Personal Privacy and the Web of Linked Data

David Corsar, Peter Edwards, and John Nelson

dot.rural Digital Economy Hub,
University of Aberdeen, Aberdeen, UK
{dcorsar,p.edwards,j.d.nelson}@abdn.ac.uk
http://www.dotrural.ac.uk

Abstract. This paper reports the results of a study investigating the user privacy challenges when personal data is published within linked data environments. Motivated by *GetThere*, a passenger information system that crowdsources transport information from users (including personal data, such as their location), four scenarios are outlined that illustrate how linked data environments can impact upon user privacy. The responsibilities of key stakeholders, including researchers, ethics committees, and the linked data community are also discussed, along with a set of guidelines designed to raise awareness of these risks and how to reduce them.

Keywords: Personal privacy, semantic web, linked data

1 Introduction

Many applications routinely combine the use of mobile devices and location-aware services. However, when location information, or any other type of personal information is made available, even in an anonymised form, there is the potential for it to be integrated with other data as part of the Web of Linked Data. Automated agents can then reason about this data, with no guarantee that such reasoning is privacy preserving.

As part of the Informed Rural Passenger (IRP) project[1] we are developing *GetThere*, a real-time passenger information (RTPI) system for public transport in rural areas. Crowdsourcing techniques are used to allow passengers to contribute public transport information using a smartphone app; the contributions benefit all users, by providing access to real-time information that is otherwise unavailable. These observations about vehicle location, occupancy levels, and facilities, are integrated with a number of other datasets using linked data principles[2]. These datasets are themselves described by ontologies, and linked using technologies such as Uniform Resource Indicators (URIs) and the Resource Description Framework[3] (RDF), to enable software agents to find and reason about information.

[1] http://www.dotrural.ac.uk/irp
[2] http://www.w3.org/DesignIssues/LinkedData.html
[3] http://www.w3.org/RDF/

Given the sensitive nature of the information collected from passengers (e.g. their location) ensuring privacy of contributors and their information is vital. However, in a linked data environment this is more challenging than simply restricting access, or removing clearly identifying features (e.g. names), as the existence of related (and linked) datasets may be used to infer characteristics of the original information source [20].

This paper presents the results of a study into *Personal Privacy and the Web of Linked Data* conducted as part of the Framework for Responsible Research and Innovation in ICT[4] project funded by the UK's Engineering and Physical Sciences Research Council. The case study investigated the risks and uncertainties associated with user privacy in linked data environments. The datasets developed to support *GetThere* (discussed in Section 2) motivated the identification of scenarios illustrating these risks (Section 3). Responsibilities for the relevant stakeholder groups to support personal privacy are discussed in Section 4. Guidelines to increase awareness of potential risks and how to reduce them are presented in Section 5.

2 Background

As noted above, the *GetThere* system uses linked data principles [9]. to integrate passenger contributions with several other datasets. HTTP URIs are used, as is RDF, a machine processable data model for the exchange of data on the Web. HTTP URIs provide identifiers for resources, which agents can look-up to retrieve information about that resource. Web-based ontologies, defined using RDF Schema[5] and the Ontology Web Language[6], add structure to RDF data, by describing domain concepts, and the relationships between these (and other) concepts.

The *GetThere* system is supported by four main datasets[7]:

- Infrastructure: provides details of the road network, extracted from OpenStreetMaps[8] and converted into RDF. This is currently not included in the LinkedGeoData[9] dataset, a linked data version of OpenStreetMap information including places, shops, and tourism sites.
- Public transport timetable[10]: provides details of bus timetables including routes and arrival/departure times at bus stops. Timetables are linked to the NaPTAN dataset[11], which provides details of each bus stop, including its name, unique ID, and location.

[4] http://responsible-innovation.org.uk/frriict/
[5] http://www.w3.org/TR/rdf-schema/
[6] http://www.w3.org/TR/owl-ref/
[7] Ontologies describing the datasets are available from http://www.dotrural.ac.uk/irp/uploads/ontologies
[8] http://www.openstreetmaps.org
[9] http://www.linkedgeodata.org
[10] Described using the Transit ontology - http://vocab.org/transit/terms
[11] http://data.gov.uk/dataset/naptan

– Users: provides details of registered *GetThere* users. This includes user accounts described using the Semantically Interlinked Online Communities[12] and Friend Of A Friend (FOAF)[13] ontologies. These provide a nickname for each user and their email address used for the system; a description of each user's mobile device(s) is also stored.
– Journeys: describes trips made by *GetThere* users on public transport during which they have contributed information. Along with the bus route and direction of travel, this also includes details of the observations (e.g. vehicle location) provided, which are represented using extensions of the W3C Semantic Sensor Network ontology[14].

