AngeLA: Putting the teacher in control of privacy in the classroom

Andrii Voznuik, Sten Govaerts, Lars Bollen, Sven Manske, Tobias Hecking, Denis Gillet

AngeLA: Putting the Teacher in Control of Student Privacy in the Online Classroom.

Andrii Vozniuk*, Sten Govaerts*, Lars Bollen†, Sven Manske‡, Tobias Hecking‡ and Denis Gillet*
*REACT, EPFL, Station 9, CH-1015 Lausanne, Switzerland
{firstname.lastname}@epfl.ch
†Department of Instructional Technology, University of Twente,
PO Box 217, 7500 AE Enschede, The Netherlands
l.bollen@utwente.nl
‡COLLIDE Research Group, University of Duisburg-Essen, 47047 Duisburg, Germany
{lastname}@collide.info

***Abstract*—Learning analytics (LA) is often considered as a means to improve learning and learning environments by measuring student behaviour, analysing the tracked data and acting upon the results. The use of LA tools implies recording and processing of student activities conducted on software platforms. This paper proposes a flexible, contextual and intuitive way to provide the teacher with full control over student activity tracking in online learning environments. We call this approach AngeLA, inspired by an angel guarding over LA privacy. AngeLA mimics in a virtual space the privacy control mechanism that works well in a physical room: if a person is present in a room, she is able to observe all activities happening in the room. AngeLA serves two main purposes: (1) it increases the awareness of teachers about the activity tracking and (2) provides an intuitive way to manage the activity tracking permissions. This approach can be applied to various learning environments and social media platforms. We have implemented AngeLA in Graasp, a social platform that fosters collaborative activities.**

I. Introduction

Recently, personal data privacy has received global attention, due to the revelations in the NSA scandal[1]. This made some users of online services much more concerned about their data privacy. They demand more transparency with regard to what personal information is collected, who collects and processes it and what for. Moreover, the users want to have more control over the data collection and processing policies.

To be able to control data privacy, it is important to understand the many aspects and definitions of data privacy. According to the state of the art analysis of data privacy done in the framework of the SPION project [1], two types of data privacy can be identified: (1) social privacy and (2) instrumental privacy. Raynes-Goldie [2] defines social privacy of users as "the control of information flow about how and when their personal information is shared with other people". As an example, social privacy can be achieved by introducing a trust-aware data sharing mechanism [3]. According to Boyd [4], instrumental privacy is defined as the control of data access by corporations and government, for instance for data analysis or data mining. Instrumental privacy is the focus of this paper.

Data privacy is regulated in different ways by many national governments and often depends on the target audience. For instance, in the case of schools and teachers, student data privacy is of particular importance, since student online activity tracking is subject to stronger legal privacy regulations, due to the age of school pupils. For instance, the European Union provides a data privacy framework, through the EU directives 95/46/EC (Data Protection Directive) and 2006/24/EC (Data Retention Directive).

Apart from governments guarding over privacy, software itself and its privacy policies have evidently a large impact on data privacy. Boyd et al. [5] discusses how privacy can be enforced on the system architecture level and thus be an inherent part of the software design. This is what we also want to achieve in the Go-Lab European project[2]. The project aims to help school students to develop inquiry learning skills and motivate them to choose STEM (science, technology, engineering and mathematics) subjects for their career path. To accomplish this, Go-Lab enables remote access to laboratory facilities so that students can remotely conduct experiments potentially involving expensive equipment. Teachers can search online labs and create learning spaces for their students using these online labs by making use of the Go-Lab Portal [6]. This portal consists of two main components: (1) the Lab Repository and (2) the Inquiry Learning Space (ILS) Platform. The latter allows teachers to build Inquiry Learning Spaces [7], which are learning environments tailored to the inquiry-based learning methodology, and enables teachers to share such an ILS with their students.

In addition to being a means to structure learning materials and an interface to the laboratory equipment, ILSs provide tools such as scaffolds to improve the learning process. The scaffolds are tools that aim to help students to stay in the zone of proximal development, providing guidance and help when needed. The scaffolds rely on the learning analytics back-end to analyse activities of students and teachers recorded during their interaction with the ILS [8]. The traces can be used as well to build learning analytics dashboards [9] helping teachers to have better understanding of what is happening in an online classroom.

