ABI research®

White Paper

Exploiting the Location Goldmine While Respecting Privacy

A Delicate Balance

Dominique Bonte
Practice Director, Navigation and Telecommunications

Since the very start of LBS, more than a decade ago, privacy has been one of users' major concerns and a major barrier for uptake. While location provides a very powerful instrument to develop compelling mobile applications, it also raises issues about the potential abuse of real-time or historical positioning data of specific users by companies, advertisers, governments, or indeed criminal organizations. The ambivalence between the power and privacy threat of location data can also be observed in the attitude of the end-users. While younger age groups do not seem to have a problem with exposing private information, including location on social networking sites – after all this is the very purpose of social networks – older age groups, that is the parents of the younger users, are much more reluctant, being more apprehensive about the risks involved.

Some of these attitudes are rooted in the older generation's instinctive fear of big brother, totalitarian societies that track the whereabouts of their citizens. At the same time many (younger) users are simply unaware – or worse, not interested – in protecting their privacy as they are completely absorbed in a culture of real-time, always on experiences characterized by the booming mobile social networking and reality TV shows with instant gratification as the new paradigm.

Governments and consumer organizations must raise overall awareness, promote best practices, and even enact legislation. In any case LBS vendors and ecosystem players must address this major inhibitor, and do it without killing the attractiveness of LBS services, in order to realize the promise of making LBS a mass market service.

1.1 LBS Categories and Privacy: An Overview

Not every LBS application suffers from the same privacy concerns. A big difference exists between push-based services such as tracking for which location history needs to be stored and pull-based services such as local search that involve a one-off operation.

- Navigation – While un-connected on-board navigation runs locally on handsets, off-board navigation such as Verizon Navigator, by its very nature, involves the exchange of GPS-data with a remote server.
- Real-time Tracking – The most obvious case of privacy concerns is the fear that unauthorized parties could get access to real-time tracking information, creating an immediate security risk. Examples of services include person-tracking and social-networking services offering friend-finder functionality. Ironically applications such as family trackers and teenage driver monitoring solutions are aimed at increasing safety and security, a clear example of privacy being subordinate to other prerogatives.
- Location-based Advertising – The fear of being spammed by advertising messages is real. Ironically, using location as an additional target parameter allows advertisers, at least in theory, to send fewer and more relevant commercial messages, benefiting both the end-user and the advertiser.
- Location-enabled Messaging –The integration of location into traditional mobile services such as texting and instant messaging is a major trend. ZOS Communications recently announced its location-based messaging platform for smartphones with Zing as the first location messaging service for consumers. This ad-hoc person-to-person location exchange raises fewer privacy concerns, though the information is available on the telecommunications network.
- Location-enabled browsing – Being defined by the W3C and trialed by Mozilla and Opera, these browsers will increase privacy concerns as location will be continually available without a need for installing individual applications. Location will become a transparent enabler invisible to the end-user and hence creating a huge privacy risk.

1.2 The Power of Location

The rewards for capturing and analyzing location data are huge. Several university projects have demonstrated that advanced location data mining algorithms can extract very accurate information such as purchasing behavior, even down to individual shop locations, information that is invaluable to advertisers. Location is clearly one of the most important parameters defining human behavior. Other examples include the use of GPS-probe data for the generation of real-time traffic information, road speed profiles, and even digital maps themselves.

For companies such as TomTom this represents a very important part of their business both in terms of enhancing their own product offers and as a service in its own right offered to other navigation vendors. As a consequence the stakes of taking control of location data are very high.

1.3 Approaches to Address or Alleviate Privacy Concerns

Many LBS vendors include settings and features in their applications in order to allow users to manage and control their privacy. Here again, a balance needs to be found between sufficient levels of privacy protection and the overall customer experience.

- Opt-in Procedure – General consensus exists about using opt-in procedures to seek approval from users to capture and use their positioning history. However, there is disagreement whether this should happen on a case by case basis or once and for all. While the first approach is not acceptable from a usability perspective, the second may lead to some customers no longer being aware about their location data being shared.

