Is Privacy Dead? – An Inquiry into GPS-Based Geolocation and Facial Recognition Systems

Jens-Martin Loebel

Is Privacy Dead? – An Inquiry into GPS-based Geolocation and Facial Recognition Systems

Jens-Martin Loebel

Humboldt-Universität zu Berlin, Department of Computer Science, Berlin, Germany
loebel@informatik.hu-berlin.de

Abstract. This paper discusses, conceptually and empirically, the proliferation of geolocation and face recognition systems embodied in modern smartphones and social media networks, which presents a growing concern for a user's rights to privacy. This increase in data sharing brings about the very real threat of misuse, as most users are not aware that their geolocation data can easily be assembled into complete profiles of their everyday activities and movements, their habits and social life. Paired with facial recognition capabilities already present in current social media services, this allows for an unprecedented tracking of users, even those "tagged" through photo uploads by other people. To illustrate this, the author analyzes his own profile, which was created by recording GPS data over a time span of five years. A critical discussion of the results follows.

Keywords: GPS, geolocation, social networks, tagging, privacy, facial recognition, locational privacy

1 Introduction

Ubiquitous energy-self-sufficient devices like smartphones and mobile navigation systems allow the user to easily track his or her position using GPS and cell tower triangulation. This in turn enables new kinds of useful applications, especially in the realm of social media. However, these applications and systems create and digitally store a plethora of user information including movements through the public space. In the coming years these systems will become more entrenched in the everyday life of Internet users but are already available today. Services like Foursquare, Gowalla or Apple's Find my Friends App allow the user to "check-in" and share their physical location with friends, collect virtual badges and get coupons by visiting restaurants or shops using their GPS-enabled smartphones in real time.

Social media giants like Facebook or Twitter have followed suit, enabling users to enrich their posts with GPS coordinates. This increase in data sharing brings about the very real threat of misuse, as most users are not aware that their geolocation data can easily be assembled into complete profiles of their everyday activities and movements, their habits and social life. Paired with facial recognition capabilities already

adfa, p. 1, 2011.

present in current social media services, this allows for an unprecedented tracking of users, even those "tagged" through photo uploads by other people.

The problem lies in the aggregation and mixing of different data sets, creating new contexts in which user data may be misused, leading to a loss of control on the part of the user. In this paper the technical details of geolocation and facial recognition systems are discussed, common applications are presented and threats to privacy and data protection are identified. To illustrate this I will create my own movement profile from meticulously recorded location data over a time period of five years. Using data mining techniques, I will present my aggregated profile to visualize what information can be derived simply from using geolocation data, facilitating a discussion about privacy.

2 GPS and Assistive Technologies

The satellite-based NAVSTAR Global Positioning System (GPS) consists of 24 active satellites on different paths in an orbit of 20183 km, completing two revolutions in a sidereal day (about 23 hours and 56 minutes). Originally developed in 1973 by the U.S. Department of Defense to provide precise guidance and navigation for missiles and soldiers in armed conflicts, the system has been fully operational since 1994. The conception as a war material manifested itself in certain design choices notably a high navigational accuracy, high resistance against signal jamming and – most importantly – the ability to passively calculate one's position using only the received GPS satellite data. Furthermore satellite distribution is not equal but higher over inhabited areas (possible conflict zones) [1].

After the deactivation of the signal degrading "Selective Availability" feature by President Clinton in 2000 the systems now allows for a high degree of accuracy (less than five meters) in civilian application. This in turn enabled civilian users to fully utilize the system, leading to a wide range of applications including electronic sea/land/air navigation systems, progress analysis and tracking in running sports and even new leisure sports like "geocaching" (a GPS driven outdoor treasure hunt) or the enrichment of holiday photos with GPS coordinates of their location. Affordable hardware GPS receivers in mobile phones or dedicated car navigation systems have made the GPS system the predominant method for position tracking, navigation and meeting friends in the real world using location-based social networks.