This paper focuses on the instrumental privacy and illustrates the design and implementation of a data tracking management system that allows teachers to control the activity data

[1]The Guardian NSA Files, http://www.theguardian.com/world/the-nsa-files

[2]Go-Lab, http://www.go-lab-project.eu/

collection policy in an online learning environment (OLE). The paper is structured as follows. First, Section II formulates the requirement for a tracking permissions management system in an OLE. Then, Section III considers existing approaches for tracking management user interfaces. Afterwards, Section IV explains the philosophy and idea behind the proposed solution (called AngeLA). Finally, Section V demonstrates how the widely applicable AngeLA mechanism is implemented in a specific context and platform.

II. Requirements

In general, five key requirements for a tracking permission management system in an online learning environment have been identified based on the Go-Lab project prerequisites and [5], namely:

1) *fostering awareness*. The user interface of the tracking management system should make a teacher aware of the ongoing activity tracking.
2) *offering intuitive UI*. The tracking management UI should be build with the help of concepts and elements of UI already familiar to users.
3) *enforcing student privacy*. A teacher should be in control of the tracking and be able to enable or completely disable it when needed.
4) *providing flexibility*. It should be possible to adjust tracking permissions depending on the context, for instance for one group of students the tracking can be enabled and at the same time for another one - disabled.
5) *enabling data aggregation*. The system should be able to aggregate relevant student activity data coming from all parts of the learning environment.

III. Related Work

An intuitive way to increase user data privacy, followed by web platforms such as Facebook[3], is to have an extensive privacy policy configuration. But even in the case when such a control mechanisms is provided, it could be hard to use and understand because of the complicated menus and navigation hierarchy. The large number of options could as well make it hard for the users to make proper privacy decisions [10]. Furthermore, the default privacy policy could change quickly[4] and it could be hard for users to follow and adapt.

To simplify understanding of data sharing policy in a social network, Iannella et al. [11] suggest to use a set of icons in the user interface. While having proper icons in the GUI fosters privacy awareness, the approach targets social privacy, i.e. sharing the data between different users of the platform and seems not to influence the instrumental privacy.

Hull et al. [12] focus on the design of user interface that can increase user awareness about how the changes made in the user interface can influence user privacy. The authors argue that most of the privacy issues often found in online social networks can be explained by the difference in the context (contextual gap) between the online and offline social contexts. Indeed, offline privacy is highly defined by the social context while online systems lack much of this context. Hull et al. showcase the privacy issues on Facebook as an example. They conclude that most of the issues could be resolved just by improving the user interface in a way that makes the information flows more transparent for users.

Another important aspect influencing the user privacy is is the default privacy settings [13]. Some websites could benefit from understandable and restrictive privacy policy. For instance as showed by Tsai et al. [14], a more protective and clear privacy policy of a shopping website increases the probability of users actually buying on the website. At the same time many websites profit from information disclosure made by users, for instance Facebook has a default policy [15] promoting data disclosure. Online platforms could even employ so-called Dark Patterns[5] to make it harder for user to change the default privacy settings into a more strict privacy policy.

IV. The Learning Analytics Tracking Agent

In this section we introduce our approach (called AngeLA) to managing activity tracking permissions. AngeLA is motivated by the privacy mechanism and policy embedded into a physical classroom. In a physical classroom the teacher is in control of the privacy of what the students do in the classroom, e.g. she can decide which student behaviour she shares with the parents. If the teacher wants to discuss in private, she can ask all unwanted parties to leave the room. AngeLA mimics in a virtual space this privacy control mechanism that works well in a physical space. In a collaborative online space (e.g. an online learning space or a chat room), user management mechanisms exist to grant and revoke access to the space or resource. AngeLA is essentially a software agent that can be invited into an online space together with other members. When AngeLA is a member of an online space, AngeLA has access to any activity taking place in this space, just like any other member of this space and like the teacher in the classroom. AngeLA can thus collect all activities of the space members and can store them in the local database and, as in our case, can send this information to a third-party LA service. The owner of the online space can revoke AngeLA's access to the space, after which AngeLA can no longer track any user activity in this space. AngeLA's permissions can be configured per space depending on the activity context in the same way as a person can be invited to be present in some room and in the same time not invited to other ones.

