Privacy, Trust and the Practice of Learning Management Systems

Kai-Uwe Loser, Thomas Herrmann, Ruhr-University Bochum, Germany,
Email: kai-uwe.loser@rub.de, thomas.herrmann@rub.de

Abstract: Current LMS like Blackboard or Moodle have a great potential to be improved with respect to privacy and data protection. Legal compliance is only one reason for this need. Another is that trust and privacy are linked and an open culture for learning with respect for each other needs contributions from respecting privacy. The paper argues from theoretical directions of privacy and data protection guidelines and from power relations with a empirical background from practical usage at a university in Germany.

Introduction

> “Trust between teachers and students is the affective glue that binds educational relationships together. Not trusting teachers has several consequences for students. They are unwilling to submit themselves to the perilous uncertainties of new learning. They avoid risk. They keep their most deeply felt concerns private. They view with cynical reserve the exhortations and instructions of teachers.” (Brookfield 1990, p. 162)
>
> “Who is not sure, that deviant behavior could be noted anytime and written down, used as information and transferred, will try to avoid to show any of this kind of behavior.” (German Constitutional Court 1984 – authors’ translation)

The first cite from Brookfield covers the topic of trust within the personal relations between teachers and learners. The latter cite comes from the historic court decision of the German Constitutional Court arguing for privacy from a constitutions perspective. It is obvious from both citations that privacy is a facet to preserve freedom, and as well it is widely acknowledged that preserving privacy is one of the components of creating trust between learners and teachers. Protecting privacy on the technology part should therefore contribute to a positive attitude in the relation between the various actors. We currently see complex systems – Learning Management Systems (LMS) like moodle or blackboard – which actually store a huge amount of data. The primary focus of course cannot be privacy and data protection, but analysing LMS we found that currently in many cases too many data about students’ behavior is processed. At some institutions we see an open discussion about whether the systems are trustable. It happens especially in a field where system application is connected with civic education that needs to be aware of rights and responsibilities. Here we can see the direct link between the two citations from the beginning of this paper. The link between trust and the learning culture is known as well as the results of ubiquitous observation, in other words limited privacy. In consequence it is a little surprise that in many LMS well known privacy and data protection principles were widely ignored.

Discussing privacy and data protection the first perspective that comes to mind is IT security. The LMS are nowadays used in large environments and therefore security aspects – especially the technical perspective – already received some attention (e.g. Eckert 2003, Eibl 2009). The organizational perspective is often argued from a policy level (Culnan & Carlin 2009) but it is also known that policies are limited. One the one hand practice is that in many countries codes of conduct are the main approach to accomplish privacy and data protection. On the other hand whether or not technical features ensure confidentiality and security largely depends on the actual behavior of users involved (Lampson 2009). In this paper our perspective is a ‘privacy-by-design’ approach which emphasizes neither a security perspective nor a pure organizational approach.

Our work was based first on an analysis of the main platform of one university with about 30.000 students. The challenges described in this paper were also backed up by a literature analysis with descriptions of systems practically used in universities. These were confirmed and clarified by discussing the issues with privacy commissioners of other universities in Germany. The overall process made several deficits visible, and on this foundation there were three interviews conducted, where it was tried to clarify the actual needs of lecturers. The following section will present some backgrounds on privacy aspects. The following section we will argue for some concrete ways to support trust by privacy and data protection measures from our empirical background and the requirements of data protection.

Background to Privacy and Data Protection

Acknowledging Power Relations

From CSCW-oriented privacy discussions (Clement 1992, Bellotti and Sellen 1993) we know that for effective cooperation personal knowledge about others is necessary (Awareness). At the same time this is intrusive to privacy. Solutions there are based on the assumption that cooperating users have a symmetrical peer-to-peer type of relationship. None of the users has the right or power to enforce another to a certain behavior. In teaching contexts we usually find this kind of symmetric role relations when students cooperate. In E-Learning we also see asymmetric constellations, where one group can sanction another: student vs. teacher, students vs. administration. Within asymmetric relationships privacy and data protection problems usually create more harm to the individuals. Privacy and data protection principles as they are defined in the legislation are intended especially for this kind of constellations.

