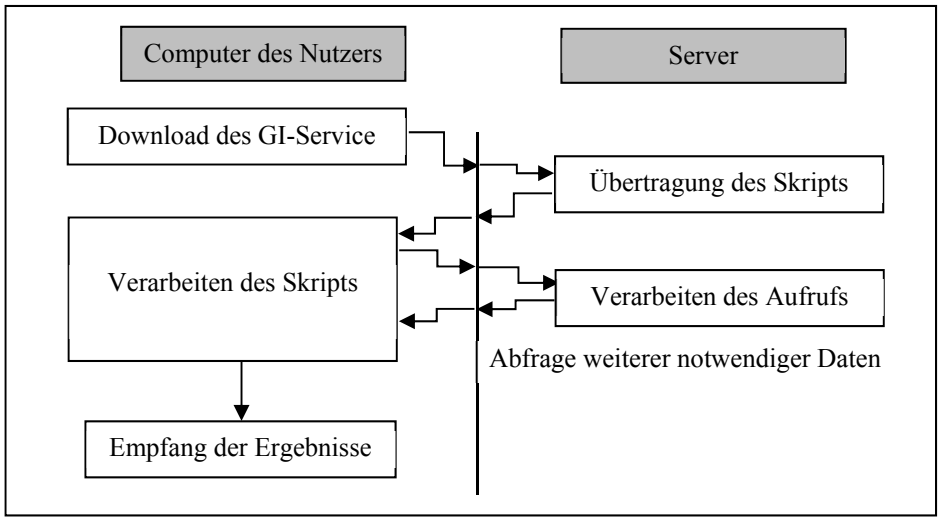

Abb. 2: Geo-Service ohne Weitergabe der persönlichen Daten

Abbildung 2 zeigt ein Konzept, in dem keine Daten des Nutzers an einen Server übertragen werden. Stattdessen wird ein Skript vom Server auf den Rechner des Nutzers übertragen, das dann die übergebenen Daten analysiert. Im Zuge der Verarbeitung kann der Bedarf an weiteren Informationen entstehen, die dann über ein oder mehrere Aufrufe von Web-Services gelöst wird. Wesentlich ist jedoch, dass für diese ergänzenden Aufrufe wesentlich weniger persönliche Daten benötigt werden als beim ursprünglichen Konzept in Abbildung 1. Somit ist die Privatsphäre auch besser geschützt.

5 Beispiel: Validierung des Kontoauszugs anhand eines GPS-Tracks

Anhand eines einfachen Beispiels soll die Problemstellung samt Lösung verdeutlicht werden: Jeder Inhaber eines Bankkontos bekommt monatlich die Liste der Transaktionen dieses Kontos zugesandt. Das können einige wenige Zeilen oder aber auch mehrere Seiten sein. Eine wichtige Funktion dieses Kontoauszugs ist die Prüfung auf unrechtmäßige Zahlungen. Nach mehreren Wochen ist es jedoch oft nicht mehr möglich, diese Prüfung durch Vergleichen der Buchungszeilen mit den eigenen Erinnerungen durchzuführen. Eine simple Prüfmethode wäre, den Standort einer Bankomatkasse mit dem zeitnahen Standort der verwendeten Bankomatkarte zu vergleichen. Gibt es signifikante Abweichungen zwischen den Positionen der

beiden Objekte, so liegt möglicherweise ein Fehler vor. Die Fragestellung ist also räumlicher Natur und bietet sich somit für ein Geo-Service an. Im Kontext dieses Artikels ist die Konzeption dieses Services relevant. Das spezielle Service soll hier auch nur als Beispiel der Problematik dienen und hätte bei einer etwaigen Umsetzung eine Reihe von Schwierigkeiten, etwa den Strombedarf derzeit verwendeter Positionierungstechnologien oder den Schutz der gespeicherten Tracks auf einem Smartphone vor weiteren Applikationen. Diese Aspekte werden im weiteren Verlauf ignoriert.

