A privacy-aware model to process data from location-based social media

Marc Löchner
Technische Universität Dresden
marc.loechner@tu-dresden.de

Alexander Dunkel
Technische Universität Dresden
alexander.dunkel@tu-dresden.de

Dirk Burghardt
Technische Universität Dresden
dirk.burghardt@tu-dresden.de

***Abstract*—Many social media services offer their users to add location data to their posts. Since this data is usually publicly available, it can be used to create thematic maps based on the topical information, e.g. derived from hashtags attached to posts. However, users might not be aware, that their publications can be used for other purposes by third parties. In certain situations it can be compromising the user's privacy.**

We introduce a conceptual model to help people who create those maps to preserve privacy of social media users. Therefore we analyze the data in a set of four facets. For each facet, we eliminate precise data by deriving multiple abstraction layers from it. Using these layers, we are able to quantitatively describe different levels of privacy. We further describe an example application to show use cases for the abstraction model on the same data in two contrary scenarios.

***Index Terms*—privacy, social computing, geospatial analysis**

I. Introduction

Location-based social media (LBSM) enables the fast distribution of spatial information, knowledge or opinions that is generated within a defined or open community. This refers to data, that is published online by users in social networks, which feature location meta data with their posts. That data can be analyzed with various methods from text and data mining, machine learning, geo-visualization for applications such as disaster management, emergency response, urban planning, environmental management or the analysis of human activities and behavior in general. An overall future goal is to do this in real time.

It has shown that many users are not aware that their data is being analyzed by third parties [1]. Researchers, authorities, journalists or other players may use LBSM data to create maps for certain tasks such as gaining knowledge on collective behavior and trends (e.g. [2]). The information that is finally shown on the resulting map will generally be of aggregate character. Nonetheless, under certain circumstances, it might be possible to draw inferences about the source of the data and thus compromise the privacy of the user.

The creation of such maps therefore may be seen as facing opposing interests. On the one side are the cartographers, with the goal of presenting aggregate information sufficiently accurate for their individual purposes, may it be a proof for scientific theses, real time emergency information, or a report on the news. These goals may certainly counteract to the privacy needs of the user on the other side, the volunteering sources of the data.

Despite the potential awareness for privacy aspects, the complexity of this topic may prevent map creators to consider it. They face the problem to choose from one of two radical options to either use any provided data and ignore the user's privacy concerns or remove data and risk loss of important information in the resulting product, or find a compromising balance between interests.

In our research, we aim at developing methods that enable people who create of maps from LBSM data to process spatial information based on measurable privacy metrics [3]. This should help map creators to prevent the accidental disclosure of private information of social media users. The goal is to provide a generic systematical way of abstracting spatial, temporal, topical and social information from LBSM data, enabling map creators to seamlessly balance between private and public interests based on the specific circumstances and individual context of the map.

II. Related work

Dealing with privacy aspects requires to define the term. In a formal notion, we se *privacy* as an individual's freedom to either fully or partially *retreat* oneself from the public or disclose information about oneself in a self-controlled manner. However, there are always multiple forms of privacy definitions, as there are differences all the way from a personal to a cultural point of view [4].

Usually privacy is protected by laws, but must also be balanced with interests of the general public. There is a contrast between the *concept of privacy* and the *right to privacy* [5]. While the right to privacy follows a clear and distinct notion, the concept of privacy is much more vague and should be seen as a value.

Privacy is subject to sacrifices, either voluntarily in exchange for perceived benefits, or imposed by others either intentional or accidental. A person's privacy is closely related to its identity [5].

In geo-sciences, privacy must be seen in the context of spatial information. *Location privacy* describes the protection of the spatial information connected to a person at a certain time. Conflicts arise not least through the mode of data contribution. There is a notable difference between Volunteered Geographic information (VGI), where people choose actively to share

This work was supported by the German Research Foundation as part of the priority programme "Volunteered Geographic Information: Interpretation, Visualisation and Social Computing", SPP 1894, DE 735/11-1, www.vgiscience.org

information (opt-in) and Contributed Geographic Information (CGI), where their data is collected per default (opt-out) [6].

It has been shown how to draw inferences from spatiotemporal movement patterns, absence and presence, visiting frequencies, associations with places, commuting and co-location habits of friends, family and co-workers [7], without users opting in to such third party usage of the data. Combined with additional and possibly public information about locations (*location semantics*), spatial information can lead to predictions based on past data and other semantics [8]. Companies who built their business model around CGI, as well as government agencies, can predict activities of people already today [9].