The success of LMS usage depends to some level on the motivation, which is also related to trust between all parties involved. The amplification of already asymmetric power relations by unbalanced functionality to control others is counterproductive. We see wide discussions of phenomena in some universities focused on this kind of topics. What is a necessary and appropriate level of control that tutors can perform? We argue for rethinking the systems reflecting these differences in relationships: access and visibility of presence information might be acceptable when students cooperate, on the other hand vision of tutors is limited to appropriate details. They especially see aggregations of data, useful to their needs. Another aspect is that sometimes actions of tutors are hidden in the system. You cannot see which documents tutors visited. Behaving transparently (within systems supporting this) is a possible strategy to create trust. Hiding behavior, and leaving intentions to the imagination of controlled parties leads to the opposite and can harm learners' motivation. Some evidence for this can be found by searching other discussion forums and social communities for discussions about subjects of courses. "Only the smart questions are asked there anyway. The stupid questions are discussed elsewhere." – a cite of a student. It should make clear that anonymity of questions – although it also may have other problems – is necessary, to get the stupid questions as helpful feedback. For our empirical background the used platforms for the discussions can be named for several faculties. Discussion of taught content is needed, but obviously this is not happening in LMS as intended, but elsewhere. Power relations seem to add on this. Beyond legislation this thought might initiate some rethinking of LMS functionality. In the following the asymmetries in power relation play a major role for the arguments to rethink the technology and practice.

Privacy and Data Protection Guidelines

The legislation from its beginning in the 1970s had a perspective first on the (power) relations between public authorities and citizens which lead to several principles which are widely used in legislation around the world. In addition the privacy perspective, which respects private spaces in comparison to public spaces, the data protection perspective accepts that the digital representation has effects that may be problematic (unwanted distribution, misinterpretation of mediated data, use in broad calculations for intrusive behavioral models etc.). This paper refers to the 1980s OECD Guidelines for data protection with the following eight principles, which can be used to discuss several practices in the LMSs and need to be considered to become legally compliant:

- Collection Limitation Principle: data collection is only allowed as lawful means for at least fair purposes. Minimizing data collection to the necessary level is a wicked problem due to the needed decision what actually is necessary in comparison to just "helpful" information.
- Data Quality Principle: it requires data processors to take care that data collected is kept accurate, complete and up-to-date.
- Purpose Specification Principle: the purpose of data collection needs to be transparently defined prior to data collection.
- Use Limitation Principle: the use of data is limited to the defined purposes.
- Security Safeguards Principle: technical and organizational measures need to be in place to secure the personal information.
- Openness Principle: that data processing should be made comprehensible to the public.
- Individual Participation Principle: The data subject has the right to get information about which data about oneself is stored.
- Accountability Principle: for all data collections it needs to be made clear who is accountable. For LMS this is mostly regulated in organizational policies.

These principles are useful as analytical categories, but are are not easy to translate to system functionality. Approaches for structured methods exist (Spiekermann and Cranor 2009). The background of the LMS as cooperative systems with some specifics induces complexity that leads to perspectives that needs a more detailed analysis and a reference to results from the field of CSCW.

Privacy Improvements to Maintain Trust

Course Based Configuration of Data Recording

One deficit with respect to the aforementioned principle of *"collection limitation"* is that data collection of usage data for awareness mechanisms cannot be configured on different levels: The low level necessities for simple lecture scenarios where the LMS is used just for sharing of presentation slides should be sufficiently configurable as well as the full featured needs of complex scenarios with teamwork in subgroups etc. Options for configuring the data collection on the course level would already be a big step forward, but it would be even more useful, to bind them to the usage of a specific functionality. So if notification is turned on, the data collection of the specifically needed events for these elements is initiated, otherwise this data will not be logged. From a data protection perspective legitimate data collection is always justified from actual (legitimate) use of the data. And this also is in line to the users' perspective: they do not want to bother which kind of data is needed. They do think from what is needed as a function to fulfill their task.