Der Inhaber eines Bankkontos mit Online-Banking-Portal kann seine Kontoauszüge nicht nur in Form einer PDF-Datei beziehen, sondern die Transaktionen auch in eine Datei (.csv oder .txt) exportieren und lokal speichern. Die Transaktionsdaten können dann ohne weiteren Internetzugriff mit lokal installierter Software geöffnet und bearbeitet werden. Jede Buchung kann dann einzeln gelesen und der Buchungstext auf räumliche und zeitliche Information analysiert werden. Jede Buchungszeile beinhaltet zumindest folgende Information:

- Datum der Durchführung der Transaktion (Valuta);
- Datum der Eintragung durch die Bank;
- Buchungstext;
- Buchungsbetrag und Währung.

Der Buchungstext enthält neben Datum und Uhrzeit der Transaktion auch Informationen zum Ort. Bei Bankomatkassen ist das meist der Name des Geschäfts und eventuell eine Filialnummer, bei Geldautomaten eine entsprechende Nummer des Geldautomaten.

Somit ist auch klar, welche räumlichen Informationen benötigt werden. Neben den Buchungsdaten sind das einerseits die Standorte aller genutzten Kassen oder Geldautomaten und andererseits die Position der Bankomatkarte zum Buchungszeitraum. Die Bankomatkarte selbst kann nicht verortet werden, die Position des Karteninhabers kann man aber bestimmen (z. B. mithilfe von Satellitenpositionierungsdiensten). Bei rechtmäßiger Nutzung der Karte befindet sich der rechtmäßige Karteninhaber am selben Ort wie die Karte, also an dem Ort an dem auch die Transaktion durchgeführt wird. Widersprüchliche Ortsangaben deuten auf eine mögliche widerrechtliche Nutzung der Karte hin. Da im Vorhinein nicht bekannt ist, wann eine unrechtmäßige Zahlung erfolgt, benötigt man somit ein lückenloses räumliches Profil des Karteninhabers. Daraus kann für jeden Zeitpunkt abgeleitet werden, wo er sich aufgehalten hat. Dieses Wissen kann genutzt werden, um die Position des Karteninhabers mit dem Standort der Bankomatkassa bzw. des Geldautomaten abzugleichen.

Zugriff auf den Kontoauszug haben sowohl der Kontoinhaber als auch die Bank. Die Zahlungsdaten liegen also bei beiden Parteien vor. Es wird vorausgesetzt, dass die Bank die Privatsphäre ihrer Kunden schützt und die Daten nicht illegal weitergibt. Zusätzlich notwendig ist das räumliche Profil des Karteninhabers. Der Einfachheit halber wird im Folgenden davon ausgegangen, dass es nur eine einzige Bankomatkarte für das zu prüfende Konto gibt, also auch nur ein einzelnes Profil berücksichtigt werden muss. Zusätzlich sind die Positionen der Bankomatkassen nötig. Diese sind bei fest installierten Bankomatkassen oder Geldausgabeautomaten konstant, könnten also beispielsweise per Web-Service bereitgestellt werden. Ist der Prozessablauf jedoch so gestaltet, dass bei jeder noch nicht bekannten Bankomatkassa vom Web-Service der Standort dieser Bankomatkassa abgefragt werden würde, dann könnte der Betreiber des Service beginnen, folgende Informationen zu sammeln:

- Kunden eines Geschäfts (nicht nach Volumen oder Frequenz aber sehr wohl nach Anzahl);

- relevante Orte für den Nutzer einer bestimmten IP-Adresse (beispielweise in der Nähe zum Wohnort oder zum Arbeitsplatz);
- annäherndes Datum der ersten nachgewiesenen Nutzung der Bankomatkassa durch den Kontoinhaber.

Natürlich kann die Abfrage maskiert werden, beispielsweise indem nicht nur die Position der benötigten Bankomatkassa abgefragt wird, sondern auch weitere Positionen, aber die Information ist trotzdem beim Service-Anbieter vorhanden, wenn auch in verrauschter Form. Bei häufiger Nutzung des Web-Service wird es an den korrekten Positionen zu Häufungen kommen, die auch detektiert werden können.