  Ideally regular opt-in reminders should be issued. Google Maps presents an opt-in screen the first time the application is launched following installation. However, the biggest issue with opt-in is the lack of information provided to the user about how often and for what purpose the location data will be used. In the case of Google Maps, users will not understand they are contributing to Google's efforts to build a reference database of Cell-IDs and Wi-Fi hotspots used as alternative positioning technologies to complement GPS for in-door coverage.
- Reduced Accuracy – A popular way to protect privacy is to share a "fuzzy" position instead of precise GPS coordinates. Inaccurate location sharing was and still often is the only possibility on non GPS-handsets. While alternative positioning technologies based on Cell-ID and Wi-Fi are becoming more widespread, they do not offer the same accuracy as GPS. However, reducing accuracy is also offered as a deliberate privacy protection measure on GPS-handsets, sharing neighborhood or city location attributes instead of precise coordinates. At the same time the reduction of the spatial – but also temporal – resolution of location information limits the usefulness of the analysis of historical location data.
- Limits in when, with whom, and where to share the location – A first range of settings allows limiting the visibility of the user's location to specified contacts. These settings should be as flexible and user-friendly as possible. In particular the user should be able to easily switch off any location sharing at any time.

  Similarly settings defining when and which locations are shared add to the overall feeling of the end-users of being in control. However, manual settings greatly deteriorate the user experience with many users forgetting to switch on and/or configure their applications on a continuous basis. Some LBS applications put full control in the hands of the end-user by only allowing manual position sharing: users decide when and where to share their location, either via address input or by clicking on their position on a map. This lowers the temporal resolution of location data.

  Nokia has attempted to combine privacy setting flexibility with ease of use by allowing users to share locations selectively, but automatically, based on matching current positions and predefined favorite places. Locations are only broadcast when users are at or near a publicly-defined and allowed place that does not require the user to take any action.

1.4 Personal versus Anonymous Location Data

Much of the debate on location privacy centers on the issue of personal versus anonymous data, the latter being much more acceptable from a user's point of view as it does not relate to specific, individual data. However, generalized data that is made anonymous by striping out identifiers such as ZIP codes and birth dates, can compromise the accuracy of data-mining algorithms. At the same time, discussions about the very definition and the effectiveness of this "anonimized" data continue unabated.

1.5 One-Time Use versus Long-Term Storage

A similar debate surrounds the time during which sensitive data are stored. In particular, data should only be stored as long as the user remains a customer and be destroyed when the service is canceled.

1.6 Privacy Control: Who's in Charge?

The most thorny privacy issue is related to who should control, manage, and be gatekeeper for sensitive user-location data. Until now, carriers were very much the only entity having access to largely network-based positioning data, but the increasing openness of the mobile and LBS environment have allowed new players to enter this area.

- Navigation Vendors – TomTom's MapShare community program is based on user feedback to keep digital maps up to date. Historic location data is logged on the navigation device and downloaded to TomTom servers whenever a PND is synchronized with a PC. The emergence of connected PNDs will allow this location data sharing to take place in real-time. In this case, the user benefits directly from the community effort.
- Carriers – Until recently, carriers controlled the whole LBS value chain. They were the only entity having access to the position of the user via control plane technologies and at the same time, only allowed hosted, carrier-branded third-party applications, blocking GPS functionality to all other applications.
- Handset Vendors – Some handset vendors such as Nokia are gradually taking over the role of carriers in the LBS value chain by providing their own A-GPS service on SUPL-compatible handsets. As such Nokia acts as the gatekeeper of the users' privacy. The recent announcement to open up access to Nokia Maps to third-party developers makes this role even more important. Nokia uses location data to establish reference databases of cell-IDs and Wi-Fi hotspots in order to offer alternative positioning capabilities in indoor environments to their end-users.
- Location Aggregators – In an attempt to open up their location assets and generate additional revenue, North American carriers such as Sprint are starting to partner with location aggregators such as uLocate, Wavemarket, and Loc-Aid, through whom third-party developers obtain access to location data. In many cases the aggregator takes over the carriers' privacy gatekeeper role.
- Third-party Developers – The arrival of the SUPL standards has made installing any third-party LBS application on any GPS-smartphone possible. Importantly, it is now up to the user to protect his own privacy by checking the trustworthiness of the developer before deciding to opt-in. The user is the gatekeeper of his own privacy by controlling which applications to install.
- Internet Companies – The arrival of geo-enabled mobile web-browsers and LBS applications puts privacy control squarely in the hands of internet companies such as Google, which offers applications such as Google Maps including local search and the Latitude friend finder and social networking solution. Google Search with My Location was recently made available on iPhone's Safari browser, subject to the user opting in.