However, a large user base also raises the potential for abuse. Gathered location data may be used to create detailed movement profiles from which daily routines, lifestyle habits or social contacts of a user can be inferred. In order to better assess the possibilities and limits of these systems, a brief description of the technical process follows.

2.1 Reception and Mobile Phones

GPS relies on the principle of indirectly measuring the distance between simultaneously observed (received) satellites and the antenna of the GPS receiver. Using an

atomic clock, each satellite continuously calculates its orbital position and broadcasts a message containing the current time and an ephemeris (a table of values which help provide the precise orbit for the satellite) wirelessly with the GPS signal.

A GPS receiver on earth – also containing a clock – then simultaneously receives the signals of all satellites above the horizon. The receiver will then calculate a pseudo distance (called pseudorange) to the respective satellite's orbital position (as received with the ephemeris) using the time difference between the received timestamp and the current time. This approximation however does not represent the actual geographical distance as the radio waves from the satellite get distorted, deflected and even slowed down on their way to earth, affecting their transit time.

The biggest source of measuring error is the complex dispersive interactions of the radio waves with the ionosphere (the so called ionospheric effect) that heavily distorts the signal and for which there is not good mathematical approximation model. However the amount of distortion is the same across all frequencies. The system therefore broadcasts two sets of data on two different frequencies.

One is the C/A-Code (Coarse/Acquisition), part of the civilian Standard Positioning Service, which is transmitted on the frequency L1 (1,57542 GHz). The other is the secret encrypted P(Y)-Code, part of the military Precise Positioning Service, which is transmitted both on L1 and on a secondary frequency L2 (1,2276 GHz), which factors out the ionospheric effect. Since the mathematical function for decoding the Y-Code is unknown, only the U.S. military and allied government forces can use it. Civilian GPS receivers do not have this advantage, which leads to a severely reduced accuracy of the calculated position to a range of about 20-50 m [1]. To compensate for this and keep the deviation less than 10 meters, a range of assistive technologies utilizing satellite and ground radio stations as well as internet-based extensions, that deliver correcting data, are being used. Satellite based systems use evenly distributed fixed reference ground stations to cover a wide area. These stations receive the GPS signal, compare the calculated location with their own known location and subsequently use this information to create a map of the ionospheric distortions. This information in turn is then sent to a satellite, which rebroadcasts the signal to GPS receivers. This technique is called differential GPS (DGPS). There are several compatible DGPS-Systems in different geographic regions of the world. In widespread use are the Wide Area Augmentation System (WAAS) in North America, the European Geostationary Navigation Overlay Service (EGNOS) in Europe, the Multi-functional Satellite Augmentation System (MSAS) in Japan and the Globalnaja Nawigazionnaja Sputnikowaja Sistema (GLONASS) in Russia. A respective system for India (GAGAN) is currently being deployed [2].

The GPS signal itself is encoded using code division multiple access (CDMA, spread spectrum around a carrier frequency) allowing for a high resistance against signal jamming. A sequence of pseudo random numbers (created with a mathematical function) is being used to synchronize the signal between the satellite and the receiver by encoding the GPS message data with it. The initialization vector of this function is the time measured by the atomic clock on the respective satellite. The GPS receiver on the ground calculates the same values using its built-in clock and then tries to find a maximum correlation with the received numbers. This process leads to an initial

startup delay as the GPS receiver tries to synchronize with all satellites and build an almanac from the received ephemerides.

The calculated pseudoranges span a spherical surface around each satellite and the GPS receiver. The intersection of two spheres is a circle. The intersection of three spheres represents the GPS receiver's position on earth (and another point inside the plasmasphere which is discarded). In the real world however, a forth sphere/satellite is needed because the clock in a GPS receiver is not precise enough to sync exactly with the atomic clock aboard the satellite. The forth sphere is used to determine the time drift between the clocks. This allows the receiver to derive the correct geographical distance from the calculated pseudorange. Therefore to calculate a GPS position at least four satellites need to be observed at the same time with each additional satellite enhancing the position accuracy.