3 Scenarios

During a meeting of, and subsequent discussion between, researchers in semantic web, linked data, and personal privacy, the *GetThere* system and datasets were used to motivate the identification of a number of scenarios[15]. Each scenario illustrates risks related to personal privacy as a result of publishing user's personal data (or data derived from it). It should be noted that these scenarios and risks arise whenever personal data is published online, regardless of the technology used, and that the use of linked data simply serves to make it easier for adversaries to access and use such data.

The scenarios were structured in terms of: name; general description; details of the data published (either user data or data derived from it), including its content and the technology used to publish it; how that data could be integrated with other datasets by an adversary; the reasoning necessary to identify characteristics of the user; and the resulting information determined about the user. We summarise the scenarios below[16].

3.1 Enhanced Phishing Attacks

Phishing attacks consist of emails that attempt to deceive the recipient into disclosing personal information (e.g. a username and password) or installing malware on their device. While basic phishing emails are easy to identify, more sophisticated emails that have been tailored to the recipient are amongst the type of spam that result in the greatest number of recipients acting upon the email [5]. Environments containing personal information potentially provide adversaries (malicious users) with the information required to automatically produce emails that are highly tailored to the recipient [18]. For example, an individual's FOAF

[12] http://rdfs.org/sioc/spec/
[13] http://xmlns.com/foaf/0.1
[14] http://www.w3.org/2005/Incubator/ssn/ssnx/ssn
[15] The discussion initially focused on the *GetThere* datasets, but quickly broadened out to discuss other types of data.
[16] A video discussing and illustrating these scenarios is available at http://vimeo.com/46583809

profile provides their name, email address, birthday, and links to FOAF profiles of people known to them. This is sufficient to produce a tailored phishing email which, for example, wishes the receiver happy birthday or references their recent blog post [18].

Within the *GetThere* datasets, a user's FOAF profile is linked to each journey they have made using *GetThere*. The journey description includes the date, start time, route travelled, direction of travel, and details of locations they provided during that journey. Publishing this information provides an adversary with details that could be used to further personalise phishing emails. For example, an adversary could retrieve the journeys made by each user and the people they know (taken from their FOAF profile), and by reasoning about the route, time, and proximity of locations contributed during those journeys, attempt to determine any journeys during which they may have travelled together. If successful, this enables a phishing email to be produced that appears to come from a friend, with the correct email address and name, references the receiver by name, and contains a small piece of relevant personal information, such as a reference to their recent shared journey.

3.2 Identifying Unoccupied Properties

The website pleaserobme.com[17] highlighted the danger of users sharing their location on sites such as foursquare[18] and Twitter[19]. Assuming the check-in/tweet is correct, such information can be used to indicate when somebody is away from home. However, this does not provide that person's home address. As part of *GetThere*, when a user boards a bus, they tap a button on the app that starts continuously uploading their location to a server. A webpage then uses a web service to retrieve this real-time vehicle location and display it on a map for other users. Upon alighting from the bus, the user stops sending their location. While no details of the source of a real-time bus location are published, such location data could potentially be used to determine unoccupied properties.

This is due to the nature of rural areas: passengers can board/alight the vehicle at any point along the route (not just at bus stops), potentially doing so very close to their home. To identify an unoccupied property, an adversary would simply need to integrate the first or last location provided by a user on a journey[20] with the postcode dataset published by the UK OrdnanceSurvey[21]. This dataset provides the centroid location (longitude and latitude) for every UK postcode. Integration can be performed by determining the postcode nearest a vehicle location either by querying the postcode dataset or using existing web services[22]. Other web services can then be used to determine the number

[17] http://pleaserobme.com
[18] https://foursquare.com
[19] http://www.twitter.com
[20] This can be determined by monitoring vehicle locations provided by *GetThere* using the web service that supports the map.
[21] http://datahub.io/dataset/uk-postcodes
[22] For example, http://www.uk-postcodes.com/api.php

of addresses at that postcode[23]. In contrast to urban areas, postcodes in rural areas can have only one or two properties, and so the adversary has potentially identified when a member of that household has left/returned to the property. *GetThere* could be monitored over time, or the journey dataset queried to determine user travel behaviour patterns, including when they regularly leave and/or return home.