By managing privacy via access control of AngeLA to an online space, the teacher is in full control of when the student activity is tracked and when not. This privacy control happens through already familiar user management functionality of inviting collaborators. Furthermore, by having the tracking agent as a visible space member, the teacher is aware of AngeLA's presence and hence that the tracking is turned on. Having easy privacy control and high visibility can also increase trust in the system due to being open about the tracking policy [14]. With AngeLA we implement a soft paternalistic privacy policy, where the system does not force a user to make specific privacy decision, but rather make her aware about the ongoing activity tracking and provide an easy and intuitive way to change it.

[3]Facebook Data Use Policy, https://www.facebook.com/about/privacy/

[4]The Evolution of Privacy on Facebook, http://mattmckeon.com/facebook-privacy/

[5]Dark Patterns, http://darkpatterns.org/

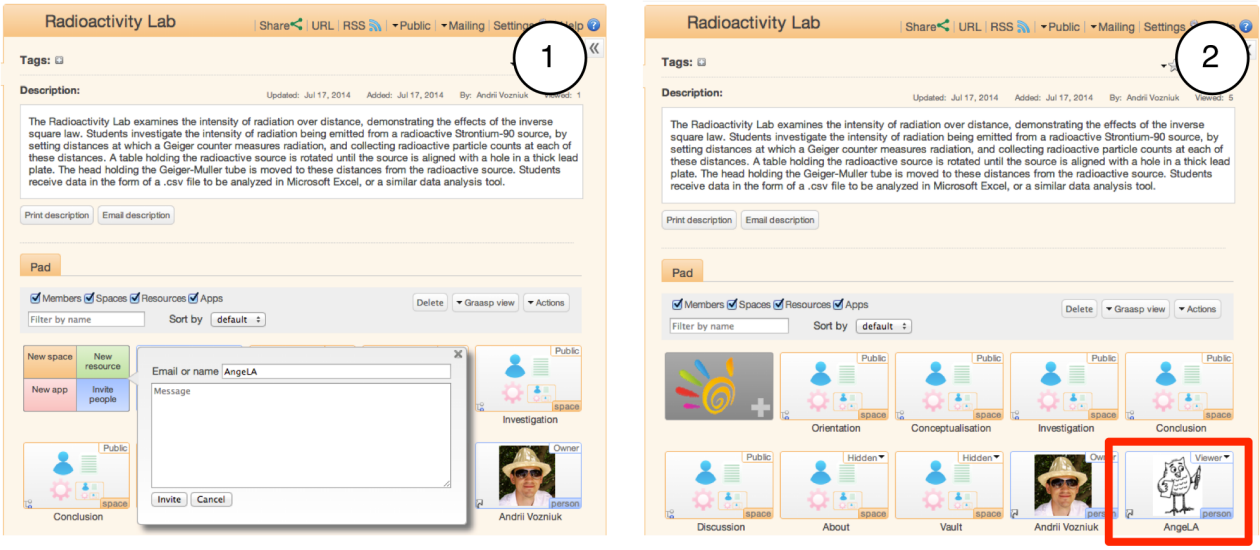

Fig. 1. (1) AngeLA is invited to become a member of the "Radioactivity Lab" space in Graasp. (2) AngeLA is a member of the space.

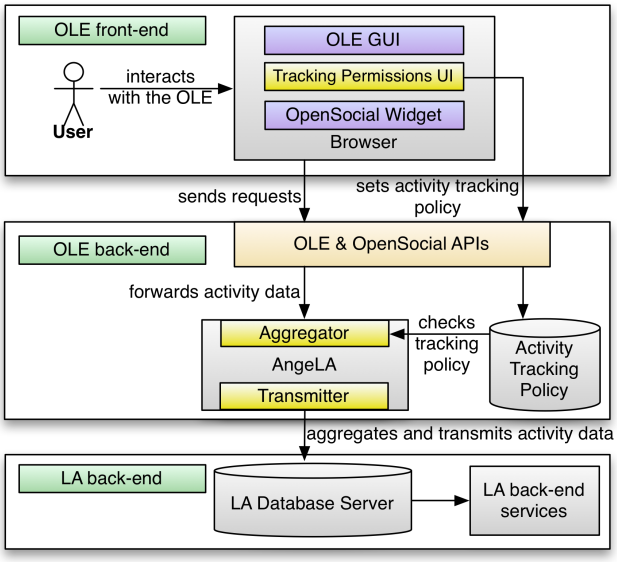

Fig. 2. An architecture of the Learning Analytics Tracking Agent (AngeLA).