Smartphones and other mobile devices are nowadays usually equipped with a GPS receiver chip and have access to the Internet. These devices employ a different technology to combat the aforementioned shortcomings (long initial startup time and poor accuracy without correction data). They utilize additional information like the ID number of connected nearby mobile GSM cell towers or the MAC-address of visible WiFi networks [2]. This data is sent via the phone's Internet connection to special information services (operated by commercial enterprises) and/or the user's cell phone carrier. The inquired services maintain a database with the geographical location of every cell phone tower as well as commercial and private user WiFi networks (if recorded). The gathered locations can then be used to triangulate the phone's location within a radius of about 50 to 500 meters. This rough location can then be used to narrow the search within the calculated satellite spheres leading to a significantly shorter startup time. In addition GPS almanac data may be received over the Internet. This technique is called assisted GPS (AGPS). Also DGPS data may be received from a server on the Internet instead of a satellite.

2.2 Geodetic Datum and Address Resolution

The so derived GPS map datum consists of latitude, longitude, height above sea level and (system-inherent) a current timestamp. A GPS datum is therefore always a 4-dimensional vector. Latitude and longitude are represented as degrees and arc minutes after the World Geodetic System of 1984 (WGS-84). This geodetic reference system defines a reference ellipsoid (segmented in degrees of latitude and longitude) around the earth and its atmosphere that is the basis for all position information.

To be useful for the user the map datum (e.g. "52° 22.711' N, 4° 54.020' E") needs to be augmented with a meaningful semantic connotation (like "Centraal Station, Entrance, Amsterdam, Netherlands"). On mobile phones this is accomplished by querying an online semantic map database with the user's location. With few exceptions these databases are again operated by commercial enterprises (see chapter 4). In any case a digital map is needed to show the user's position in a geographical context.

Most importantly the usage of such assistive technologies and online map databases add an active return channel to the otherwise passive GPS system that needs to be examined further.

3 Facial Recognition Systems

In addition to GPS chipsets practically all modern smartphones are equipped with a digital camera. In recent years advances in image and face recognition algorithms have led to a number of online applications that could potentially affect a user's right to privacy.

Traditionally facial recognition/identification has been employed in a security context, particularly in the realm of government (e.g. biometric passports) and law enforcement applications. However face detection and recognition systems are increasingly being used in consumer products and social network software. One has to differentiate between simple face detection algorithms, which are built-in to digital cameras, smartphones and webcams, tracking user movement and helping to adjust lens/focus settings. These systems while able to detect a human face cannot differentiate between two or more faces. For this purpose face recognition systems are employed that have the ability to match human faces in images or video frames. Utilizing feature detection algorithms the geometry of a detected face is analyzed and distilled as a unique hash value / feature set for a particular person.

3.1 Common Uses and Privacy Concerns

Such technology is ubiquitously being used in consumer photo manipulation and/or digital media management applications – offline as well as online.

Programs like Apple's iPhoto automatically detect faces in all imported photos and can match faces with the user's address book contacts after an initial pairing. While iPhoto works "offline", online photo albums like the Windows Live Photo Gallery and Google's Picasa have the ability to automatically detect faces in all uploaded photos. These services are popular and commonly used to share photos with family and friends. Moreover the images may be enriched with GPS location data.

Social media giant Facebook adds another dimension by employing face recognition on all stored photos as well as the ability for users to manually "tag" photos with the person's name in any public photo and identify the faces of users, helping to organize and easily find photos of friends and family.

The main privacy issue affected by face recognition technology is the ability to covertly and more or less reliably identify persons using only the facial features extracted from a photograph. It therefore becomes possible to do this on a large scale and match faces in newly uploaded photographs with previously extracted facial features. This makes it possible to attribute online behavior and posts to specific users and infer more information like visited places or travel patterns.

