Supporting Trust and Engagement in Personalized Learning

Irina Kondratova[1(✉)], Heather Molyneaux[1], and Helene Fournier[2]

[1] Human-Computer Interaction Team, Digital Technologies Research Centre,
National Research Council of Canada, Fredericton, Canada
{Irina.Kondratova,Heather.Molyneaux}@nrc-cnrc.gc.ca
[2] Human-Computer Interaction Team, Digital Technologies Research Centre,
National Research Council of Canada, Moncton, Canada
Helene.Fournier@nrc-cnrc.gc.ca

Abstract. This paper discusses the benefits and challenges associated with supporting learner trust and engagement in personalized learning. Personalized learning refers to instruction in which the pace of learning and the instructional approach are optimized for the needs of each learner. Quality of personalization depends on information collected from the learner and stored in a personal profile. The authors elaborate on research and design solutions to support privacy, trust and engagement in the context of the Learning and Performance Support (LPSS) program at the National Research Council of Canada. The paper builds on earlier work by the authors related to learning personalization, trust and privacy, and on the results of user surveys and usability studies of the LPSS system related to trust, privacy and user engagement.

Keywords: Human-computer interfaces
Technology support for collaboration and learning · Personalization
Trust · Digital ethics · Learner engagement

1 Introduction – Personalized Learning

Personalized learning refers to instruction in which the pace of learning and the instructional approach are optimized for the needs of each learner. Quality of personalization depends on quality of information collected about and from the learner and stored in a personal profile. To support personalization, learning ecosystems collect a great deal of personal data and track learner's activities and context. Information collected frequently includes personal data; social relationships including social networking and preferences for collaboration; emotional and sentiment information; prior knowledge or performance; user activities including browsing history; schedule; interests and preferences; location; physical context information; and current computing devices, etc. [1]. Personal profiles are often mentioned in industry reports in connection with lifelong learning, competency-based education, informal learning, and personalization technologies. There is a growing trend within the corporate learning suites market for providing context aware learning capabilities for the users, indirectly pointing to the growing need for the incorporation of contextual information in the

personal profiles. Gartner [2] suggests: "… by 2018, nearly 50% of learning providers will look to streamline the learner's experience by providing context-aware capability (similar to adaptive learning)."

The two primary components of learning personalization engines are analytics and data; both are required to deliver a personalized experience to the learner. The use of multiple types of analytic tools enable personalization engines to: identify user intent, starting with the search process; detect behavior patterns; identify user's location and discover correlations in behavior among users. Gartner [3] notes that currently "…more sophisticated vendors are moving to "smart" personalization, which incorporates predictive, adaptive learning analytics. Predictive, adaptive analytics is the application of logic and mathematics to data to anticipate future behavior or estimate unknown outcomes. As more data is gathered during the execution process, models are frequently retrained. Smart personalization uses analytics to continually assess what is known about a customer and compares it with what is being learned. These engines continually validate known customer interests and intent or gain new insight about the customer's interests and intent that may not be intuitively obvious. This, in turn, provides a better online experience for the customer."

Personalized learning is an essential part of the learning ecosystem framework. Rosenberg and Foreman [4] define a learning and performance ecosystem as "enhancing individual and organizational effectiveness by connecting people, and supporting them with a broad range of content, processes, and technologies to drive performance."

Based on the literature review related to the personal learning profiles [1, 5], we found that, within the learning ecosystems, the context aware recommendation systems frequently accumulate significant amounts of sensitive data about the learners, including:

- **Basic Personal Information** - identification information, name, contact information, affiliations, authentication information, information on accessibility, including language capabilities and disabilities, and other personal characteristics such as gender, age, profession, and educational level.
- **Knowledge/Performance -** prior knowledge levels of the learner or stored information about measured performance of a learner through the learning material.
- **Interests -** interests or preferences of learners. Values that are typically stored include search terms of the user, user tags, comments and resources created, read, or rated.
- **Learning Goals -** these include the short-term goals, where a learner intends to solve a certain problem, and the long-term goals that are related to a course or plans for lifelong learning.
- **Learning and Cognitive Styles -** examples of different cognitive styles are visual, textual, or auditory presentation of information. Different learning styles affect the presentation of examples, presentation of theoretical knowledge, and practical exercises.
- **Affects -** the use of affective or sentimental information related to the learner.