  Interestingly, two separate opt-ins are requested, one for Safari and one for Google. As positioning will become available ubiquitously and transparently via the browser, location privacy enters the complex arena of internet security, and becomes the subject of initiatives launched by both the W3C and IETF organizations.

1.7 Location Data in Return for Rewards?

Users of mobile services are increasingly becoming aware of the value their location data represents to LBS vendors.

In the advertising space, users have come to expect something in return when accepting to receive advertising messages on their phones. Both in Europe and the United States, Locationet is already offering a free navigation service subsidized by advertising. While for the time being it might be difficult for many vendors to have the cost of their services fully covered by advertising, they should at least offer discounts to users who opt-in for advertising.

Similarly the “free services in return for access to location history” paradigm will start to gain momentum. This is particularly true for applications such as TomTom MapShare where location data are used to improve the quality of the service. The same holds for Google and Nokia, who use location data to build reference databases of base station Cell-IDs and Wi-Fi hotspots.

There is something fundamentally unfair about letting users pay the full price for information they have helped to collect. Players in the location ecosystem will have to realize the location goldmine comes at a price.

1.8 Standardization and Legislation

As control over location data is being acquired by an ever larger number of companies, transparent standards and effective legislation becomes a necessity. Both the W3C and the IETF have launched working groups to address location privacy issues. W3C’s Geolocation API Specification covers security and privacy considerations defining permission user interfaces, trust relationships, and permission revoke functionality when browsing to a different URL. IETF’s GEOPRIV Working Group has been created to specify a suite of protocols for the representation and transmission of location data as wells as user policies.

Governments are also getting involved. They are increasingly worried about their own privacy with national security concerns forcing countries such as China to strictly regulate the digital map industry. Google’s Street View has also come under the scrutiny of many nations. However, most attention goes to protecting the privacy of LBS users. Ironically governments have infringed on users’ privacy many times in history – a powerful lesson not to trust anybody as far as privacy is concerned.

Facebook, the high-profile social site, is currently facing heavy criticism. Most recently the Canadian government accused it for failing to delete personal information of users who cancelled their accounts (illegal according to Canadian law) as well as not communicating privacy functionality clearly. In another case Facebook came under fire for planning to launch generic privacy settings that would be valid across all features, reducing configuration complexity, but also tempting some users to share too much information. Obviously, with 250 million users, Facebook has a lot to loose if it becomes subject to stringent privacy regulation. Fortunately many governments understand that regulation should respect a user’s desire to freely share personal information. Many social sites planning to geo-enable their solutions will have to face the even stricter location data privacy regulations.

1.9 Recommendation for LBS service providers

LBS providers must address location data privacy concerns proactively. At the launch of Latitude, Google has gone to great lengths to alleviate any privacy concerns by ensuring location data are not saved. Unfortunately the company has been less proactive with respect to Street View, being forced many times to make faces, buildings, or sites invisible at the request of governments. Companies must not only stress that location data are only used in an anonymous, statistical way, but also demonstrate that individual data are neither used nor stored. Obviously all companies state that they do not provide access to third parties, but companies should communicate more clearly exactly *what* they do with the data. If not, they'll get into even more trouble and incur further damage to their images.

1.10 Conclusions

While privacy is a major issue that needs to be addressed by the location industry, it should not lead to over regulation, reducing functionality and slowing down the uptake of LBS services. Consumer organizations and governments alike need to be aware that overly protecting consumers will also deprive them from using life-enhancing location services. Standardization as well as transparent and clear legislation will be key components in achieving the balance between protecting individuals and allowing the location industry to reach its full potential. Person trackers and advertising are two examples in which added-value is clearly provided to the end-user for the enhancement of safety and more relevant commercial information (respectively). While privacy concerns are legitimate, they should never become a barrier for the uptake of LBS. However, end-users should always remain the gatekeepers and should be rewarded for the location information they make available.

Published 3Q 2009

©2009 ABI Research
PO Box 452
249 South Street
Oyster Bay, NY 11771 USA
Tel: +1 516-624-2500
Fax: +1 516-624-2501
http://www.abiresearch.com/analystinquiry.jsp