

Modeling and Reasoning Upon Facebook Privacy Settings

Mathieu d'Aquin and Keerthi Thomas

Knowledge Media Institute, The Open University, Milton Keynes, UK
{mathieu.daquin, keerthi.thomas}@open.ac.uk

Abstract. Understanding the way information is propagated and made visible on Facebook is a difficult task. The privacy settings and the rules that apply to individual items are reasonably straightforward. However, for the user to track all of the information that needs to be integrated and the inferences that can be made on their posts is complex, to the extent that it is almost impossible for any individual to achieve. In this demonstration, we investigate the use of knowledge modeling and reasoning techniques (including basic ontological representation, rules and epistemic logics) to make these inferences explicit to the user.

1 Introduction

The notion of social translucence (as defined in [4]) concerns the design of systems with a social process component, to achieve coherent behaviours from the user(s) through making such behaviours visible and understandable to them. This notion is especially relevant in relation to privacy, where the principles of visibility, awareness and accountability promoted by social translucence are used to enable a coherent and informed behaviour from the users with respect to the distribution and propagation of their personal information. This idea is well illustrated in the notion of “Privacy Mirrors”, i.e., systems that integrate the necessary tools of “awareness and control to understand and shape the behaviour of the system” [6].

While these notions might appear to naturally apply to social networking systems such as Facebook¹, their privacy settings and of the mechanisms for information sharing they implement are only deceptively simple: for an individual user to keep track of all the necessary elements to understand what information others might have access to, and what inferences they might derive from it, is actually too complex to be achieved. For example, while individual photos have specific privacy scopes, the tagging, comments, likes, geographical information attached to them can make much more information about the user available to much more people than the user might intend, without the user’s ability to understand the full scope of the implications of such sharing and tagging.

In this demonstration, we show how a privacy mirror for Facebook can be implemented using knowledge modeling and reasoning techniques, to make explicit to the user some of the inferences that can be made out of information available about them on the social platform. We use basic ontology modeling, rules and a simplification of the basic concepts of epistemic logics.

¹ <http://facebook.com>

2 Information from Facebook

In this demonstration, to simplify the discussion, we focus on information about photos, especially the ones (explicitly) referring to the user. However, the basic notions and approach described apply similarly to other types of information. The basic concepts extracted using the Facebook Graph API² concern people (users), photos, comments, places and dates. Individuals (variables and constants) therefore represent instances of these concepts. Predicates represent relationships. For example, users can be friends with each-other ($friend(bob, alice)$), a photo can be at a place ($photoAt(photo1, segovia)$), at a certain date ($date(photo1, 08 - 07 - 2013)$) and include some users ($onPhoto(photo1, bob)$). Finally, any post including photos have a privacy scope which could be *everyone*, *friendoffriend*, *allfriends*, *custom* (e.g., $scope(photo1, allfriends)$).

3 Basic ontological modeling and reasoning

From the explicit data extracted from Facebook, basic information can be inferred using ontology-based mechanisms. For example, including range and domain information associated with the predicates mentioned above can help identifying types of objects (e.g., $friend(bob, alice)$ implies that $person(bob)$ and $person(alice)$). Similarly, using constructs available in OWL 2, the *friend* predicate can be declared to be reciprocal (as it is in Facebook): $friend(bob, alice)$ implies $friend(alice, bob)$.

Property hierarchies can also be used to introduce intermediary predicates, more abstract than the notions explicitly available in Facebook. For example, declaring *friend* as a sub-property of *know* (so that $friend(bob, alice)$ implies $know(bob, alice)$). The same mechanisms, combined with the property composition construct available in OWL 2, can be used to represent much more complex inferences (e.g., that if two people are on the same photo, they know each other). However, for convenience, we choose to use rules (which can also be used for other types of inferences not feasible with basic OWL constructs) for such complex implications.

4 Rule-based inference

As mentioned above, some more complex inferences need to be represented that are not conveniently achieved with ontological constructs. This includes information such that being on a picture, geotagged with a certain place, implies that the user was at that place ($wasIn(Per, Pl) :- onPhoto(Pic, Per), photoAt(Pic, Pl)$) or that two users on the same photo know each other ($know(Per1, Per2) :- onPhoto(Pic, Per1), onPhoto(Pic, Per2)$), and possibly that they were at the same place.