The term *Geoslavery* [10] has been introduced to describe a dystopic but possible scenario in which a master controls the physical location of a slave, which can be achieved with technology that is available for more than a decade.

In order to prevent such dystopic scenarios, governmental action has been called for [11], but also the geo-community is demanded for social responsibility [10].

Several techniques to prevent this have been introduced, that are anonymity-based (*mixed zones*, *k-anonymity*), obfuscation-based (*imprecision*) or policy-based (*restriction*) [12].

Other approaches are shown, that hide locations by means of generalization [13], replacing exact positions in the trajectories by approximate positions, privacy-aware LBSM applications that require a trusted [14] or an untrusted [15] server.

In turn, it has been shown that the mere existence of detailed privacy settings in LBSM applications can mitigate privacy concerns among users [16]. Visual warnings increase awareness, higher awareness results in stricter settings, knowledge of spectators reduces concerns and real-time feedback for location requests results in more location request rejections [17]

The utilization of publicly available LBSM data can be regarded as an addition to gain information for the public good, if there is no other information available (e.g. sensor data). User studies in this area show the awareness of the legal situation in terms of privacy among end users of such data [18].

III. Concept

We present a conceptual model to help map creators to preserve privacy of social media users, when processing spatial information from their posted data. In the following subsections, we introduce the important parts of the model.

A. User

To define what is a user, we need to consider the focus on privacy. Within our research, we define that a person's privacy is compromised, if it is possible to derive to a real person from the map.

For a user, a suitable way to prevent this is to use a pseudonym as an identifier for their user account other than their real name [19]. But today, most users do not make use of pseudonyms but rather use their real name or at least attach it to the details of their account [20].

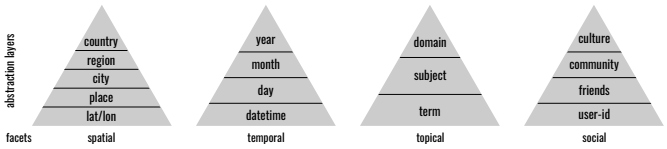

Fig. 1. Abstraction layers for each facet

If not being a corporate profile or a bot [21], a user account today may consist of a name, birth date, sex, contact information, etc. Any of this is personal data and must be treated as relevant in terms of privacy. Depending on how many details a real-world person provided with its user account, any of that information can be used to infer back to the real-world person [22].

This makes the identifier of a user in a certain social media service be a sufficient data record to link to a real-world person. So we consider a real-world person's privacy compromised, if the corresponding *user ID* is able to be determined.

B. Post

A post is defined as a data structure consisting of the following facets, that are relevant in terms of our analysis:

- *location* - spatial information, either a *lat/lon* object, an administrative unit or an arbitrary place
- *datetime* - temporal information, usually a *datetime* object
- *user-ID* - the username as the primary identification of a person (see previous subsection)
- *content* - usually arbitrary text, but also consists of *hashtags*, which act as informal taxonomy of the post

C. Abstraction layers

The here presented model was developed to improve privacy for social media users, in particular in the context of spatial applications. We eliminate precise data that could disclose users by deriving multiple abstraction layers of the LBSM data. Using these layers, we are able to quantitatively describe different levels of privacy.

The bottom layer is formed by the original data as read from the post. Each following layer represents an increase in privacy protection for the user. This way, a map creator has the ability to adjust the level of detail of the data in his output in a fine-grained and context-dependent way.

It should be noted, that abstraction layers do not only gain privacy for the social media users, but they also diminish the accuracy of the data. This makes applying abstraction to LBSM data be a compromise between privacy and accuracy.

The number of abstraction layers can be chosen arbitrarily, as granularity of the data can change. To demonstrate this, we show five layers in the location facet, four in the temporal, three in the topical and again four in the social facet, as shown in figure 1.

D. Facets

We can describe a post as an entity of social media data in four facets: *spatial*, *temporal*, *topical* and *social*. These facets

characterize the context of a post [23]. For each facet, the post data can be separated into a number of abstraction layers (see previous subsection).

1) Spatial: The spatial facet concerns the location data related to a post. The lowest abstraction layer is the plain *lat/lon* data, if provided in a post. All following abstraction layers are based on arbitrary user-generated *place* descriptions, as well as administrative units *city* and *country*, as provided by the social media services.