Daher ist es ein sinnvollerer Ansatz, eine solche Datensammlung erst gar nicht zu ermöglichen. Dazu gibt es zwei mögliche Ansätze:

- Alle Standorte von Bankomatkassen in Österreich werden lokal gespeichert und dann für die Identifikation genutzt. Bei diesem Ansatz ist die Nachführung der Daten in der Zentralen Abfragestelle kritisch. Wenn die Daten fehlerhaft oder unvollständig sind, kann es zu falschen Ergebnissen bei der Analyse kommen. Somit ist fraglich, ob ein solcher Service realisiert werden könnte.
- Die Lokalisierung der Bankomatkassen geschieht mittels des räumlichen Profils des Kontoinhabers. Eine erstmalige Zahlung definiert lokalisiert die Bankomatkasse und jede weitere Zahlung verbessert dann die Genauigkeit der Lokalisierung.

Bei Geldausgabeautomaten ist die Problematik nicht gegeben, da die vollständige Liste aller Automaten bei der Payment Services Austria GmbH (PSA) bezogen werden kann. Hier ist also die erste Methode anwendbar. Das ist bei Bankomatkassen nicht möglich. Einerseits gibt es keine zentrale Stelle, an der alle Standorte abgefragt werden können. Andererseits kann es durchaus sein, dass eine Bankomatkassa jeden Tag ihren Standort wechselt, z. B. die vom Fanartikelshop eines Künstlers auf Tournee verwendete Bankomatkassa.

Im Rahmen einer Bachelorarbeit wurde ein Service zum Prüfen der Kontobewegungen realisiert (Pöchtrager, 2014). Dabei wurden für die Standorte der Geldausgabeautomaten die Liste der PSA herangezogen und für die Bankomatkassen der Ansatz der Lokalisierung mittels räumlichen Profil realisiert. Zur Prüfung der Nutzbarkeit wurde an einigen Geldautomaten Geld behoben und währenddessen das räumliche Profil des Karteninhabers mittels Smartphone ermittelt. Die Abweichung der Lokalisierung von Gerät und Karteninhaber lag bei 25 Testbuchungen an den (bekannten) Geldautomaten zwischen 20 und 25 m. Eine automatische Verifikation gelang während des Tests für alle Geldbehebungen, wenn sich der Geldautomat im Freien befand. Ein unterirdisch im Ausgangsbereich einer U-Bahn-Station aufgestellter Geldautomat konnte mangels Satellitenpositionierung nicht verifiziert werden. Das hätte nur durch kurzzeitiges Verlassen des Gebäudes kurz vor oder nach der Transaktion verhindert werden können. Allgemein kann man sagen, dass die Verifikation von Bankomatkartenbuchungen erfolgreich ist, wenn man nach dem Einkauf bzw. der Buchung das Geschäft und damit das Gebäude zügig verlässt. Alle Analysen (mit Ausnahme der initialen Geocodierung der Geldausgabeautomaten) konnte lokal durchgeführt werden. Somit wäre die Privatsphäre des Nutzers geschützt, da die Geocodierung der Geldausgabeautomaten vor der ersten Nutzung des Services erfolgte und danach keine weiteren Informationen mehr an andere Services übertragen wurden.

6 Schlussfolgerungen

In dem Artikel wurde versucht aufzuzeigen, wie ein Web-Service gestaltet sein müsste, das die Privatsphäre der Nutzer wahrt. Es hat sich gezeigt, dass die Realisierung eines solchen Dienstes durchaus möglich wäre. Dazu müssen Speicherung und Analyse der sensiblen Daten auf dem Rechner des Nutzers selbst erfolgen. Somit kommen keine serverseitig laufenden Skripts infrage, sondern das Skript muss auf den Rechner des Nutzers übertragen und dort aufgeführt werden. Dabei muss natürlich sichergestellt sein, dass das Skript keine negativen Auswirkungen auf den Rechner des Nutzers hat, also keine Trojaner o. Ä. installiert. Die ausschließliche Nutzung seriöser Anbieter ist zwar ein vernünftiger Ansatz, bietet aber keine Garantie, wie das Beispiel Apple zeigt (Welt.de, 2012; Deutsche Wirtschafts Nachrichten, 2015).

