#hylo – Privacy Preserving Geosocial Network for Sharing Hyperlocal Information on a Map

Mikko Rönneberg, Hanna-Marika Halkosaari, Mari Laakso, Eero Hietanen, José Vallet, Pyry Kettunen, Tapani Sarjakoski
Finnish Geospatial Research Institute
Masala, Finland
firstname.lastname@nls.fi

Abstract

This paper describes the early development of #hylo – a privacy preserving geosocial network for sharing hyperlocal information on a map. #hylo demonstrates how to ensure users identity and location privacy in a geosocial network. Via the #hylo mobile map application users share public hyperlocal information and are able to manage their location and interest information. Being a geosocial network #hylo gathers both public and personal data, while the user is able to determine the privacy level and is in control of their personal data. With these 'privacy by design' elements supported by the MyGeoTrust platform, #hylo encourages users to share information. #hylo strives to increase awareness and personal attachment of people to their local surroundings.
Keywords: privacy, geosocial, hyperlocal, map, mobile application

1 Introduction

Privacy is becoming more relevant to everyday life as mobile technology advances, thus tools for controlling ones private data should be improved. Mobile operating systems for example have users accept license agreements that let systems to share the location information of the user to whom they choose [6]. The location information of users can be for instance used to obtain popular meeting locations accurately [7]. Therefore, it's no wonder why users for the most part want to have more control over their data. A user study participant expressed something most would agree on: "I would like to make my location information private, seen only by myself and by the people I choose." [1] Users have a need to improve their knowledge of, access to and visibility of their data sets but more importantly users need means to control and manage their location data [1]. It is currently difficult to fulfil the last need, since a person can have many devices and services that collect and store location information. Trying to improve the knowledge of people about data collected from them is also challenging since most users never fully even read the license agreements [2]. There are already many solutions that enhance the privacy in geosocial networks [8, 9], but users still lack control over their own data.

This all raises questions about privacy in today's network environments that almost everyone are a part of. One such question is how to ensure users identity and location privacy in a geosocial network where users share hyperlocal information? This paper answers the question by presenting #hylo – a privacy preserving geosocial network for sharing hyperlocal information on a map. A geosocial network is defined as a social network where geographic services and capabilities are used to enable additional social dynamics [11]. Another a more detailed definition of a geosocial network is as follows: "*a web-based or mobile-based service that allow users to (1) construct a profile containing some of their geolocated data (along with additional information), (2) connect with other users of the system to share their geolocated data and (3) interact with the content provided by other users (for instance by commenting, replying or rating)*" [4]. The data shared in #hylo is designed to be hyperlocal, defined as information relevant to small communities or neighbourhoods [5]. The importance of geosocial networks have been identified already before the mobile technology was available and widespread [3].

2 Description of #hylo

#hylo strives to increase awareness and personal attachment of people to their local surroundings. The idea is to help people who want to join others in doing something they are interested in and form a better understanding of their local surroundings. We actually want people to "go out there", instead of just sharing information at the comfort of their home. A typical #hylo user could be someone who just moved to a new area or someone who is simply interested in learning more about what is happening in their surroundings.

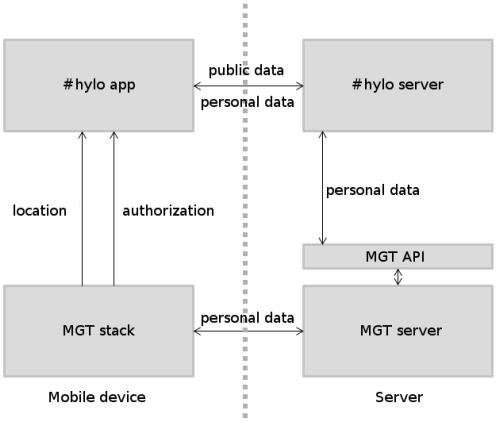
2.1 #hylo and MyGeoTrust

#hylo is part of MyGeoTrust [6] project that focuses on the user privacy of location information. The vision of MyGeoTrust is to create an alternative location platform for mobile users, which allows users to enjoy the benefits of location technologies without sacrificing their privacy [6]. The user can choose between several privacy modes all the way from stealth to public contributor for any given situation. If the user for example enables stealth mode while on their way home, the users location data is not stored anywhere. On the other hand settings can be adjusted to allow third-parties to gain access to the location data of the user, but only in anonymous or aggregated-form. Basically the user identity is always separated from the location data for third-party access. Third-party is here assumed to be some other entity than the user themselves or the organization operating the MyGeoTrust

server. MyGeoTrust also allows the user to control their data by for example deleting it or by disallowing data transfer.

MyGeoTrust (referenced from here after as MGT) platform is used in #hylo for preserving the privacy of the user, as depicted in figure 1. On the mobile device side, the user has MGT stack and #hylo mobile application (referenced from here after as #hylo app) installed. MGT stack handles the location data and also provides the location information for #hylo app. MGT stack also provides user authentication and authorization in #hylo app. MGT stack sends the location information of the user to the MGT server according to the selected privacy mode. On the server side, #hylo server stores and transfers all the public data used in #hylo app. Personal data from the #hylo app is passed on to the MGT server via the MGT API. Personal data requests are also done through the API.