If deployed widely enough or given a big enough database these systems can reliably track users online and offline movements (if used in CCTV systems), which could fundamentally change expectations of privacy, as it becomes possible for commercial enterprises to covertly track users and use the gathered information for advertising and other purposes. As it is undesirable or even impossible to constantly cover one's face when moving through the public sphere there is little a user can do to protect him

or herself. However privacy-preserving facial algorithms do exist and are currently being researched which could help mitigate this problem [3].

4 Location-based Applications and Dangers

While the use of GPS and facial recognition systems yields many benefits for users, the potential for misuse is high. Complications may arise from concatenating or merging separate data sets (thereby creating a complete profile of the user's social activities), using the acquired information in a new and unwanted context or even deriving new data from gathered profiles. Since most of this information is gathered by or stored at private companies, commercial interests play an important part.

As security expert Bruce Schneier recently pointed out, private companies are on the verge of becoming huge data collectors of personal information. With their business interests in marketing and profiling, this creates new kinds of threats that as of yet are not always fully governed by current laws. Schneier calls this new model "feudal security", whereby users have to place their trust with companies like Apple or Facebook [4].

Also since companies operate most online map databases the aggregation of (new) location information is very valuable. Besides fee-based services from companies like Navteq or Tele-Atlas one of the biggest player is Google, which offers its "Google Maps" service and accompanied digital maps free of charge for end users. Users with smartphones running the Google-owned Android operating system (but also those using Apple's iOS devices) compulsory transmit their phone's current location to Google each time the service is queried as these systems utilize the Google's database and maps.

If AGPS is being used, data identifying a user's location is also transmitted to either the cell phone carrier or – in the case of using WiFi data – to other companies like Skyhook Wireless[1]. Beyond that Google and Apple actively build up and maintain their own respective location databases utilizing the user's phone to (in the background) constantly transmit anonymized information about observed WiFi networks paired with a GPS location. Apple grants itself and its partners and licensees extensive rights to "collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device" [5]. Accepting these terms of service is mandatory if a user wants to use the GPS features and "Location-Based Services" provided by Apple.

Even though clearly stated in the terms of service's privacy policy, concerns about the possibility of abuse led to outrage and criticism in 2010 in U.S. specialized and daily press as well as online publications [6-8]. In Germany federal commissioner for data protection (Bundesbeauftragter für den Datenschutz) Peter Schaar and federal consumer affairs minister (Bundesverbraucherschutzministerin) Ilse Aigner voiced concerns and condemned the hidden transmission of location data when using geolocation applications [9].

---

[1] Skyhook (http://www.skyhookwireless.com/) is one of the biggest companies offering MAC address to geographical location translation services.

Another example of hidden data transmission is online navigation systems for cars. These systems (available either as dedicated hardware or in the form of a mobile phone app) – while in navigation mode – transmit the car's exact position, speed and heading in regular intervals to the navigation system's manufacturer. The collected movement data is then used by the manufacturer to create traffic profiles and identify areas of traffic congestion. This information in turn is transmitted back to every connected navigation device, helping users of the system to avoid congested areas. The upside of this is highly accurate and up to date traffic information, the downside being that the manufacturer gains a complete movement profile of the user [10].

There is a strong imbalance between the commercial value of a complete movement profile and (in this case) the user's ability to better avoid traffic jams. It is technically easy to (covertly) collect and transmit GPS data. The associated monetary value makes this a desirable enterprise in the private sector with the main focus being the usage of a user's location especially for location-based ads (mobile ad targeting)[2]. The Trojan "AndroidOS.Tapsnake" for Android phones, which was discovered in 2010 by Symantec, can exemplify the value of location data. Disguised as a simple game, this program sends the user's location to a remote server that can be freely configured by the attacker.

The movement data of its citizens may also be of interest to the government as shown by the recent call for a GPS-based car toll system for German highways [11].

4.1 Location-based Social Networks

The transmission of location data is not always hidden from the user. In fact in the majority of cases the user consciously and willingly initiates the transfer to gain some form of added value.