Problematisch ist die Abfrage zusätzlich benötigter Informationen. Aus dem Inhalt der Abfragen könnten zumindest auf Teile der persönlichen Daten geschlossen werden. Im konkreten Beispiel waren das die Standorte der Geldausgabeautomaten. Würden diese Automaten erst bei erstmaliger Nutzung geocodiert, so würde das wieder Rückschlüsse auf das räumliche Profil des Nutzers zulassen. Man muss also bei der Abfrage sonstiger Informationen aus dem Internet Vorsicht walten lassen um nicht unbeabsichtigt private Daten preiszugeben.

Literatur

Bundesverfassungsgericht (2010). *Urteil vom 02. März 2010 In dem Verfahren über die Verfassungsbeschwerden gegen die §§ 113a, 113b des Telekommunikationsgesetzes*. ECLI:DE:BVerfG:2010:rs20100302.1bvr025608.

Deutsche Wirtschafts Nachrichten (07.08.2015). *Ende einer Legende: Apple-Computer können von Virus befallen werden*. Retrieved Feb 01, 2017, from https://deutsche-wirtschafts-nachrichten.de/2015/08/07/ende-einer-legende-apple-computer-koennen-von-virus-befallen-werden/.

DSG (2000). *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz)*. BGBl. I Nr. 165/1999. Retrieved Jan 31, 2017.

Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. In: J. Drummond, R. Billen, E., João, & D. Forrest (Eds.), *Dynamic & Mobile GIS: Investigating Change in Space and Time* (pp. 35–51). Boca Rator, FL: CRC Press.

EU (2000). *Charta der Grundrechte der Europäischen Union*. Amtsblatt der Europäischen Gemeinschaft, 2000/C 364/01, 22 p.

Fichtinger, C. (2006). Schutz der Privatsphäre. *Öffentliche Sicherheit*, *5-6*(6), 155–159. Retrieved Feb 01, 2017, from http://www.bmi.gv.at/cms/bmi_oeffentlichesicherheit/2006/05_06/files/persoenlichkeitsschutz.pdf.

Google (2016). *Google Maps APIs*. Retrieved Feb 01, 2017, from https://developers.google.com/maps/documentation/javascript/geocoding?hl=de.

McKenzie, G., & Janowicz, K. (2014). Coerced Geographic Information: The Not-so-voluntary Side of User-generated Geo-content. In: K. Stewart, E. Pebesma, G. Navratil, P. Fogliaroni, & M. Duckham (Eds.), *Extended Abstract Proceedings of the GIScience 2014* (pp. 228–231). TU Wien: GeoInfo Series, Vol. 40.

Moser-Knierim, A. (2014). *Vorratsdatenspeicherung*. Heidelberg: Springer Vieweg, DuD Fachbeiträge.

ORF (2013). *VPN und SSL bieten keinen Schutz*. Retrieved Feb 01, 2017, from http://orf.at/stories/2197467/2197468/.

Pany, T. (2016). *US-Geheimdienste machen Terror gegen Verschlüsselung*. Retrieved Feb 01, 2017, from https://heise.de/-3378390.

Pöchtrager, M. (2014). *Automatische Verifikation von Bankomatkartenbuchungen in Kontoauszügen mittels GPS-Track* (Bachelorarbeit). TU Wien, Department für Geodäsie und Geoinformation.

W3C (2004). *Web Service Glossary*. Retrieved Jan 30, 2017, from https://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/#webservice.

Wagner, L. (2014). *Schnittstellen zur Nutzerinformationsgewinnung von Android und iOS* (Bachelorarbeit). TU Wien: Department für Geodäsie und Geoinformation.

Welt.de (2012). *Hacker schießen sich auf Apple-Geräte ein*. Retrieved Feb 01, 2017, from https://www.welt.de/wirtschaft/webwelt/article106261140/Hacker-schiessen-sich-auf-Apple-Geraete-ein.html.