Figure 1: #hylo mobile device and server interactions.



2.2 #hylo mobile application

#hylo app is a map based interface designed for gathering, sharing and viewing the #hylo data. It has the following main functionalies: a map and a feed for browsing content, view for sharing content and a search that displays an interest heat map. Messages placed on the map by the #hylo users are called *geonotes*, see figure 2. Geonotes can be questions, events, announcements etc. The map serves as a combination of a feed and a search, features that are found in other social network applications as in form of lists. The geonotes on the map are by default filtered according to the users own interests. For example someone who has added "#swimming" into their interests will see geonotes related to "#swimming". The geonote feed functions as in other social network applications in listing recent posts, but it also takes the user location into consideration showing nearby geonotes. Both the map and the feed can be filtered by own places, own current location, geonote category, most interesting, most replied to, a search query and so forth.

When geonotes are added #hylo app performs a look up [10] on the suburb and neighborhood names and suggests them as the hashtags of the geonote. This helps users interested in the area to see the geonotes which are shared there. When there are large amounts of geonotes on the mapview they are clustered and filtered by a time frame to avoid clutter. The user can customize the time frame. Other fore mentioned filters can be selected by the user to further filter the data.

The interest heatmap works by querying for example "#music" that will show hot spots of places on the map where users with the interest in #music have been to. The more users have been to a place with the interest music, the more that place will stand out in the data. Individual location tracks or interests cannot be obtained through the heat map. Either the heat map contains enough data to be anonymous or no results are shown. However, geonotes searched by the user will always be shown. Combining the geonotes and the interest heatmap on the map will provide the user a valuable geographic representation of the search term they used. The user can also view the search results as a feed and filter it accordingly.

Figure 2: Geonotes on the map view of #hylo app

Currently #hylo mobile application is in closed alpha testing stage and has limited features. By open beta stage the features presented in this paper are to be tested with real users. Also the interest heatmap functionality is in concept phase, since we lack the data and application functionality to gather and present them.

3 Privacy by design in #hylo

The #hylo data is divided into public and personal data. The public part of the #hylo data is answering the question: "Where is something happening?" In addition to the public hyperlocal information, #hylo also collects personal information in the form of location tracks and interests from the users. This data will allow #hylo to provide anonymous and aggregated data for the #hylo users to enhance the user experience. Aggregated data also provides valuable information to third-parties such as the public agencies and private companies. The #hylo data accumulation can be seen as a loop, where the personal data gathered from the users is transformed into public data and given back to all the users in

a form where individual users cannot be identified. The personal data is answering for example to the question: "Where users interested in football are gathering?" MyGeoTrust platform gives the user complete control over their location information and interests. The user decides whether their information is shared and who has access to it. The desired benefit of privacy by design in #hylo is that users would be more willing to share their data when they know that they control it and their anonymity is secured.

As a #hylo is a location aware application, most of the users' actions can be attached to a location. Questions such as where a user made an action are easy to answer by looking at their data. As a general principle, whenever data is stored to MGT server it is considered to be personal. #hylo server on the other hand stores both personal and all the public data (geonotes). Personal data on the #hylo server is considered to be something that only the users themselves should have access to. Examples of these are user profile details and logs of user actions when for instance a user flags a geonote as inappropriate. #hylo data accumulates in a loop where the personal data gathered from the users is transformed into public data and given back to all the users in a form in which individual users cannot be identified. It is important to distinguish public from personal data, examples of which are given in table 1.

Table 1: Examples of public and personal data in #hylo

#hylo data examples	**Privacy**
contents of a geonote	public
list of most interesting geonotes	public
list of geonotes by a user	personal
interest list of user	personal
location track of user	personal
interest heatmaps	public
user profile details (e.g. email)	personal
user actions (e.g. flagging a geonote)	personal
searches made by user	personal

The public data is visible to all #hylo users and consists of geonotes and heatmaps. Attributes of a geonote currently contain following elements: title, description, hashtags, username, time of post and theme (question, event, announcement etc.). The location of the geonote is chosen by the user and is not necessarily the location the user is sharing the geonote from. Geonote comments, number of marked as interesting and number of flagged as inappropriate by other users are considered public data and shown with the geonote.

Users' location data is personal information and will also very quickly begin to follow a pattern, where the users' home and other places of frequent visit become apparent. Combining this information with the interests of users makes the data even more personal. The personal data consists for example of location data and interests. Location data consists of tracks and points whereas the interests are stored as hashtags entered by the user in various circumstances. These circumstances include adding a new interest and using search in the #hylo app. Location information is stored according to the privacy mode selected by the user. A simple example of the personal data would be as follows. Let's say a user is interested in football and regularly plays with their friends in a nearby football field and they all use #hylo that tracks their location and interests. One location track of a player with an attached interest of #football is personal even when the user cannot be identified, because this track displays where the user came from and went to in addition to the time spent playing. All location information and interests collected from these players is considered personal. Another example of personal data is where the user was when they performed a search. This information may not be that interesting when looking at a single search location, but can provide interesting results when applied to large amounts of search queries. A data set of what geonotes a user has marked interesting or replied to is personal data and useful to the user themselves, but if aggregated also useful for the #hylo community or third-parties. Similarly, the most used hashtags by a user can be considered personal data.