Some information on LBSM is not directly machine readable, such as user defined home locations on Flickr or Twitter, or post locations added by users on Instagram or Facebook. To systematically generalize such arbitrary place descriptions, where various *place* entities may actually refer to the same place, we aim to perform a best-match of the referenced locations to places explicitly contributed on OpenStreetMap [24]. Places which have no representation on OSM can be regarded of only private relevancy and can thus be omitted entirely or generalized up-hierarchy based on OSM information (e.g. city level).

2) Temporal: For the temporal facet we use the *datetime* data of a post as the lowest abstraction layer. Further layers may be the *day*, the *month* or the *year* of a post, as those distances imply to be suitable for the analysis of social media content [25].

3) Topical: To analyze the topical facet, we focus on hashtags given in a post. Every hashtag defines the lowest abstraction layer and is defined as *term*. A large percentage of user hashtags refer to only personally relevant aspects with few overlap of other user's terms [26]. Tags conforming with only a few users' posts can be seen as likelier to identify a single user as those used by many users. Therefore, the number of users using a certain tag overall can be seen as a systematic approach to generalization, e.g. by omitting tags used by few users first. To define additional abstraction layers, an approach is to use topic modeling technology [27]. Subsequent abstraction layers would be a *subject* and an even more generic *domain*.

4) Social: The social facet describes the user and his extended social network. The base layer is defined by the *user-ID*. As the next abstraction layer, we create a group of users called *friends*, where we add other user accounts connected to that user account, usually known as friends or followers. Using network analysis (see [28]) we define clusters to define a user's *community* as the third abstraction layer and further on a *culture* as the top-most layer.

IV. Application

The model of abstraction layers enables a certain quantification of privacy levels. A showcase application may advertise a user interface for map creators, who are to visualize specific spatial information derived from LBSM data. A mockup of such an application is shown in figure 2.

Besides a central canvas visualizing the LBSM data, the application user interface features a set of adjustment units, that correspond to the four facets. Each slider controls the abstraction layer of each facet and therefore the privacy level

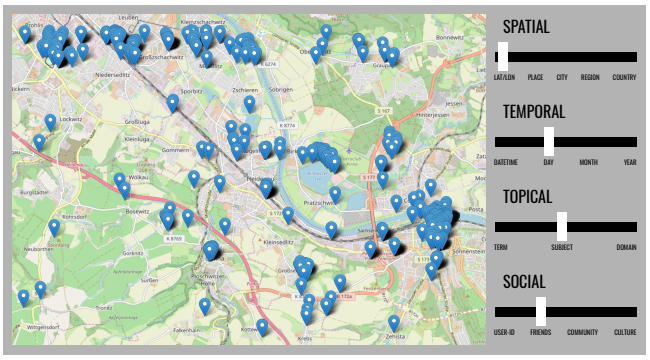

Fig. 2. Showcase application mockup

within that facet. The resulting abstracted data will then be visualized in the canvas.

Possible positions of the sliders vary depending on the number of abstraction layers. Also, the optimal slider positions differ depending on the data. In a situation, it is safe to push all sliders to the maximum data depth (base abstraction layer). In other situations the map creator is requested to to adjust settings, because there is only one hashtag used, that identifies a specific user account. This gives the map creator multi-dimensional abstraction options, which can preserve the privacy of social media users.

V. Case studies

Given real time data taken from social media services like Twitter or Flickr, we are able to create maps for very specific purposes. With every posting we have data about the user and his social network, the timestamp, the location data and hashtags, that define the topic of the posting. This information can be used to draw maps.

During a flood scenario in a large city, real time social media data can be used to draw maps, that show the current state of the flooding. Postings containing the hashtag `#flood` with the location data in the relevant area will be concerned.

We introduce two hypothetical use cases for users of a real time mapping application: both a rescue team and a journalist will be given maps for their very specific task, that may be created in real-time by a map creation tool similar to our proposed showcase application (see previous section). Figure 3 shows the significance of details in the data and thus, a possible slider position for each facet.

