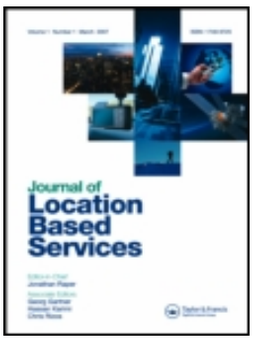

Journal of Location Based Services

ISSN: 1748-9725 (Print) 1748-9733 (Online) Journal homepage: https://www.tandfonline.com/loi/tlbs20

Special issue on privacy aware and location-based mobile services

Matt Duckham , Mohamed Mokbel & Silvia Nittel

To cite this article: Matt Duckham , Mohamed Mokbel & Silvia Nittel (2007) Special issue on privacy aware and location-based mobile services, Journal of Location Based Services, 1:3, 161-164, DOI: 10.1080/17489720802089489

To link to this article: https://doi.org/10.1080/17489720802089489

Published online: 24 Apr 2008.

Journal of Location Based Services
Vol. 1, No. 3, September 2007, 161–164

Taylor & Francis
Taylor & Francis Group

EDITORIAL

Special issue on privacy aware and location-based mobile services

Location-aware computing provides the ability to continuously monitor, communicate, and process information about an individual's location with a high degree of spatial and temporal precision and accuracy. The benefits to individuals and society of location-based services (LBS), which rely on location-aware computing, are potentially enormous. An ever-broadening range of LBS applications, from personal navigation to emergency response, m-commerce to elder care, are being proposed, developed, and deployed. Although LBS remains a relatively small market today (estimated US$200 million worldwide market for wireless LBS in 2007), recent industry trends seem to indicate that LBS are at last transitioning into a mature technology (as evidenced by Nokia's stated objective of ubiquitous GPS-enabled phones and recent US$8 billion acquisition of Navteq).

Many researchers in the area of LBS, however, argue that location-privacy jeopardises all that. Our precise location uniquely identifies us, potentially more so than our name, address, or even our genetic profile. Failure to protect a user's location privacy has been associated with undesirable consequences in at least three distinct areas (Clarke 1999, Kaasinen 2003, Duckham and Kulik 2006, Raper *et al.* 2007). First, unscrupulous businesses may bombard a person with unsolicited marketing for products or services related to that person's location (termed location-based "spam"). Many of us may already be somewhat familiar with this phenomenon, for example with bluecasting (unsolicited proximity-based advertisements beamed to Bluetooth-enabled mobile devices) becoming increasingly common in bars, near billboards, and in other public spaces. Second, location is inextricably linked to personal well-being and safety. Failing to protect location privacy can potentially result in harmful activities, such as stalking or assault. Third, knowledge about location can be used to infer other personal information about an individual, such as a person's political views, state of health, or personal preferences.

Breaches of location privacy are already beginning to result in lengthy and complex legal cases (for example, in the US (Chicago Tribune 2001) and Korea (Lee 2005)) and are arguably a barrier to the development of new and critical location-based services (Muntz *et al.* 2003). For LBS, location privacy is the "elephant in the room".

Against this background, interest and research into location privacy has been growing rapidly over the past five years. In an attempt to capture some of this growing interest in the topic, the First International Workshop on Privacy-Aware Location-based Mobile Services (PALMS 2007) was held in conjunction with the 8th International Conference on Mobile Data Management (MDM 2007) in Mannheim, Germany, May 11, 2007. The workshop included presentations of 11 fully peer-reviewed short papers, as well as a keynote from Alistair Beresford, University of Cambridge, UK. The authors of accepted papers, published in IEEE MDM 2007 proceedings (Mokbel *et al.* 2006), include leading

ISSN 1748–9725 print/ISSN 1748–9733 online

DOI: 10.1080/17489720802089489
http://www.informaworld.com

researchers in the field from nine different countries in Europe, Asia, and North America. The papers in the proceedings cover a wide range of topics including social studies, query processing for private data, privacy-preserving query processing, anonymisation techniques, and RFID environments.

