Location privacy in web-based LBS
Position paper

Maria Luisa Damiani [1] and Pierluigi Perri[2]

[1] Dept. Informatics and Communication, University of Milan (I)
[2] School of Law, University of Milan(I)

1 Motivation and background

MODAP (Mobility, Data Mining and Privacy, 2009-2012) is a project funded by the European Commission to promote awareness of the privacy issues in mobility data collection and data mining (http://www.modap.org). The project consortium consists of 11 institutions from various European countries, for the major part universities. The University of Milan is one of the members of the project. Within our research, mainly focused on privacy-enhanced technologies [1, 3], we are experiencing interdisciplinary collaboration between jurists and researchers on the issue of location privacy in web-based location-based services (LBS)[2]. We call web-based LBSs those applications in which users can request a LBS through a geo-enabled browser compliant with the W3C geolocation API specification. Accordingly, the user visiting a geo-enabled website is prompt with the question on whether he/she gives consent to the disclosure of the location to the website owner. In our research, we are concerned with the analysis of the privacy risks emerging in this scenario and with the problem of how to enhance user's awareness for a more responsible user's participation. In this position paper we want to contribute to the discussion with some considerations.

2 Enhancing users' awareness

2.1 Who is tracking me?

Users are not fully aware of all parties, or Data Controllers in a privacy-oriented taxonomy, which track their position. For example the users accessing the Foursquare website through the Firefox browser deliberately decide to share their position with the members of the geo-social network and thus also with the website owner. It is very likely however that inexperienced users are not aware of the fact that, in doing so, they disclose their position to some third party (i.e., the location provider) other than the website owner. In essence, the location provider which computes the position on behalf of the geo-enabled browser is transparent to the user. Indeed the user has only evidence of the fact that the position is tracked by the website owner, without knowledge of how many other subjects may be included in this tracking. This follows from the compliance of browsers with the W3C Geolocation specification. For the sake of transparency the user should get the full information when the yes/no consensus is requested.

2.2 Freedom of choice

Location providers have the ability to track users with great precision across different (geo-enabled) websites. Moreover, it can be shown that personal and sensitive information can be easily extracted from the collected location data, e.g. the home address [2] or the hospital in which the user is undergoing a medical visit.

Now consider an user willing to share his/her position with a trusted website, say the website of the ecologist organization the user belongs to, without letting the location provider know that he/she is at home or hospitalized. Note that this scenario is specular to the one commonly adopted by the research community working on privacy in LBS [4] in which the LBS provider is untrusted while the location source is trusted. Of course one could say that disclosing the position to the location provider is the prize that the user must pay to access the LBS. Indeed, this is only in part true, because users are not allowed to choose the location provider, based on personal preferences. The only way for the user to interact with a different location provider is to use a different browser or operating system and that of course is not an usable solution.

2.3 No invasive privacy

Users, even those who are sensible to privacy, might desire not to be bothered by privacy when they are working or doing something else. On the other hand, specifying privacy settings by clicking on a set check-boxes can be extremely boring. Moreover if this operation is to be repeated for every geo-enabled application, it takes time and is costly. In this view it might be useful some form of automation working across multiple applications. In the simplest case, it could be a sort of "red button" that the user may activate to immediately, and easily, stop tracking. A more sophisticated solution would be trying to minimize the interaction with the location provider, to limit the dissemination of location information [2].

3 Conclusion

In summary, web-based LBSs offer extraordinary opportunities to location and LBS providers to collect huge amount of position data in a simple way. This also raises challenging opportunities of research on privacy enhanced technologies. Therefore it is important to bring this scenario to the attention of researchers working in the area, because the level of awareness seems still limited. In this perspective, experiments with the users of web-based LBS can be of vital importance to gain insights into user's expectation on privacy.

References

1. M.L. Damiani, E. Bertino, and C. Silvestri. The PROBE Framework for the Personalized Cloaking of Private Locations. *Transactions on Data Privacy*, (3)2:123–148, 2010.

2. M.L. Damiani, P. Perri, and C. Yildizli. Third party positioning services: novel challenges in location privacy in LBS. Technical Report, March 2011. Universita degli Studi di Milano,TR38-11.
3. M.L. Damiani, C. Silvestri, and E. Bertino. Fine-grained cloaking of sensitive positions in location sharing applications. IEEE Pervasive Computing (accepted for publication, pre-print online).
4. M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *Proc. of the 1st International Conference on Mobile systems, Applications and Services.* ACM Press, 2003.