We evaluated the practical information needs from current use in our study. First we made a course data review looking at actually used functionality in the courses. Secondly we detailed hypotheses and results with three interviews with teaching personnel as well as consulting experts. Our results here are that there are possible groupings of the whole list of functionality which can be differentiated with certain needs regarding personal data. It became clear that the feature driven development and configuration of the systems is problematic. A discussion forum for example is in one pattern used as a personal broadcasting communication channel, disclosing work, detailed times etc. (discussion is part of the personal work assignment) whereas in another scenario it is sufficient to have an anonymous but public communication channel without any further information of user details. For further elaborating on a solution we derived seven clusters of system modules with a proximity in usage grouping functionality like "Lecture support" or "projectbased courses" that can be regularly seen as part of the same usage scenario. Using patterns the configuration process for regularly performed scenarios can be simplified, while justifying the data and information needs from the point of view of these scenarios. Systems may support these standard cases with preconfigured enforced "policies". Each tutor can decide on his practical needs which scenario is acceptable, at the same time adhering to the privacy and data protection requirements. In any necessary case individual solutions remain possible can be implemented after personal consultancy of knowledgeable institutions. The data analysis shows that these are single instances where the higher administrative overhead is reasonable.

Identity Management

In many installations the creation of accounts for system use is not bound to any checking of the identity, which leads to problems regarding identity theft scenarios. This is related to the *data quality principle*. Often one can simply create an account using another students' name and make someone look odd from a teachers' perspective. In open platforms on the web this aspect is negligible, because the primary contact is on the web (with the pseudonyms in discussion forums, wikis and the like). In LMS the primary contact is in the reality, and pseudonyms can be used to mislead the connection between an online and a real identity. The pseudonym "John_Smith" may be controlled from "Eddy Evil" in reality, although a John Smith actually exists in an organization. This may lead to problems when teachers will have to grade students in reality. Therefore it is useful to use identity management and assured authentication within LMS. On the other hand not in all scenarios it is useful nor necessary to know all persons performing actions. Sometimes necessary checks might be reduced to the decision of just checking if someone is allowed. This can be done with anonymous credentials (Welch et al. 2005). One scenario where this might be applied is the download of teaching materials. In many cases it is not necessary to actually know who downloaded the material. With anonymous credentials the access right is checked without knowing the identity at the stage of access (cf. Franz et al. 2006).

Anonymization and Data Retention

In some countries it is legally required to delete data in compliance with a defined process to follow the *use limitiation principle*. A student that discussed a topic naively in a first semester course discussion forum should have a chance that these utterances will disappear at some point in time. There are basic legal rules requiring to mandatorily delete data when their purpose is no longer existing according to the *purpose specification principle*. In principle it should be clear at the time of data collection when data will be actually be deleted (or anonymized). "When" refers to a concrete time or a condition mostly bound to a process status. This aspect is not widely thought through in LMS. We found three types of functionality to delete data. First objects can be deleted by a user with the appropriate access rights, e.g. entries in discussion forums can be deleted. Secondly complete courses can be deleted, mostly by administrators. Thirdly courses can be reused by teachers. Supporting this is a definitely necessary functionality and this is usually implemented with a limited transfer. To some extent personal information especially of earlier participants is not transferred to the new course. In some cases one can also find ways to work around these limited options and find a way to delete groups of data, data in a discussion forum etc.

But it is obvious that this limited functionality leads to prolongued storage of data. Deletion on the micro level is usually not available. An example is the timestamp usually written with discussion forum contributions. Although it is helpful to know that an answer actually came seconds ago ("maybe I get a chatting answer, when I give a quick response myself now"), there is very little use of the information at that level of detail when the responses were days ago. These timestamps document some types of behavior ("Student X usually works at midnight."). From a privacy point of view this level of detailed data should be avoided.