- **Background -** a common name for a set of features related to the learner's previous experience outside the core domain. Elements typically included are work experience in related areas, religion, and cultural characteristics.
- **Social Relations** - social relations describe social associations, connections, or affiliations between persons. Social relations can contain information about friends, neutrals, enemies, neighbors, coworkers, relatives, and communities, including online communities.
- **Collaboration preferences** - user preferences on collaboration with other users.
- **Location** - learner proximity areas, geographic location, GPS coordinates.

Due to the large amount of sensitive data collected about the user by the system or directly entered by the user into the system, there are significant privacy challenges associated with the implementation of personal learner profiles within learning ecosystems. To alleviate users' privacy concerns, personalized learning technology developers must comply with internal privacy policies within their organizations, adhere to the privacy regulations and legislation in effect in their jurisdictions and make sure that information about data security and privacy protection is available to the users. Making this information transparent improves user trust and data quality. It was found that users will provide more truthful data about themselves if they are informed in advance about privacy measures and are assured that their privacy will be preserved [6].

2 Trust and Learner Engagement

Research demonstrates that the learner engagement in personalized learning is significantly influenced by trust [7, 8]. To create and maintain trust and support learner engagement and positive user experience in learning ecosystems, certain challenges need to be addressed. They include safeguarding privacy of both, learner's personal information and learner's interactions with the system, as well as assuring ethical use of learning analytics. Collection of data about the learner and use of these data face a number of ethical challenges related to acquisition, storage and interpretation of data, informed consent of the learner, privacy and de-identification of data, and classification and management of data. This section of the paper focuses on design principles and ethical considerations for maintaining trust and user engagement in learning ecosystems.

2.1 Design Principles of the Trusted Environments for Learning

The National Research Council Canada began research within the Learning and Performance Support research program (LPSS) in 2014. The program was focused on implementing adaptive and personalization strategies, and developing software components for learning, training, performance support, and enterprise workforce optimization. NRC researchers conducted a literature review of research and development efforts related to trust for connected learning and developed internal LPSS guidelines for addressing trust issues and complying with relevant privacy laws in Canada and abroad [9, 10]. Our literature review identified the following general design principles of the trusted environments for learning [9, 11, 12]:

- **Transparency and Openness:** Provide easy-to-read disclosures to enable learners and other stakeholders to clearly understand who is participating, what the norms and protections are, what data is collected and how it is used.
- **Participation:** Provide opportunities for individual and interest group participation in decision making and policy making related to the development and deployment of connected learning solutions.
- **Data Stewardship:** Find ways to protect data that may include mechanisms to reduce the risk of harm, such as clearly delimiting the permissible uses of data, de-identifying sensitive data and/or deleting data once it no longer has value for learning.
- **Oversight and Enforcement:** Establish regulatory arrangements to protect the integrity of learning networks with competent and appropriately-resourced bodies in place to enforce these principles.
- **Ethical use of learning analytics:** Address ethical challenges to create trust in connected learning. The collection of data and their use face a number of ethical challenges including location and interpretation of data, informed consent, privacy and de-identification of data, and classification and management of data.

2.2   Digital Ethics for Learning Ecosystems

The importance of ethically sound technology design is gaining special attention from researchers. It is not always straightforward. Albrechtslund [13] notices that while the value sensitive design (VSD) process aims to presuppose the connection between the design context and the user context, the designers' intentions do not always correspond with the users' practice; frequently the relation between design and use is very complex and unpredictable. Most often the process of designing technology is also the process of shaping the multitudes of ethical technology use scenarios. Sometimes it is called "front loading of ethics"; the phrase was coined by Jeroen van den Hoven in his keynote address "Values, Design and Information Technology: The front loading of ethics" delivered at ETHICOMP 2005. It refers to the process of shaping the information technology values in the design process.

Digital ethics research is rapidly becoming a prominent topic in big data, data analytics and AI. Gartner report on AI defines [14]: "Digital ethics comprises the systems of values and moral principles for the conduct of electronic interactions between people, businesses and things. Some areas of concern include social and mobile technologies, and social interaction; cloud and security; big data and privacy; autonomous technologies and freedom; artificial intelligence/robotization and the value of work; and predictive algorithms and free will." The 2017 Gartner report on AI [14] puts digital ethics towards the apex of the AI technology hype curve with projected high industry benefits to arise from digital ethics guidelines implementation within the next five to ten years.