For example Apple's "Find my Friends" app – built into iOS version 5 – is based on this concept[3]. Users can allow their friends to track their location to arrange a meeting or quickly find one another in crowed public places. As long as the user does not block a "friend" again, he or she may constantly monitor the user's whereabouts. For this to work the device periodically send the user's location to Apple's servers which in turn theoretically allows Apple to create complete movement profiles of all participants.

Furthermore Internet enabled smartphones allow the user to participate in so-called location-based social networks. These networks make it possible (like "Find my Friends") to share the user's location in real-time with friends or others. Moreover they offer new forms of interaction like the possibility to collect "virtual badges" or get coupons by visiting certain hotels, restaurants or clubs. Known representatives of this genre are networks like Foursquare (http://www.foursquare.com), Gowalla (http://www.gowalla.com) and Google Latitude (http://www.google.com/latitude),

---

[2] In fact Google owns a Patent concerning location-based advertising. See U.S. Patent number 8,138,930 "Advertising based on environmental conditions".

[3] See "Find my Friends" and "Find my iPhone" at http://www.apple.com/icloud/features/find-my.html.

which enjoy increasing popularity. The allure of combining the virtual world of the Internet with the real world using location data hasn't passed social media giants like Facebook or Twitter. Both have for some time now offered the ability to enrich user posts with location data. The use cases for location enabled social networks are predominantly to make contact with other persons in the vicinity, play location-based games (with either virtual or real rewards) and to automatically record one's daily routing in a virtual diary [12].

Location data may also be used associate digital photos with the photograph's location (called Geotagging). Paired with Facebook's facial recognition and tagging ability this allows to identify a user at a given location even if the photo was taken by someone else. What all these services have in common is the concatenation of location data with personal information or posts, which can become a sort of "currency" within these services [13].

As is the case with any economic system, the increased availability of this type of data brings with it (besides benefits) an increased potential for commercial exploitation and misuse like identity theft. It is possible for these companies to generate detailed movement profiles from the aggregated data with insights into a user's daily routine, lifestyle and social contacts. This carries broad implications for user privacy rights and is in direct contrast to their expectation when using these services or networks. A user generally does not assume that his or her every step will be recorded, kept indefinitely and mined at any point in the future for alienated purposes.

The hazard potential is best made clear by the 2010 project "Pleas Rob Me" [14]. The algorithm on the associated website raided social networks for private information like home address, first and last name and the current location that users had posted publically. If distance between the home address and the current location stayed above a certain value for several days, the collected information was published on the site as an "opportunity" for theft. The authors wanted to raise awareness about the inherent dangers of location sharing in social networks.

The Electronic Frontier Foundation (EFF), a U.S.-based non-profit digital rights group, summarized this problem in 2009 and coined the term Locational Privacy as "the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use" [15]. Locational Privacy is a property worthy of protection, as it cannot be regained once the data has been shared.

5 Self Experiment

To bring this unperceived data to the surface and generate my own extensive movement profile to see what data can be inferred, I started my own experiment. For the past five years I have recorded all of my movements in the public sphere using several GPS receivers. With the collected data I was able to create and analyze a comprehensive movement profile. Of particular concern were questions about what conclusions about my social contacts and personal lifestyle could be drawn from my profile, and

how much data over what time period was necessary to answer the first question to a high degree of accuracy.

The data was stored in the form of waypoints, which were arranged logically as tracks by my GPS receivers. Each time satellite reception was lost for more than 30 seconds or the device was turned on (usually when entering or leaving a building) a new track was created. If the device could determine my location, a waypoint was automatically recorded once every second if it was at least 5 meters apart from the last waypoint or a maximum of 5 seconds had passed.

The collected data was extracted from the devices using the open source software GPS-Babel (http://www.gpsbabel.org) and subsequently stored in a SQL database.

5.1 Data Analysis and Combination

Only two consecutive waypoints are needed to infer my current speed (using the difference between timestamps) and heading (creating a vector from the coordinates). Combining speed information with digital maps that show roads and train tracks, it was possible to reliably infer my mode of transportation, whether I was walking, riding a bike, driving a car or boat or even being a passenger in an airplane.