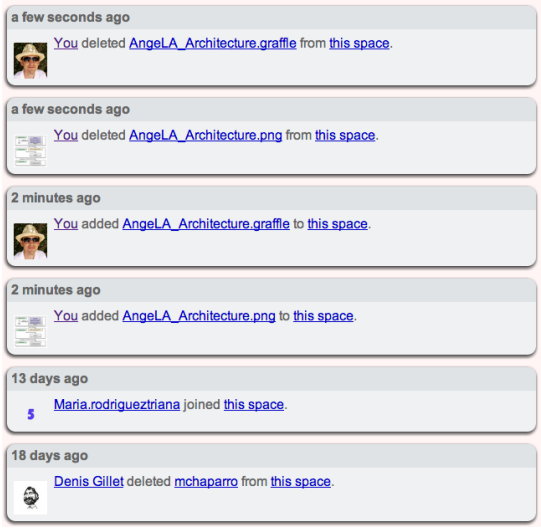

Fig. 3. A sample stream of user activities in a space.

V. Implementation

We implemented the proposed approach in Graasp,[6] a social platform supporting people in collaborative activities that is often used as an online learning environment. For instance, in the Go-Lab project teachers use Graasp to construct Inquiry Learning Spaces [6].

The Learning Analytics Tracking Agent (AngeLA) architecture as presented in Figure 2 consists of the following three components:

Tracking Permissions UI. AngeLA aggregates user activities only from the learning spaces where it is a member. This provides an easy-to-use and familiar manner to manage privacy: (i) to enable the activity tracking in a space the teacher just needs to invite AngeLA to this space (see Figure 1 (1)) and (ii) to disable tracking the teacher can just removed AngeLA from the space. When AngeLA is present in the space (as in Figure 1 (2)), all the activities of space members will be collected, stored and sent to the LA back-end. This behaviour is intuitive and familiar for the teacher, since all space members are expected to be aware of the space activities.

User Activity Aggregator. AngeLA continuously aggregates activity streams of the Graasp users across the spaces where it is a member into a single activity stream as shown in Figure 3. In the case of Go-Lab the data is coming from the following sources: (1) ILS Platform, i.e. Graasp, where the ILS authoring is done. (2) ILS student view, where students interact with the platform. In the latter case the activity data is submitted from within OpenSocial widgets via the Opensocial API (see Figure 2).

Activity Data Transmitter All the activity records col-

[6]Graasp, http://graasp.epfl.ch

```
{
  "published": "2014-07-12T15:04:55Z",
  "actor": {
    "id": "887",
    "objectType": "User",
    "displayName": "Andrii Vozniuk"
  },
  "verb": "add",
  "object": {
    "id": "1279",
    "objectType": "Asset",
    "displayName": "Lecture Notes.pdf"
  },
  "target": {
    "id": "1354",
    "objectType": "Space",
    "displayName": "Social Media Class"
  },
  "generator": {
    "id": "4574",
    "objectType": "Widget",
    "displayName": "File upload widget"
  }
}
```


Fig. 4. A sample user activity represented in the ActivityStreams format.

lected are sent to the LA back-end [8] for further processing. The Activity Streams format is used to represent the actions during the transmission (see Figure 4). As a mean to provide additional privacy in the Go-Lab portal, as proposed by Li et al. [16], students use nicknames instead of real names to represent their identity in Graasp. In this case only the teacher is able to do the mapping between the nickname and real student name and hence knows a student's identity.

The nicknames approach indeed provides an opportunity for students to hide their real name from the platform. A teacher could ask students to use nicknames but she can not guarantee that none of the students would put a real name. Moreover, since the data collection is happening, it is possible that student identity could be revealed if proper data mining algorithms are applied. AngeLA approach aims to provide teachers with a mechanism to completely disable the data tracking, which guarantees that activity data is not collected.