Within the learning ecosystems, significant ethical challenges need to be addressed, including protecting privacy of leaner's personal information and assuring ethical use of learning analytics. The collection of learner data and their use face a number of ethical challenges [1]. These challenges are related to location and interpretation of learner's data, informed consent, privacy and de-identification of data, and

classification and management of data. The authors researched the best practices and guidelines for the ethical use of learning analytics, and found a significant number of publications on the topic of ethics for learning analytics. Researchers proposed the following ethical learning analytics framework principles [7, 8, 15–18]:

- **Applying learning analytics as a moral practice**: resulting in understanding rather than measuring.
- **Treating learners as agents**: students should provide informed consent regarding the collection, use and storage of data and also collaborate in providing data and access to data to allow learning analytics to serve their learning and development needs.
- **Considering the learner identity and performance as temporal constructs**: learning analytics provides a snapshot view of a learner at a particular time and context. Data collected through learning analytics should have an agreed-on life span and expiry data, and mechanisms for leaners to request data deletion under agreed upon criteria.
- **Understanding that learner's success is a complex and multidimensional phenomenon**: the data could be incomplete and analysis could be vulnerable to misinterpretation and bias due to imperfect algorithms. Data are always incomplete and dirty and our analyses vulnerable to misinterpretation.
- **Maintaining transparency**: transparency regarding the purposes for which data will be used, under which conditions and who will have access to data, and the measures through which identities will be protected.

2.3   Ethical Considerations for Learning Analytics

Increased use of learning analytics raises a number of ethical and legal issues including privacy concerns [17]. The institutions that use learning analytics tools need to have in place clear guidelines on ethical considerations including the rights and dignity of individuals, and openness about processes and practices [7, 8, 16]. The concerns with learning data mining include significant privacy and data ownership concerns. Griffiths et al. [15] write about the importance of "privacy as a show stopper for learning analytics." "Once the Pandora's Box of data availability has been opened, then individuals lose control of the data about them that have been harvested. They are unable to specify who has access to the data, and for what purpose, and may not be confident that the changes to the education system which result from learning analytics will be desirable" [15] (p. 3). Privacy concerns for both learners and teachers currently prevent wide-spread adoption of learning analytics outside of university research labs. To address this important issue, researchers within the EU LACE (Learning Analytics Community Exchange) project developed a DELICATE checklist for organizations and developers that help them to design and evaluate learning analytics design and implementation [19]. The checklist contains the following eight action points be considered by managers and decision makers planning the implementation of learning analytics solutions [19]:

- Determination – why do you want to apply Learning Analytics?
- Explain – what are the objectives and boundaries?

- Legitimate – why are you allowed to have the data?
- Involve – involve all stakeholders and the data subjects
- Consent – make a contact with the data subjects
- Anonymize – make the individual not retrievable
- Technical aspects – establish procedures to guarantee privacy
- External partners- if you work with external partners, make sure they follow the rules

Ethical concerns with use of learning analytics are numerous and include possibilities for unfair discrimination of data subjects; violation of personal privacy rights; unintended pressure on the users to perform according to some artificial indicators; lack of transparency of the learning analytics systems; loss of control due to AI systems that force certain decisions; the difficulty of fully anonymizing data; problems with safeguarding access to data; data reuse for other purposes; algorithmic logic opaqueness and accountability; data science and black box issues, etc. [15, 19, 20].

The authors' research experience in the area of MOOCs and Personal Learning Environments has provided both bigger and richer datasets than ever before, with powerful tools to visualize patterns in the data, especially on digital social networks [21, 22]. The work of uncovering such patterns, however, has provided more questions than answers from the pedagogical and technical contexts in which the data were generated. In trying to understand why MOOC participants produced the data that they did, a critical reflection was also prompted regarding what big data, educational data mining, and learning analytics could and could *not* tell us about complex learning processes and experiences. Boyd [23] expressed it in the following way:

> Much of the enthusiasm surrounding Big Data stems from the opportunity of having easy access to massive amounts of data with the click of a finger. Or, in Vint Cerf's words, "We never, ever in the history of mankind have had access to so much information so quickly and so easily." Unfortunately, what gets lost in this excitement is a critical analysis of what this data is and what it means (p. 2).

Open learning environments combined with powerful data analysis tools and methods bring new affordances and support for learning. They also highlight important ethical issues and challenges that move learners from an environment characterized by human communication to one that includes technical elements over which the learner has little or no control.

The dynamic pace of technological innovation, including educational data mining and learning analytics also requires the safeguarding of privacy in a proactive manner. In order to achieve this goal, researchers and system designers in the fields of educational data mining and advanced analytics must practice responsible innovation that integrates privacy-enhancing technologies directly into their products and processes [24]. According to Oblinger [25], "Analytics is a matter of culture — a culture of inquiry: asking questions, looking for supporting data, being honest about strengths and weaknesses that the data reveals, creating solutions, and then adapting as the results of those efforts come to fruition" (p. 98).