3.3 Attacking Location Obfuscation

Location-based services typically utilise the GPS in a mobile device to accurately[24] monitor and record a user's location [16]. However, apps using this information can potentially violate a user's location privacy [3]. Obfuscation methods attempt to maintain location privacy by degrading the quality of such information, reducing the probability that the reported value is the user's true location [8].

When a location is obtained from GPS, the device is actually somewhere within a circle centred on that point with a radius equal to the accuracy of the GPS reading. The probability that the user's true location is any point within that circle can be calculated as a function of the circle's area [1]. A basic approach to location obfuscation is to provide a randomly selected point within that circle; alternatives to this include increasing the circle's radius or decreasing the circle's radius (as the true location may be outside of the smaller circle) and providing a random point within the revised circle, or creating an overlapping circle with the same radius (but different centre) and providing a random location within the overlap [1].

While such obfuscation helps maintain location privacy, additional information could be used to attempt to undo its effects. For example, if we know that a location was obtained while an individual was travelling, we could attempt to identify the road and their location on that road. Map matching algorithms [19, 22, 28] have been developed by the Geographic Information Systems community to perform this task in the context of GPS locations in navigation systems.

The initial step for map matching involves querying datasets (such as the *GetThere* infrastructure dataset) for details of road segments close to a given location. Each road segment consists of a start and end point, with roads being modeled as a list of such segments. The number of segments can be reduced, for example, with the knowledge that the individual was travelling on a particular public transport route, by only retrieving segments for that route. Map matching algorithms then calculate a probability that the individual's true location is on each segment. The segment with the highest probability is then selected, and an estimated location on that segment determined [28]. This allows an adversary to estimate an individual's true location by effectively reversing the obfuscation, thus exposing them to a number of risks.

[23] For example, http://www.postoffice.co.uk/postcode-finder
[24] With an error margin of as little as five metres.

3.4 Resetting User Passwords

Security questions are routinely used by websites to identify a user for the purposes of, for example, resetting their password. Ideally, the answer to security questions cannot be easily guessed or researched, is persistent over time, memorable, and definitive [26]. However, several studies have shown how many common security questions can be successfully attacked by searching publically available information and linking information from multiple sites. This then enables answers to be determined for challenging questions, such as "What were the colours of your secondary school uniform?" [23, 14, 24, 25].

While these studies were performed manually, the growth in online social networking and open data is resulting in the necessary types of information becoming available online in machine readable formats. For example, social network sites have extensive social graphs for their users (a record of all the relationships between a user, the resources they have produced, group memberships, relationships with other users, etc.) [13]. Each social graph contains different pieces of personal information: Linkedin[25] contains details of education and employment; facebook[26] contains friends and family relationships; and LiveJournal[27] contains details of interests. Other datasets providing relevant information are also becoming available online, for example, transcripts of births, deaths, and marriages.

Although each site provides a limited amount of information, if these can be unified into a single graph describing an individual, an adversary has an extensive dataset describing that person. This could be produced automatically using web APIs or screen scraping techniques, with RDF used as a common data format to support integration. The main challenge is then linking the different profiles for a given individual across different sites. Initiatives such as OpenID[28] and research in ontology matching [27, 2, 6] could be used to automate this task. Additional information can then be obtained by linking to datasets on the Web of Linked Data. For example, Linkedin could provide details about the secondary school attended by an individual, which can be linked to the DBPedia[29] entry describing that school, including the uniform colours. This potentially provides the adversary with information about an individual, which could include their name, address, date of birth, social networks, participation in groups, employment history, family relationships, and education; providing sufficient information to answer many common security questions. If successfully used to gain access to an account, the adversary then gains access to any personal information stored within that account.

[25] http://www.linkedin.com
[26] http://www.facebook.com
[27] http://www.livejournal.com
[28] http://openid.net/
[29] http://dbpedia.org

4 Maintaining Personal Privacy - Who is Responsible?

Based on the scenarios described above and our own experience deploying the *GetThere* system, we have identified four stakeholder groups that have a role to play in ensuring users' personal privacy. Briefly, these are the linked data community (including researchers, developers, and practitioners), developers of software that obtains and uses personal information from users (both in general, and within the semantic web community), individuals that share their personal information with software, and ethics committees.