A. Rescue team

The rescue team needs a very fine-grained map of potential people in danger, who need to be rescued as soon as possible. In this case, the location data of every occurrence for postings with `#flood` needs to be visualized on the map. Temporal information is crucial for the rescue team to evaluate the urgency of every person in danger. Analyzing other hashtags in the posting besides `#flood`, for example `#help` or `#injury`, define the subject to exclude irrelevant data and avoid distraction through too much detail. No information should be shown about the social network of the social media

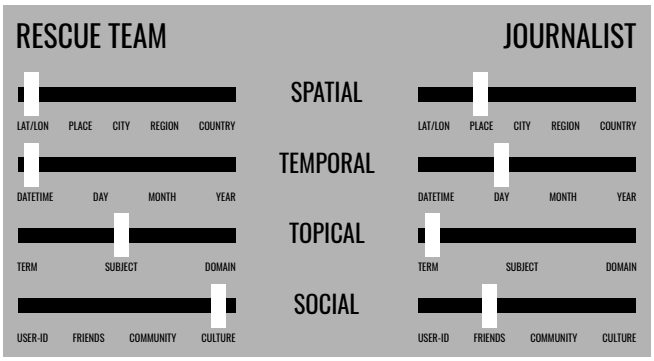

Fig. 3. Significance of details in the data for each facet

user, since the rescue team should not be able to decide who to rescue first, based on the social standing of the user.

B. Journalist

On the other side, the journalist wants to provide coverage about the flood. His map should provide information about social standing of affected people, to identify differences in the amount of financial harm to people of different regions. Individual users should not be able to be located on the map. Location data is relevant to a certain degree, that lets the reader be able to identify city regions, but no individuals. Temporal data may be taken into account just to the degree to ensure, that the data is taken from this flood incidence. The topic of the post should be very detailed, to identify the amount of potential damages through context detection.

VI. Evaluation

The herein presented model to preserve privacy of users when processing data from LBSM is describing a theoretical concept. The described scenarios are hypothetical and have not been evaluated with real-world situations, yet. The following steps in our research will include the actual implementation of an example application with real LBSM data. With this example application we will then be able to show a case study with real-life scenarios.

The presented model will also not be able to process all kinds of data visualization that can be derived from LBSM, but it helps to quantify privacy and understand the diversity of that matter. As shown, other research has described models and frameworks before, but their results are very closely related to a certain use case. With LBSM data mapped onto the four introduced facets, we provide a framework to describe privacy in LBSM in a very generic format. This can help understand privacy aspects in a wider scale and form a basis for further discussion.

The goal of this research project is certainly not to prevent malicious attackers from violating the privacy of social media users. We make use of LBSM data which is available to everyone on the internet. Preventing malicious attacks on that data would involve not only dealing with the for-profit companies behind those services, but also with the users themselves, as it is them who releases personal information to the public, either accidental or on purpose. If data is publicly available on the internet, everyone, including attackers have the same access to that data as we do, so this is not our target.

Instead, we are trying to prevent accidental disclosures of user-generated data in a scientific, cartographic context. Users of LBSM do not necessarily realize, that their published data may be used for other purposes than they intended. Creators of LBSM data driven maps may also not consider all implications of what is a possible privacy violation for each single user.

There are various ways to accidentally disclose private data. If map creators ignore these threats and keep using LBSM data carelessly, privacy violations will result in a lack of trust in research. This will harm the society we live in [29], and might lead people to re-think of sharing data, ultimately limiting the many positive ways in which these data can be used to provide benefits to the public. In contrast, if a fraction of people's daily generated data can be used to improve public well-being without compromising privacy, the potential is high that the sharing of valuable data continues to develop. For this means, we need to take care of privacy.

VII. Conclusion

We created a conceptual model to preserve privacy of users in location-based social media, when processing spatial information from their posts. For this model, we splitted the data into four facets. For each facet, we eliminated precise data by deriving multiple abstraction layers from it, that can be chosen arbitrarily.

With these layers we are able to describe different levels of privacy in a quantitative manner. This evolved the chance to evaluate the varying significance of each of the facets from different viewpoints. We showed the preservation of privacy aspects of the social media users in two contrary scenarios.

References

[1] K. Polous, "Event cartography: A new perspective in mapping," PhD thesis, Technische Universität München, 2016.

[2] G. Sagl, B. Resch, B. Hawelka, and E. Beinat, "From social sensor data to collective human behaviour patterns: Analysing and visualising spatio-temporal dynamics in urban environments," in *Proceedings of the gi-forum*, 2012, pp. 54–63.

[3] J. Lane, V. Stodden, S. Bender, and H. Nissenbaum, *Privacy, big data, and the public good: Frameworks for engagement*. Cambridge University Press, 2014.