In dealing with so much data and information so quickly, our role as researchers was to envisage the optimal processes and techniques for translating data into understandable, consumable, or actionable modes of representation in order for results to be

useful and accessible for our end users to digest. The ability to communicate complex ideas effectively was critical in producing something of value that translated research findings into practice. Questions have been raised about how stakeholders in the educational process (i.e., learners, educators, and administrators) might access, manage, and make sense of all these levels of information effectively. Educational data mining and learning analytics methods hint at how automated data filtering and analysis could do exactly that.

Rich inferences about learning and learners were made from the large data sets available from our research on MOOCs and PLEs but also raised many new interesting research questions and challenges in the process. Researchers must strive to demonstrate how the data are meaningful, as well as appealing to various stakeholders in the educational process while engaging in responsible innovation with thoughtful research designs and implementations [26].

With this in mind, we strongly recommend that those designing and building next generation analytics ensure that they are informed by Privacy by Design. This entails mindfulness and responsible practice involving accountability, research integrity, data protection, privacy, and consent [24, 27]. The line between private and public data is increasingly becoming blurred as more opportunities to participate in open learning environments are created and as data about participants, their activities, their interactions, and their behaviours are made accessible through social media, such as Facebook, Twitter, Google, and potentially any other social media tool available online. In the context of big data from MOOCs and PLEs, we agree with the European Data Protection Supervisor [28] who states that "People want to understand how algorithms can create correlations and assumptions about them, and how their combined personal information can turn into intrusive predications about their behaviour" (p. 10).

Significant questions about truth, control, transparency, and power in big data studies also need to be addressed. Pardo and Siemens [7] maintain that keeping too much data (including student digital data, privacy-sensitive data) for too long may actually be harmful and lead to mistrust of the system or institution that has been entrusted to protect personal data. Discussions around the ethics of big data and learning analytics have underscored important methodological concerns related to data cleaning, data selection and interpretation [29]. The invasive consequences of data analytics, as well as the potential dehumanizing effects of replacing human communication and engagement with automated machine-learning algorithms and feedback are ethical priorities currently being investigated by industry and academics involved in responsible innovation. Global ethics initiatives, including IEEE Standards Association and the UK Engineering and Physical Sciences Research Council [30] are now embedding ethics into the design of processes for machine-learning, AI, and autonomous systems with research guidelines that encourage innovators to "anticipate, reflect, engage and act" in ways that promote opportunities for science and innovation that are socially desirable and undertaken in the public interest (p. 162).

Furthermore, we should not underestimate the fact that most of the algorithms currently in use were produced for economic gain and not necessarily to enhance deeper levels of learning or add value to society. Kitchin [31] claims that "Software is not simply lines of code that perform a set of instructions, but rather needs to be understood as a social product that emerges in contingent, relational and contextual

ways, the outcome of many minds situated with diverse social, political and economic relations" (p. 5). Clearly, the development of automated algorithm systems has another inherent problem wherein it might be hard to point a finger towards who is responsible when things go wrong.

Researchers and developers must be mindful of the affordances and limitations of big data (including data mining and predictive learning analytics) in order to construct useful future directions [32]. Researchers should also work together in teams to avoid some of the inherent fallacies and biases in their work, and to tackle the important issues and challenges in big data and data-driven systems in order to add value to the educational process.

3   LPSS Design Considerations

The National Research Council of Canada (NRC)'s Learning and Performance Support (LPSS) program implements adaptive and personalization strategies and develops software components for learning, training, performance support and enterprise workforce optimization. These technologies are designed to benefit NRC clients and their users by: facilitating lifelong learning, reducing learning and training costs, reducing demands on physical infrastructure, enabling streamlined and rapid skill development, reducing time to competency, supporting informal, personal and personalized learning, increasing learner engagement, optimizing sustainable workforces, and increasing operational performance and productivity [33].

LPSS goal is to improve efficiency of training by using learning records and performance analytics to recommend the most useful learning services and resources specific to workplace environments and competency profiles. LPSS tools originated as a web-based prototype open to the public at lpss.me that offers personal rather than personalized learning. The prototype lpss.me was active from the Fall 2014 to the Fall of 2016.