In addition to the development of technologies to protect user privacy, such as security models and access control (e.g. [7, 29]), we argue that the linked data community should also work to educate stakeholder groups about the risks. For example, developers should consider these risks throughout the design and development process in order to influence decisions regarding the amount and type(s) of personal information that will be collected, and how this data, or data derived from it, will be stored, used, and published. These considerations can also influence any other information developers provide that could be useful to adversaries.

When software utilises linked data to represent and publish personal information obtained from users, they should be educated about the resulting potential privacy risks. This will allow users to make an informed decision regarding the information they provide. Education can include providing a simple, clear description of the personal data that will be obtained and any associated risks [21], as desired by both users and regulators [4, 15, 17]. If these details are provided, where appropriate, for software produced by the linked data community, this will raise user awareness of how potential risks arise. This enables users to make similar assessments of any software they share their personal information with, even if such descriptions are not provided.

The linked data community should also shape ethical approval processes to reflect the privacy risks. For example, currently when software is developed as part of a University research project, it may be required to undergo an ethical approval process. However, this process may only ask if any data will be generated and/or stored that could be used to identify an individual. Given the potential risks, we argue that the ethical approval process should require details of the data that will be generated, how it will be processed (including any anonymisation) and published, a review of the privacy risks individuals may be exposed to, and evidence that these are sufficiently minimised and/or justified. The linked data community should be involved in training for ethics committees, equipping them with the ability to appreciate, understand, and evaluate potential risks, enabling them to perform a more comprehensive review of such software.

5 Guidelines

We now discuss a set of guidelines which aim to raise awareness of the issues discussed above and suggest means to address them.

- Many of the risks arise as a result of data from a single user being published (or data derived from an individual's data). Application developers should therefore consider not publishing information when it is based on data from a single user, preferring, for example, to aggregate data from multiple users, making it more challenging to infer characteristics of an individual.
- When acquiring and using fine grained location information from an individual user, location obfuscation techniques based on reporting a false location can be insufficient and are vulnerable to attack in certain scenarios. Therefore, alternative obfuscation techniques should be considered, such as: publishing locations generated by merging those of multiple users; careful use of landmarking (where a nearby landmark is reported instead of the true location); or the return of more abstract locations, such as street or town/city name [10].
- Developers of software that uses personal information from users should produce a set of scenarios exploring the resulting privacy risks. Each scenario should include a general description, the data that is made publicly available, and how an adversary could use that data for malicious purpose(s). When developing such risk scenarios, it may be useful to adopt the role of the adversary, and consider questions such as "How would I (an adversary) use the published data to [stalk, harass, rob, spam, obtain additional personal/private information, gain access to an account of, steal the identity of] a user of the system". Further, developers should consider performing a Privacy Impact Assessment (PIA) for the software. A PIA is designed to allow organisations to "assess and identify any privacy concerns ... and address them at an early stage" [12]. The PIA handbook provides a detailed guide for the process, which includes: evaluating the type of assessment that should be performed (full-scale or small-scale); producing a project outline describing the project, its context, motivations, and objectives; developing a plan for performing the assessment; performing the assessment through consultations with stakeholders, risk analysis, and the identification of problems and solutions; documenting the PIA process; and finally, reviewing and auditing the PIA process.
- Users should be provided with sufficient details to allow them to make an informed choice about using software/contributing personal information. These details should include a concise and jargon free description of the data collected, how that data is used and published, and a description of the associated privacy risks. As many users do not read documentation such as terms and conditions[30], it may be desirable to include non-textual descriptions (e.g. pictures or video) to assist them in understanding the risks.
- Ethical approval processes for research involving linked data should require details of, and justification for all data collected from users, and should not simply ask if identifiable or "sensitive personal data" (as defined by the UK Data Protection Act [11] or equivalent legislation) will be collected. This

[30] It is estimated that 90% of users did not read Google's revised terms and conditions in 2012 [4].

should include requiring evidence that potential risks have been evaluated and addressed. In addition, details of where the data will be physically stored, how it will be stored, the format, how it will be accessed electronically, who will have access to each part of it, and how appropriate access controls will be implemented and enforced within a system, should also be required.