This special issue presents three extensively revised and extended versions of papers in the PALMS 2007 proceedings that adroitly illustrate three fundamental features of the emerging body of research into location privacy and location privacy protection. Taken together, the papers highlight the need to be able to 1) integrate a *range* of approaches for location privacy protection; 2) understand both strategies for privacy protection and *counter-strategies* for invasions location privacy; and 3) achieve a *balance* between location privacy and quality of location-based service.

First, a coherent strategy for location privacy protection relies on a wide range of tools, techniques, and approaches to location privacy. Location privacy is a complex issue with social and technical implications. Traditional regulatory approaches to privacy protection, such as legislation, cannot on their own hope to provide complete privacy protection in new location-aware computing environments. Regulation can only hope to *punish* breaches of privacy, and although acting as a deterrent, can never *prevent* these breaches. Conversely, new technical approaches can potentially prevent breaches within certain domains, but are only sensible in the context of broader regulatory agreement on the principles of privacy protection. In short, there can be no ''silver bullet'': we require a combination of different regulatory frameworks and technical solutions for location privacy protection.

Second, information is only worth protecting if it is also worth attacking. Thus, a prerequisite for understanding strategies for location privacy protection is an understanding of strategies for attacks on location privacy. The situation is analogous to that in cryptography: any advances by code-breakers are ineluctably matched by subsequent advances by code-makers. Despite an inevitable ''arms-race'' of strategies and counter-strategies for location privacy, progress can be made. The struggle for a balance between imperfect privacy protection and invasion has important social benefits in generating greater understanding of the fundamental limits on location privacy. Indeed, the entire question of privacy ''protection'' can be viewed from the opposite perspective of a legitimate security organisation that needs to track individuals attempting to hide their location. In such cases, invasion of privacy is presumably in the broader interests of society, and those who wish to protect information about their location are in a sense the ''attackers.'' Research into location privacy must account for both perspectives, and acknowledge the inextricable relationship between privacy protection and privacy attacks.

Third, an individual's desire for location privacy protection will often be affected by the benefits to that individual of an LBS. Unlike some other forms of privacy, location privacy typically exhibits a sliding scale of privacy protection, where hard boundaries between what is private and what is not are difficult to draw. Many of us are already comfortable with the principle of relaxing privacy constraints in certain specific situations, such as where it might aid the emergency services (for example, as provided for by the US FCC E911 rules). Several studies have shown that there can exist a balance between level of privacy and level of service, with higher levels of privacy usually associated with lower levels or quality of service (e.g., Duckham and Kulik 2006, Mokbel *et al.* 2006).

Deciding where exactly to draw the line between level of privacy and level of service is expected to vary based on the individual and their specific context. Some ''hard'' lines can be drawn using legislation and regulation, but beyond that our systems for privacy protection need to enable LBS users to adapt the levels of privacy to the quality of service the user wishes to receive.

The paper in this special issue by van Loenen and Zevenbergen strongly illustrates the first of these fundamental issues, that location privacy has both technical and social aspects. The paper examines the question of whether privacy legislation in Europe, and specifically the Dutch legal framework, threatens the development of new location-based services and technology. The paper argues that LBS has ''little to fear'' from current privacy law and concludes that location privacy in Europe strikes a reasonable balance between the needs of individuals, LBS providers, and national security organisations.

The paper by Mascetti *et al*. focuses primarily on the second of these fundamental issues: that privacy research must address both strategies and counter strategies for location privacy. A range of previous research on location privacy has addressed the issue of adapting the level of spatial detail in location information in order to protect an individual's location privacy (termed *spatial generalisation* by Mascetti *et al*., but also variously termed in the literature ''spatial cloaking'' (Gruteser and Grunwald 2003), ''obfuscation'' (Duckham and Kulik 2005), the ''need-to-know principle'' (Hutter *et al*. 2004), and the ''principle of minimal asymmetry'' (Jiang *et al*. 2002)). Mascetti *et al*. construct a formal model that underpins much of this previous work, providing a framework for reasoning about and comparing different spatial generalisation algorithms.