² <https://developers.facebook.com/docs/reference/api/>

5 Epistemic inference

The mechanisms described above make it possible for the model to explicitly make the inferences possible from the information being shared. However, the important aspect here is not only which inferences can be made, but who can make them. To address this, we use notions from epistemic logics [5]. Indeed, epistemic logics are a type of logic that allows one to express not only statements about the world, but also about the way the world is perceived or known by agents in the world. In such a logic, a statement of the form $\mathbf{K}_a \alpha$ indicates that the agent a ‘knows’ the statement α to be true. Basic properties, such as the one of self reflection (i.e., $\mathbf{K}_a \alpha \rightarrow \mathbf{K}_a \mathbf{K}_a \alpha$) and rules can be used to reason upon the knowledge agents have of some information.

This framework, combined with information about the privacy settings of Facebook, allows us to express information regarding which user might have access to what item of information. Straightforwardly for example, information on who knows about a photo can be derived from the privacy scope of the photo (e.g., $\mathbf{K}_a photo(Pic) :- author(Pic, Per), scope(Pic, allfriends), friend(Per, a)$). More complex mechanisms are also represented using this type of rules however, for example that the friends of somebody tagged in a photo would know about the photo, or that knowing about a photo implies knowing all the information attached to a photo and the possible inferences that can be made from them (e.g., that somebody was in a certain place with somebody else).

6 Implementation



Fig. 1. Screenshots of the system making explicit privacy inferences in Facebook.

The implementation of the system showing to a user the inferences that can be made from information sharing items concerning them (currently focusing on photos) and by who is a Web-based interface built in PHP and Javascript, that allows the user to connect to their Facebook account and extract the relevant information. The knowledge representation and reasoning mechanisms described above is delegated to a Prolog-based API, carrying out the ontological reasoning

(through a basic mapping between OWL and Prolog), the rule-based reasoning and a simplified implementation of epistemic rules described in the previous sections.

As shown in the screenshots of Figure 1, the system displays the inferred information to the user: 1- the people they are friend with, the ones they know (without being friends) and the people the user might not know, but who might have access to some of their information; 2- the photos depicting the user; 3- the places where the user have been (who with and on what date). Clicking on a person (as shown on Figure 1) displays information about items shared by this user, as well as the information they know about the logged-in user. Clicking on an item displays the information that can be inferred from this item, and the people who might have access to these inferences.

7 Conclusion

Our goal in this demonstration is to show that knowledge modeling and reasoning techniques can support the notion of privacy mirrors, in systems where the privacy implications of information sharing are complex and difficult for a user to keep track of. In the demonstration, participants will be able to connect the system to their own Facebook account, to check whether the results are surprising, concerning or on the contrary, just reassuring (which are the types of reactions we uncovered in another study [3]). In terms of future work, besides completing and validating the modeling of Facebook's privacy mechanisms (which can be a complex task), one of the interesting research directions is to integrate the model of Facebook with other sources of personal information sharing (using for example techniques described in some of our previous works, e.g., [1, 2]). The other direction we plan to investigate is the use of more sophisticated knowledge representation techniques to deal with the complexity of online social situations, including uncertainty and different levels of epistemic knowledge of information (e.g., having access to information vs. having surely seen a piece of information).

References

1. M. d'Aquin, S. Elahi, and E. Motta. Personal monitoring of web information exchange: Towards web lifelogging. *Web Science*, 2010.
2. M. d'Aquin, S. Elahi, and E. Motta. Semantic technologies to support the user-centric analysis of activity data. In *Social Data on the Web (SDoW) workshop at ISWC*, 2011.
3. M. d'Aquin and K. Thomas. Consumer activity data: Usages and challenges. Knowledge Media Institute, Tech. Report kmi-12-03, 2012.
4. T. Erickson and W. A. Kellogg. Social translucence: an approach to designing systems that support social processes. *ACM transactions on computer-human interaction (TOCHI)*, 7(1):59–83, 2000.
5. J.-J. Ch. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge University Press, 2004.
6. E. D. Nguyen, D. H. ; Mynatt. Understanding and shaping socio-technical ubiquitous computing systems. GVU Technical Report;GIT-GVU-02-16, 2002.