6 Conclusion

In this paper we have discussed issues relating to personal privacy and linked data environments. Although by no means comprehensive, the four scenarios presented here illustrate how adversaries can exploit linked data and semantic web technologies to support attacks on individuals. This is a particular concern as the number of machine-readable, interlinked datasets becoming available online continues to grow.

Technology based approaches being developed (such as controlling access to linked data [29, 7]) form part of the solution to this problem. Tools could also be produced to analyse datasets/ontologies and highlight potential issues to designers. For example, by searching for the use of vocabularies that provide personal information (e.g. a *sioc:UserAccount* with a *sioc:email*) and informing the designer of potential risks (e.g. that publishing this information could result in the user receiving phishing emails). Such tools could also examine potential risks arising from integrating personal data with other data (e.g. if a *sioc:UserAccount* is linked to *geo:lat* and *geo:long* values, this potentially indicates location information about that user will be published). This analysis could also be used to inform users of potential risks when sharing their information with systems.

Another aspect is educating relevant stakeholders, including software developers, users, and ethics committees, about the potential risks to personal privacy. This should allow developers to design software that attempts to minimise the potential risks; enable users to make more informed decisions about the data they share with applications; and provide ethics boards with a greater appreciation and understanding of the risks, enabling them to make more thorough assessments of ethical approval submissions.

To support this, we have designed an initial set of guidelines; however, we recognise that they are just that - a starting point. We would like to see the creation of an open online repository of privacy scenarios and associated guidelines. This repository would serve as a reference point for stakeholders, which can be updated as the semantic web community continues to improve its understanding of issues related to semantic web and linked data technologies and their impact on the personal privacy of individuals. While the actions necessary to minimise the risks are likely to be specific to any given application, and there may be no way of reducing these risks completely, a greater understanding will allow stakeholders to attempt to minimise such risks.

Acknowledgements The research described here is supported by the award made by the RCUK Digital Economy programme to the dot.rural Digital Econ-

omy Hub (award reference EP/G066051/1); and an award from the Framework for Responsible Research and Innovation in ICT project.

References

1. Ardagna, C., Cremonini, M., Damiani, E., Capitani di Vimercati, S., Samarati, P.: Location privacy protection through obfuscation-based techniques. In: Barker, S., Ahn, G.J. (eds.) Data and Applications Security XXI, Lecture Notes in Computer Science, vol. 4602, pp. 47–60. Springer Berlin Heidelberg (2007), http://dx.doi.org/10.1007/978-3-540-73538-0_4
2. Bellahsène, Z., Bonifati, A., Rahm, E. (eds.): Schema matching and mapping. Springer (2011)
3. Beresford, A., Stajano, F.: Location privacy in pervasive computing. Pervasive Computing, IEEE 2(1), 46–55 (2003)
4. Big Brother Watch: Nine in ten people haven't read google's new privacy policy (2012), http://www.bigbrotherwatch.org.uk/home/2012/02/ten-people-havent-read-googles.html#.UBZyUG9ZWb2
5. Brown, G., Howe, T., Ihbe, M., Prakash, A., Borders, K.: Social networks and context-aware spam. In: CSCW '08 Proceedings of the 2008 ACM conference on Computer supported cooperative work. pp. 403–412 (2008)
6. Choi, N., Song, I.Y., Han, H.: A survey on ontology mapping. SIGMOD Rec. 35(3), 34–41 (Sep 2006), http://doi.acm.org/10.1145/1168092.1168097
7. Costabello, L., Villata, S., Rodriguez R., Corcho, O., Gandon, F.: Access control for http operations on linked data. In: Cimiano, P., Corcho, O., Presutti, V., Hollink, L., Rudolph, S. (eds.) The Semantic Web: Semantics and Big Data, Lecture Notes in Computer Science, vol. 7882, pp. 185–199. Springer Berlin Heidelberg (2013), http://dx.doi.org/10.1007/978-3-642-38288-8_13
8. Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: Gellersen, H.W., Want, R., Schmidt, A. (eds.) Pervasive Computing, Lecture Notes in Computer Science, vol. 3468, pp. 152–170. Springer Berlin Heidelberg (2005), http://dx.doi.org/10.1007/11428572_10
9. Heath, T., Bizer, C.: Linked Data: Evolving the Web into a Global Data Space. Synthesis Lectures on the Semantic Web: Theory and Technology, Morgan & Claypool Publishers (2011)
10. Hong, J.I., Landay, J.A.: An architecture for privacy-sensitive ubiquitous computing. In: Proceedings of the 2nd international conference on Mobile systems, applications, and services. pp. 177–189. MobiSys '04, ACM, New York, NY, USA (2004), http://doi.acm.org/10.1145/990064.990087
11. Information Commissioner's Office: UK data protection act 1998 (1998), http://www.legislation.gov.uk/ukpga/1998/29/contents
12. Information Commissioners Office: Privacy impact assessment handbook, version 2.0 (2012), http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
13. Ishold, A.: Social graph: Concepts and issues. ReadWriteWeb (September 2007), http://www.readwriteweb.com/archives/social_graph_concepts_and_issues.php
14. Just, M., Aspinall, D.: Personal choice and challenge questions: A security and usability assessment. In: SOUPS 09: Proceedings of the Fifth Symposium on Usable Privacy and Security. ACM, New York (2009)