Lastly, Langheinrich describes the development of FragDB: a system for controlling access to stored information based on an individual's location. Rather than accessing information based on *who* you are (e.g., using secret passwords) Langheinrich presents a mechanism of information access based on *where* you are. As such, the system is closely related to the third fundamental issue identified above: that there exists a balance between the level of location privacy and the level of services an individual may wish to receive. Langheinrich argues strongly that his vision of a radically different form of access to digital information has important advantages, in particular simplifying the infrastructure and access rules required to protect many types of sensitive information. However, in order to access this new level of service, the individual must necessarily reveal some information about their location. Privacy protection is built in to the FragDB system at the most fundamental levels, but as a basic principle, users must accept some loss of location privacy if they wish to access the wide range of new and beneficial services that can be provided based on location information.

As the papers in this special issue show, location privacy is establishing itself as an active topic for innovative research in the area of LBS. The key features of location privacy research are to integrate social and technical issues, using strong theoretical underpinnings, to develop a broad range of new location-based applications.

Before presenting the three special issue papers themselves, it only remains for us to extend our sincere thanks to all the special issue reviewers, who contributed timely and thorough reviews; to the journal staff and Editor-in-Chief Jonathan Raper for their support and input; and especially to all the authors who submitted papers to the

special issue, providing the raw materials for this snapshot of the very latest ideas in the area of privacy aware and location-based mobile services.

Matt Duckham
University of Melbourne
Australia
Email: matt@duckham.org

Mohamed Mokbel
University of Minnesota
USA
Email: mokbel@cs.umn.edu

Silvia Nittel
University of Maine
USA
Email: nittel@spatial.maine.edu

References

Chicago Tribune, 2001. Rental firm uses GPS in speeding fine. July 2nd, p. 9. Chicago, IL: Associated Press, 2001.

Clarke, R., 1999. Person-location and person-tracking: technologies, risks and policy implications. *In*: *Proc. 21st International Conference on Privacy and Personal Data Protection*, 206–231, Hong Kong.

Duckham, M., and Kulik, L., 2005. A formal model of obfuscation and negotiation for location privacy. *In*: H.W. Gellersen, R. Want, and A. Schmidt, eds. *Pervasive 2005*, volume 3468 of *Lecture Notes in Computer Science*. Berlin: Springer, 152–170.

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

Gruteser, M., and Grunwald, D., 2003. Anonymous usage of location-based services through spatial and temporal cloaking. *In*: *Proc. MobiSys '03I*, 31–42.

Hutter, D., Stephan, W., and Ullmann, M., 2004. Security and privacy in pervasive computing: State of the art and future directions. *In*: D. Hutter, G. Miiller, and W. Stephan, eds, *Security in Pervasive Computing*, volume 2802 of *Lecture Notes in Computer Science*. Springer, 284–289.

Jiang, X., Hong, J.I., and Landay, J.A., 2002. Approximate information flows: socially-based modeling of privacy in ubiquitous computing. *In*: G. Borriello and L. E. Holmquist, eds, *Proc. 4th International Conference on Ubiquitous Computing*, volume 2498 of *Lecture Notes in Computer Science*. Berlin: Springer, 176–193.

Kaasinen, E., 2003. User needs for location-aware mobile services. *Personal and Ubiquitous Computing*.

Lee, J.-W., 16 November 2004. Location-tracing sparks privacy concerns. Korea Times. Available from: http://times.hankooki.com [Accessed 26 July 2005].

Mokbel, M., Duckham, M., and Nittel, S., Eds, 2007. Proceedings International Workshop on Privacy Aware and Location-Based Services (PALMS'07). *In*: *Proceedings Mobile Data Management 2007 (MDM'07)*. IEEE, 232–287.

Mokbel, M.F., Chow, C.-Y., and Aref, W.G., 2006. The new Casper: query processing for location services without compromising privacy. *In*: *Proc. of the 32nd International Conference on Very Large Data Bases (VLDB)*, 763–774.

Muntz, R.R., Barclay, T., Dozier, J., Faloutsos, C., Maceachren, A.M., Martin, J.L., Pancake, C.M., and Satyanarayanan, M., 2003. *IT Roadmap to a Geospa-tial Future*. Washington, DC: The National Academies Press.

Raper, J., Gartner, G., Karimi, H., and Rizos C., 2007. A critical evaluation of location based services and their potential. *International Journal of Geographic Information Science*, 1 (1), 5–46.