[4] D. Solove, "Understanding privacy," 2008.

[5] M. Hildebrandt, "Privacy and identity," *Privacy and the criminal law*, vol. 43, 2006.

[6] F. Harvey, "To volunteer or to contribute locational information? Towards truth in labeling for crowdsourced geographic information," in *Crowdsourcing geographic knowledge*, Springer, 2013, pp. 31–42.

[7] F. Alrayes and A. Abdelmoty, "Privacy concerns in location-based social networks." GEOProcessing, 2014.

[8] B. Ağir, K. Huguenin, U. Hengartner, and J.-P. Hubaux, "On the privacy implications of location semantics," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 4, pp. 165–183, 2016.

[9] K. Biermann, "Betrayed by our own data." https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz/, 2011.

[10] J. E. Dobson and P. F. Fisher, "Geoslavery," *IEEE Technology and Society Magazine*, vol. 22, no. 1, pp. 47–52, 2003.

[11] P. Sánchez Abril, A. Levin, and A. Del Riego, "Blurred boundaries: Social media privacy and the twenty-first-century employee," *American Business Law Journal*, vol. 49, no. 1, pp. 63–124, 2012.

[12] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Privacy-enhanced location services information," *Digital Privacy: Theory, Technologies and Practices*, pp. 307–326, 2007.

[13] A. Monreale, G. L. Andrienko, N. V. Andrienko, F. Giannotti, D. Pedreschi, S. Rinzivillo, and S. Wrobel, "Movement data anonymity through generalization." *Trans. Data Privacy*, vol. 3, no. 2, pp. 91–121, 2010.

[14] J. Horey, S. Forrest, and M. Groat, "Reconstructing spatial distributions from anonymized locations," in *Data engineering workshops (icdew), 2012 ieee 28th international conference on*, 2012, pp. 243–250.

[15] R. Schlegel, C.-Y. Chow, Q. Huang, and D. S. Wong, "Privacy-preserving location sharing services for social networks," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 811–825, 2017.

[16] P. Coppens, C. Veeckman, and L. Claeys, "Privacy in location-based social networks: Privacy scripts & user practices," *Journal of Location Based Services*, vol. 9, no. 1, pp. 1–15, 2015.

[17] A. I. Abdelmoty and F. Alrayes, "Towards understanding location privacy awareness on geo-social networks," *ISPRS International Journal of Geo-Information*, vol. 6, no. 4, p. 109, 2017.

[18] D. Thom, R. Krüger, and T. Ertl, "Can twitter save lives? A broad-scale study on visual social media analytics for public safety," *IEEE transactions on visualization and computer graphics*, vol. 22, no. 7, pp. 1816–1829, 2016.

[19] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," *Version v0*, vol. 31, p. 15, 2008.

[20] B. Hogan, "Pseudonyms and the rise of the real-name web," 2012.

[21] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," *Communications of the ACM*, vol. 59, no. 7, pp. 96–104, 2016.

[22] D. Nield, "How to Find Anyone Online." https://fieldguide.gizmodo.com/how-to-find-anyone-online-1798301196, 2017.

[23] A. Dunkel, G. Andrienko, N. Andrienko, D. Burghardt, E. Hauthal, and R. Purves, "A conceptual framework for studying collective reactions to events in location-based social media," 2018.

[24] F. Krumpe, "Point Location." https://gitlab.vgiscience.de/Filip/point_location/, 2018.

[25] J. F. Allen and P. J. Hayes, "Moments and points in an interval-based temporal logic," *Computational Intelligence*, vol. 5, no. 3, pp. 225–238, 1989.

[26] S. T. Peesapati, H.-C. Wang, and D. Cosley, "Intercultural human-photo encounters: How cultural similarity affects perceiving and tagging photographs," in *Proceedings of the 3rd international conference on intercultural collaboration*, 2010, pp. 203–206.

[27] G.-B. Ivanov, "Complete Guide to Topic Modeling." https://nlpforhackers.io/topic-modeling/, 2018.

[28] A. Maireder, S. Schlögl, F. Schütz, M. Karwautz, and C. Waldheim, "The european political twittersphere," *Universität Wien & GfK*, 2014.

[29] P. M. Schwartz, "Privacy and democracy in cyberspace," *Vand. L. Rev.*, vol. 52, p. 1607, 1999.