Heatmaps in the #hylo app are created using aggregated anonymous user location tracks and the user interests related to them. This data originates from personal data collected from the users. In our previous example of the football players, their data would show a correlation between the interest #football and the football field they regularly play at, if the volume of data allows it to be displayed without compromising their privacy. This data is presented as an interest heatmap generated according to the search terms provided by the user. A user who wants to play football can search for #football in #hylo app and will likely find a hot spot around the football field area in the heatmap.

Privacy has been one of the main focuses when developing #hylo. Similarly to the MyGeoTrust, #hylo has adopted the *privacy by design* thinking. In addition to the examples given in this paper before, usernames are by default generated automatically and cannot be searched for in the application. User can also type in their username if they so choose. User avatars, small images displayed next to the username, cannot be chosen by the user in order to maintain privacy. Avatars are though part of the gamification aspects of #hylo, designed to promote interesting content. Users who have shared a lot of interesting geonotes acquire new predefined avatars according to a leveling system familiar in other games. This way a quality content provider will be more distinguishable by other users.

4 Future Work

As the #hylo mobile application is in its early phase and only limited user tests have been conducted mainly as a proof of concept. One of the requirements for having an open beta for the #hylo app is to complete the MyGeoTrust integration that also allows for gathering personal location data. Through the personal data, MyGeoTrust will enable us to create the interest heatmap visualizations. However, this requires that an initial data set is gathered from the beta users. The idea of the open beta is to let one beta user group use the #hylo application freely while monitoring the produced content and gathering feedback. Other smaller beta user groups will use the app in a more controlled setting with predefined tasks. The aim of both is to find out if #hylo increases awareness and personal attachment of people to their local surroundings.

5 Conclusions

This paper introduced the early development of #hylo which is a geosocial network for securely sharing hyperlocal information on a map. To conclude, it is possible to give the user more control over the information they share and also collect data that can be used to enhance the user experience and offer interesting but privacy-aware data to third-parties.

6 Acknowledgements

Support for this research was provided by Tekes, the Finnish Funding Agency for Innovation through a strategic research grant for the MyGeoTrust project. The authors thank Robert Guinness and the rest of the MyGeoTrust project team for providing valuable support for this paper.

References

[1] Alrayes, Fatma and Abdelmoty, Alia, No place to hide: a study of privacy concerns due to location sharing on geo-social networks. *International Journal On Advances in Security 7 (3/4)*, pp. 62-75, 2014

[2] Rainer Böhme, Stefan Köpsell, Trained to accept?: a field experiment on consent dialogs, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, April 10-15, 2010, Atlanta, Georgia, USA

[3] Espinoza, F., Persson, P., Sandin, A., Nystrom, H., Cacciatore, E. and Bylund, M. 'GeoNotes: social and navigational aspects of location-based information systems', *Proceedings of the 3rd International Conference on Ubiquitous Computing, Atlanta, Georgia, USA, pp.2–17.*, 2001

[4] Sébastien Gambs, Olivier Heen, Christophe Potin, A comparative privacy analysis of geosocial networks, *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, Chicago, Illinois, 2011

[5] Glaser, Mark, "Citizen Journalism: Widening World Views, Extending Democracy". *The Routledge Companion to News and Journalism, edited by Stuart Allan*. London and New York: Routledge, 2010

[6] Guinness, R.E., Kuusniemi, H., Vallet, J., Sarjakoski, T., Oksanen, J., Islam, M., Syeed, M., Halkosaari, H-M., Kettunen, P., Laakso, M., Rönneberg, M., 2015. "MyGeoTrust: A Platform for Trusted Crowdsourced Geospatial Data," Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, Florida, USA, pp. 2455-2469.

[7] Ankur Gupta, Sanil Paul, Quentin Jones, Cristian Borcea, Automatic identification of informal social groups and places for geo-social recommendations, *International Journal of Mobile Network Design and Innovation, v.2 n.3/4, p.159-171*, 2007

[8] Malina, L., Hajny, J., and Zeman, V., Light-weight group signatures with time-bound membership. *Security Comm. Networks*, 2015

[9] Amirreza Masoumzadeh and James Joshi, Anonymizing geo-social network datasets. *In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS (SPRINGL '11). ACM, New York, NY, USA, 25-32*, 2011

[10] Nominatim, OpenStreetMap Nominatim Wiki, Website: http://wiki.openstreetmap.org/wiki/Nominatim, 2016

[11] Tiwari, S., Kaushik, S., Jagwani, P., Tiwari, S., A Survey on LBS: System Architecture, Trends and Broad Research Areas. *Proc. 7th Int. Workshop on Databases in Networked Information Systems, p.223–241*, 2011