Systems functionality needs to offer options to configure deletion, data detail reduction or anonymization. One can think of a discussion forum in a LMS about the organization of a course, where comments other than the ones of the teacher are deleted after a configurable time (for example 4 months).

Roles and Privileges

The basic idea of confidentiality is linked to the use limitation principle: each user should only see those data relevant to their task. The translation from the task descriptions to technical roles with privileges is usually done with authorization schemes. These schemes are in comparison to other kinds of systems simple in LMS. Roles in authorization schemes are usually limited to administrators (technical and organizational administrators are usually not distinguished), teachers with full access to their courses and some types of supportive roles: content managers, assistants usually being students. Beyond these basic roles more dynamic roles for access rights need to be considered. Users can be part of a course or of (sub-) group within the course. For all these types of role models access control mechanisms are usually available in the systems.

From a cultural differences perspective it is interesting to see that in some systems a "parents' view" is implemented, allowing parents to view the workspace of their children. If this is allowed or necessary access seems to depend on the age of students. In higher education there is no use for this kind of backdoor access. The access of parents also is hidden from the students. From a privacy point of view this is in any case contradictory to the general principles. Another type of hidden account with a false identity is often used for checking the students' perspective on the configuration.

But the main deficit is coming from the fact that in practice the available access control functionality with their roles and mechanisms are simply not applied. Professors take for granted that their responsibility lead to full permissions although it is rare that they actually perform tasks themselves. Instead student assistants are active in the LMS and perform tasks like updating course information, uploading presentations and other material or making test results available. But those assistants should act in the background, but should have full access. We found that all administrative actors in the LMS have full permissions to the course information. The problematic constellations arise from identities being assistants as well as fellow students that regularly happen. They have access to detailed information (marks, contributions) about their fellow students. This becomes especially problematic, when this access is also hidden, so that a student cannot even know, that a colleague knows these details. General privacy guidelines require to select specific roles with limited privileges and specific restrictions in this case. But the existing technical options are not widely used. An analysis of the actually used roles showed that within 2194 courses at our University 33% had more than one lecturer with full access. On the contrary only 21% used roles with limitations. At that time it was also possible and regularly reported that passwords were passed on, so that there were even more courses managed by more than one user with full access. Responsible people from other universities in Germany supported these figures from their experience.

To overcome these deficits first there are policies needed. But secondly the reasons are also grounded in technological obstacles. For example users cannot foresee the results of specific selections for access control. Since it is much easier to select full access – there will never be a problem that the assistants have access problems – those are selected. It has to be easier to see which limitations are bound to a certain role, what can be done with this role and from a usability perspective there might be specific views to support the respective tasks of the role more efficiently than with the general roles. If it would be easier to predecide, whether a problem might really occur or not, decisions about privileges might be made more reluctant.

Visibility in LMS: Public and Private Spaces

Linked to access privileges is a view on the LMS rethinking their conception of place and space (Snowdon and Munro 2001). LMS should support learning. So far the idea behind most LMS is that learning happens best under the guidance of a teacher in the classroom. But this is also sometimes perceived as under the control of a teacher. The systems are conceptualized as a replacement of the classroom or an extension of it. In all times at schools and universities learning also happened in solitude and between uncontrolled groups of learners. LMS tend to control these places of learning. This contributes to students evading to other platforms out of sight of teachers. Assuring private and closed peer group spaces in LMS's may bring some of the students back and may make some of the "stupid questions" visible, because the teacher is closer. To reach this we need a trustable environment first. We see a strong link to the openness principle and the discussed topics of power relations.

Openness and Power Relations

A different approach would be that in principle the groups with lesser power (students) are allowed to see behavior of the one with power (teacher). This may seem odd at first. The consequences would be twofold: Firstly teachers may reduce problematic behavior since it might become visible, and might be interpreted as misuse. Secondly students will get an impression of what actually goes on behind the scenes. When the system itself is open, transparent and trustable it will also create trust to the teacher. Access limitations or gatekeeper-models to possibly problematic functionality is no longer needed, because teachers will reduce possibly problematic behavior themselves. This is similar to the equivalence principle which was developed in the CSCW discussion and which was based on more or less symmetrical power relations. In LMS this is not the case. In some cases the "symmetry" assumption can be displaced in "asymmetries with a controlling public". A group of people can create a kind of open public, they can build alliances, so that a power asymmetry should often be overcome and become less problematic with respect to the privacy discussion. Of course in one-on-one situations this kind of transparency may also be considered harmful with respect to privacy.