More importantly the accumulation of several consecutive waypoints around an area or a speed of 0 km/h would indicate that I stayed at a certain place for longer periods of time. If the time difference between the first and last recorded waypoint in this area was greater than 15 minutes this usually indicated that the place was somehow significant. It could be my residence, my place of work, hotel, restaurant or a doctor's office that I visited. To identify such significant places in the database I used time-based cluster analysis algorithms [16], which interpret the waypoint data as a directed graph (waypoints being the knots, the vector of two adjacent waypoints being an edge). The computed clusters represent waypoints of proximity in time and space. The time-based approach also eliminates intermittent measuring errors due bad GPS reception [17]. In this case all clusters represent significant places.

My next step was to attach a semantic meaning (like "Fernsehturm, Alexanderplatz, Panoramastraße 1a, Berlin, Germany") to every cluster using the Google's as well as the OpenStreetMap project's map databases. This information was stored again in my SQL database. Using the timestamps of each cluster I was able to construct a graph with chronologically sorted transitions between clusters representing my complete movement profile.

This profile showed every place I had visited and I could easily infer a lot of my lifestyle choices (e.g. what food I prefer based on the restaurants I had visited).

I was also able to construct a probability model by analyzing the frequency of transitions between two places in the graph. This allowed me to make educated guesses with a high degree of accuracy about my future movements, especially if they were part of my daily routine [18]. If I had the movement profile of other people (like social network operators do) I could have inferred all my social contacts using profile correlation.

Generally only 3 to 4 weeks worth of data was needed to create a 90% accurate probability model of future movements, the worst-case being 3 months worth of data.

5.2 Technical, Lawful, Social Restrictions/Limits

My experiment faced pragmatic and technical limits that prevented a complete capture in certain situations. Sometimes it was not possible to wait for a satellite fix after turning on the receiver (as not all receivers I used has AGPS) due to time constraints or pressure from colleagues to start walking. Due to the low power nature and chosen frequency of the GPS signal the radio waves can only penetrate bodies of water up to a depth of about 2 meters. This meant that I could not record any of my scuba dives. When travelling in an airplane all electronic devices must be switched off during taxiing, takeoff and landing, which prevented me from recording a complete flight. Reception was generally only possible in a window seat given the shielded nature of airplanes. Lastly certain countries like Egypt prohibit the use and possession of civilian GPS receivers. Despite these constraints I was able to construct a complete movement profile. For further details on how the conscious process of recording affected my behavior in the public space and data visualization techniques see [19].

6 Conclusion

Portable GPS receivers like mobile phones or navigation systems have permeated our daily life and allow for new and interesting usage scenarios and applications. The (unwanted) continuous transmission of location data via a return channel as well as the enrichment of personal information or photos with location data in social networks, however, have a high potential for misuse with concrete ramifications for a user's privacy and data protection. Combined with facial recognition technology and the ability to tag persons in photos on social media networks this allows for an even higher degree of surveillance and yields the ability to connect location data with the identity of a user. In addition face recognitions systems are covert by nature and do not require any action or presence on part of the user.

The experiment shows how easy it is to collect and process GPS data. Users are generally unaware of the extent to which their data are transmitted, processed and used, which creates gap between what is technically possible and a user's assessment of the situation. Using cluster analysis I was able to determine all significant places of my daily routine, create a detailed movement profile and make highly accurate predictions about my lifestyle choices and future movements. One the one hand the wealth of information that can be deducted is frightening. On the other hand the conclusion should not be to avoid geolocation services and applications, as they offer many benefits. Rather one should take the EFF's position and educate users about the process, clearly explain benefits and possible dangers, and teach a principle of data economy.

This could help users to critically reflect on the services they use. In addition many services have data protection and privacy settings that can be enabled by the user. Smartphones using Android or iOS, for example, have the ability to disable location sharing on a per-app basis. Additionally it is the job of regulators to augment current privacy laws to better reflect current use cases set up barriers for companies and government bodies on what information may be recorded and in what context it may be processed and used. These new systems need to have locational privacy built-in.