15. Kidner, S.: Clause for concern: most people baffled by online t&cs. Which? (July 2012), http://conversation.which.co.uk/technology/online-privacy-policy-terms-and-conditions-confusion-investigation
16. Kupper, A.: Location-Based Services: Fundamentals and Operation. John Wiley & Sons, Ltd (2005)
17. Masnick, M.: Web privacy policies confuse net surfers (June 2003), http://www.techdirt.com/articles/20030625/0158245.shtml
18. Nasirifar, P., Hausenblas, M., Decker, S.: Privacy concerns of FOAF-based linked data. In: Trust and Privacy on the Social and Semantic Web Workshop (SPOT 09) at ESWC09. Heraklion, Greece (2009)
19. Ochieng, W.Y., Quddus, M.A., Noland, R.B.: Map-matching in complex urban road networks. Brazilian Journal of Cartography 55(2), 1–18 (2004)
20. Ohm, P.: Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review 57, 1701 (2010)
21. Out-Law.com: Regulators demand clearer privacy policy (Feburary 2009), http://www.out-law.com/page-9795
22. Quddus, M.A., Noland, R.B., Ochieng, W.Y.: A high accuracy fuzzy logic based map matching algorithm for road transport. Journal of Intelligent Transportation Systems: Technology, Planning, and Operations 10(3), 103–115 (2006), http://dx.doi.org/10.1080/15472450600793560
23. Rabkin, A.: Personal knowledge questions for fallback authentication: security questions in the era of facebook. In: Proceedings of the 4th symposium on Usable privacy and security. pp. 13–23. SOUPS '08, ACM, New York, NY, USA (2008), http://doi.acm.org/10.1145/1408664.1408667
24. Schechter, S., Brush, A.J.B., Egelman, S.: It's no secret. measuring the security and reliability of authentication via 'secret'; questions. In: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy. pp. 375–390. SP '09, IEEE Computer Society, Washington, DC, USA (2009), http://dx.doi.org/10.1109/SP.2009.11
25. Schechter, S., Reeder, R.W.: 1 + 1 = you: measuring the comprehensibility of metaphors for configuring backup authentication. In: Proceedings of the 5th Symposium on Usable Privacy and Security. pp. 9:1–9:31. SOUPS '09, ACM, New York, NY, USA (2009), http://doi.acm.org/10.1145/1572532.1572544
26. Scoville, G.: Good security questions. http://www.goodsecurityquestions.com (2012)
27. Shvaiko, P., Euzenat, J.: Ontology matching: State of the art and future challenges. IEEE Transactions on Knowledge and Data Engineering 25(1), 158–176 (2013)
28. Velaga, N.R., Nelson, J.D., Sripada, E., Edwards, P., Corsar, D., Sharma, N., Beecroft, M.: Development of a map-matching algorithm for rural passenger information systems via mobile phones and crowd-sourcing. In: Proceedings of the 91st annual meeting of the transportation research board (2012)
29. Villata, S., Delaforge, N., Gandon, F., Gyrard, A.: An access control model for linked data. In: Meersman, R., Dillon, T., Herrero, P. (eds.) On the Move to Meaningful Internet Systems: OTM 2011 Workshops, Lecture Notes in Computer Science, vol. 7046, pp. 454–463. Springer Berlin Heidelberg (2011), http://dx.doi.org/10.1007/978-3-642-25126-9_57