To enforce privacy it is important to setup a strict and clear default privacy policy [13]. In Graasp we suggest teachers to decide if they want to have AngeLA as a member of a space upon its creation. In this way a teacher is able to define a clear permission policy for a space from the very beginning, before students start working with the space. After the space is created it is still possible to change the policy at any time by simply inviting or removing AngeLA from the space.

VI. Conclusion & Future work

The proposed approach to control activity tracking makes use of familiar user rights management functionality to grant or revoke access of a software agent to an online space. AngeLA provides an intuitive and contextual way to control privacy while enabling privacy awareness cues and potentially trust. This concept can be extended beyond the implementation discussed above to other learning environments or collaborative web platforms where there is a notion of a group, a room or a space.

We expect that employing a clear and protective privacy policy in Go-Lab would lead to higher level of adoption of the platform. Indeed, Tsai et al. [14] showed that more protective and clear privacy policy of a website could lead to users shopping more on the website. In the near future, we plan to evaluate AngeLA with teachers and students to verify our expectations with the data. Additionally, we want to extend the implementation with a configuration for the LA back-end service where AngeLA sends data to.

Acknowledgment

This research is partially funded by the European Union in the context of the Go-Lab project (Grant Agreement no. 317601) under the Information and Communication Technologies (ICT) theme of the 7th Framework Programme for R&D (FP7). This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

References

[1] A. Acquisti, E. Balsa, B. Berendt, D. Clarke, R. D. Wolf, C. Diaz, B. Gao, S. F. Gürses, A. Kuczerawy, J. Pierson, F. Piessens, R. Sayaf, T. Schellens, F. Stutzman, B. V. Alsenoy, and E. Vanderhoven, "SPION Deliverable 2.1 State of the Art," COSIC internal report, 2011.

[2] K. Raynes-Goldie, "Aliases, creeping, and wall cleaning: Understanding privacy in the age of facebook," *First Monday*, vol. 15, no. 1, 2010.

[3] N. Li, M. Najafian-Razavi, and D. Gillet, "Trust-aware Privacy Control for Social Media," in *Work-in-Progress of CHI 2011*.

[4] D. Boyd, "Taken out of context: American teen sociality in networked publics," Ph.D. dissertation, University of California-Berkeley, 2008.

[5] D. Boyd and A. E. Marwick, "Social privacy in networked publics: Teens' attitudes, practices, and strategies," in *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, 2011.

[6] S. Govaerts et al., "Towards an Online Lab Portal for Inquiry-based STEM Learning at School," in *ICWL 2013*.

[7] D. Gillet, T. de Jong, S. Sotirou, and C. Salzmann, "Personalised Learning Spaces and Federated Online Labs for STEM Education at School: Supporting Teacher Communities and Inquiry Learning," in *EDUCON 2013*, pp. 769–773.

[8] T. Hecking, S. Manske, L. Bollen, S. Govaerts, A. Vozniuk, and H. U. Hoppe, "A flexible and extendable learning analytics infrastructure." Springer, 2014, pp. to appear, accepted 2014/05/12.

[9] A. Vozniuk, S. Govaerts, and D. Gillet, "Towards portable learning analytics dashboards," in *ICALT 2013*.

[10] B. Schwartz, "The Paradox of Choice: Why More is Lesss." Harper Perennial, 2005.

[11] R. Iannella and A. Finden, "Privacy awareness: Icons and expression for social networks," in *8th International Workshop for Virtual Goods*, 2010.

[12] G. Hull, H. Lipford, and C. Latulipe, "Contextual gaps: Privacy issues on facebook," *Ethics and information technology*, vol. 13, no. 4, pp. 289–302, 2011.

[13] Y.-L. Lai and K.-L. Hui, "Internet opt-in and opt-out: Investigating the roles of frames, defaults and privacy concerns," in *ACM SIGMIS CPR 2006*.

[14] J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," in *WEIS 2007*.

[15] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 2005, pp. 71–80.

[16] N. Li, A. C. Holzer, S. Govaerts, and D. Gillet, "Enforcing Privacy for Teenagers in Online Inquiry Learning Spaces," in *Understanding Teen UX workshop at CHI 2014*.