References

1. Xu, G.: GPS – Theory, Algorithms and Applications, 2nd edition. Springer, Berlin (2007)
2. Dodel, H., Häupler, D.: Satellitennavigation, 2. korrigierte und erweiterte Auflage. Springer, Berlin (2010)
3. Sadeghi, A. –R., Schneider, T., Wehrenberg, I.: Efficient Privacy-Preserving Face Recognition. In: Lee, D., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 229-244. Springer, Heidelberg (2010)
4. Goodin, D.: Schneier: government, big data pose bigger 'Net threat than criminals. In: ars technica, blog article, 23.2.2012, http://arstechnica.com/business/news/2012/02/schneier-gov-big-data-pose-bigger-net-threat-than-criminals.ars
5. Apple: Privacy Policy, last revised October 2011, http://www.apple.com/privacy/
6. Sarno, D.: Apple Collecting, Sharing iPhone Users' Precise Locations, Los Angeles Times Online, http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html
7. Allan, A., Warden, P.: Got an iPhone or 3G iPad? Apple is recording your moves, O'Reilly radar, 20.4.2010, http://radar.oreilly.com/2011/04/apple-location-tracking.html
8. Johnson, B.: Researcher: iPhone Location Data Already Used By Cops',GigaOM Blog, 21.4.2011, http://gigaom.com/2011/04/21/researcher-iphone-location-data-already-used-by-cops/
9. Meyer, C.: Datenschutzbeauftragter warnt vor Missbrauch bei Handy-Ortung, Heise-Newsticker, 30.5.2010, http://heise.de/-1010712
10. Greene, K.: Staumeldung gegen Bewegungsprofil, Technology Review Online, 25.11.2008, http://www.heise.de/tr/artikel/Staumeldung-gegen-Bewegungsprofil-275834.html
11. Barczok, A.: Kretschmann will satellitengestützte PKW-Maut, Heise-Newsticker, 16.10.2011, http://heise.de/-1361871
12. Kirkpatrick, M.: Why We Check In. The Reasons People Use Location-Based Social Networks,ReadWriteWeb, http://www.readwriteweb.com/archives/why_use_location_checkin_apps.php
13. Heuer, S.: Sag mir, wo Du bist! – Geodaten werden zur neuen Währung im Web – mit zwiespältigen Folgen für Anbieter und Nutzer. In: Technology Review, volume 07, pp. 44-49. Heise Zeitschriftenverlag, Hannover (2010)
14. Borsboom, B., van Amstel, B., Groeneveld, F.: Please Rob Me – Raising Awareness about Over-Sharing, http://pleaserobme.com/
15. EFF – Electronic Frontier Foundation (ed.): On Locational Privacy, and How to Avoid Losing it Forever, Whitepaper, San Francisco, CA (2009), http://www.eff.org/wp/locational-privacy
16. Cao, Xin et al.: Mining Significant Semantic Locations from GPS Data. In: Proceedings of the VLDB Endowment, 3, pp. 1009–1020 (2010)
17. Kang, J. H., et al.: Extracting Places from Traces of Locations. In: ACM SIGMOBILE Mobile Computing and Communications Review, 9 (3), pp. 58-68. ACM, New York (2005)
18. Gutjahr, A.: Bewegungsprofile und -vorhersage, LBS/Location Awareness - Technische Hintergründe und juristische Implikationen, http://www.ks.uni-freiburg.de/download/papers/interdiszWS08/Alexander_Gutjahr.pdf
19. Loebel, J.-M.: Aus dem Tagebuch eines Selbstaufzeichners. Laborgespräch mit Ute Holl und Claus Pias. In: Zeitschrift für Medienwissenschaft, Volume 4 – Menschen & Andere, I/2011, pp. 115-125. Akademie Verlag, Berlin (2011)