Conclusions

This contribution should have made clear that there is a great potential to improve LMS with respect to privacy and data protection. On the one hand laws may give reason for these improvements. Laws and culture are different in countries, so that this is sometimes considered a low priority. On the other hand we see that a learning and education culture based on trust between actors is a desirable goal. The respect for privacy is part of such a culture. Setting up an agenda with priorities for improving LMS, it would look like this:

1. The data collection should be configurable and adjusted to the necessities of the current practice of actual e-learning based courses and lectures. This could be eased by example scenarios with privacy aware configurations
2. Deletion, Anonymisation and data granularity reduction should be applied where possible and made transparent to the users to enhance motivation.
3. It should be visible which data is stored and visible in the platforms to the individual users.

All mentioned improvements are not new from a technological standpoint, but privacy needs higher priority to become implemented. Legal requirements are only one possible reason to pay attention to privacy and data protection, another is students' motivation. "The stupid questions are asked elsewhere anyway."- Learning more about these stupid questions is learning about one's own failures in teaching and helps to improve. Students trust in the privacy of learning platforms is a basis for a feeling for a safe learning environment. Rethinking this may lead to an environment where questions may be asked, teachers never heard before.

References

Bellotti, V.; Sellen, A. (1993). Design for Privacy in Ubiquitous Computing Environments. Third European Conf. Computer-Supported Cooperative Work ECSCW'93 (Milano, Italy), 77-92. Dordrecht, Kluwer.

Brookfield, S. D. (1990). The skillful teacher. San Francisco: Jossey-Bass.

Clement, A. (1993). Working in (and on) the Electronic Fischbowl? Privacy Aspects of Multi-Media Communications. NetWORKing 1993. pp.123-132

Culnan, M. J. & Carlin, T. J. (2009). 'Online Privacy Practices in Higher Education: Making the Grade?', Commun. ACM 52(3), 126-130.

Eckert, C. (2003). Sicherheit und E-Learning. Beitrag zum Workshop „E-Learning: Beherrschbarkeit und Sicherheit". TU Ilmenau. Juli 2003.

Eibl, C.J.: Privacy and Confidentiality in E-Learning Systems (2009). In: Perry, M.; Sasaki, H.; Ehmann, M.; Ortiz, G.; Dini, O. (Eds.): Fourth International Conference on Internet and Web Applications and Services (ICIW 2009). IEEE Computer Society Press, Mai 2009.

Franz, E., Böttcher, A., Wahrig, H., Borcea-Pfitzmann, K. (2006). Access Control in a Privacy-Aware eLearning Environment. In: Proc. of AReS 2006 Workshop on Security in eLearning (SEL), Vienna, 2006.

German Constitutional Court (1984). Court Decision: "BVerfGE 65, 1 – Volkszählung", 1984.

OECD (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD - Organization for economic cooperation and development. 1980.

Rezgui, A.; Bouguettaya, A.; Eltoweissy, M. (2003). Preserving Privacy in the Web: Facts, Challenges and Solutions. IEEE Security & Privacy, Vol. 1, No. 6/2003.

Welch, V., Barton, T., Keahey, K., Siebenlist, F. (2005). Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration, Proc. of the 4th PKI R&D Workshop, 2005.

Spiekermann, S. & Cranor, L. F. (2009). 'Engineering Privacy', IEEE Transactions on Software Engineering, 35(1), pp 67-82.

Acknowledgments

The authors have to thank Marco Ibscher, Volker Riedel and Holger Hansen for their contributions and their dedicated participation in this effort.