The LPSS pilot site lpss.me was developed with learner privacy and trust in mind. The personal learner profile (see Fig. 1) enabled the user to choose preferences for connecting with other users, recording learning activities and consenting to LPSS research. The LPSS research consent form explained to the users LPSS research data collection process, what data is being collected, for what purpose, data privacy and confidentiality. A separate information on privacy of data was provided to the LPSS users in the "About" section of the LPSS menu (Fig. 2).
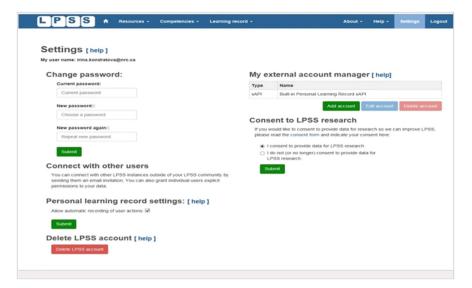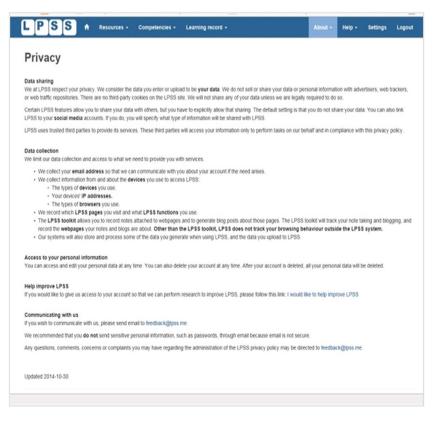
Fig. 1. LPSS learner profile

Fig. 2. LPSS privacy page

4 User Feedback on LPSS

User feedback on functionalities within LPSS, including privacy concerns, was elicited via an online survey of lpss.me users and through users' responses to questions regarding LPSS functionality in the course of the remote usability testing of lpss.me conducted in February of 2016.

4.1 Online Survey

This section draws upon the findings of the survey sent out to lpss.me users between April 2015 and October 2016. Survey invitations were sent out to lpss.me participants 1–2 weeks after users first logged into the system, with a reminder email sent one week after the initial survey request. In total 141 were invited to take part in the survey with 28 participants responding.

The users represented in the survey responses are "super users" of elearning tools and system; they represent a well-educated mature demographic highly involved in the field of elearning. 62.96% of respondents (17) reported being fifty years or older. The majority of the survey respondents (77.78% - 21) reported having a graduate degree, with more than 20 years of work experience (74% - 20) and/or have had more than 11 years of experience with online learning (64.28% - 18). The findings of this survey are not representative of the general population but offer sample viewpoints from power users within the elearning community.

The survey asked 25 questions including demographic questions as well as questions about LPSS functionality and information pages. Of those 25 questions, 4 questions were relevant to user privacy.

Survey participants were asked "Have you read any of these LPSS information pages" - a list which included the LPSS "terms and conditions" and "privacy" pages. These two pages were the least read pages in the LPSS system, with 24.14% (7 respondents) and 20.69% (6 respondents) users respectively stating they did not look at the terms and conditions and privacy pages (see Tables 1 and 2).

Table 1. Responses regarding reading information on LPSS terms and conditions page

Question: Have you read terms and conditions page?	
Response	% of respondents
Yes, read it in detail	34.48
Glanced at it	34.48
Did not look at it	24.14
Not sure	6.9

Survey respondents were then asked a follow up question related to privacy: "In general, do you have any concerns about information privacy or data privacy (or data protection) with regards to the collection and sharing of your personal data, technology,

Table 2. Responses regarding information on LPSS privacy page

Question: Have you read privacy page?	
Response	% of respondents
Yes, read it in detail	31.03
Glanced at it	41.38
Did not look at it	20.69
Not sure	6.9

and the legal and political uses surrounding them?" Surprisingly a large number of users (48.28%, 14 respondents) responded that they had no concerns (see Table 3). As a follow up question, survey respondents were asked to "Please share your thoughts about privacy and the LPSS privacy page". Twelve survey respondents answered this optional question (see Table 4 for responses). Luckily, the optional text answers shed light on user responses (Table 4).

Table 3. Responses regarding information and data privacy

Question: In general, do you have any concerns about information privacy or data privacy (or data protection) with regards to the collection and sharing of your personal data, technology, and the legal and political uses surrounding them?	
Response	% of respondents
Yes	34.48
No	42.28
Not sure	17.24

For the most part, respondents noted that they trusted NRC over other agencies, and that they were comfortable using the system because it does not require information they consider to be personal or valuable; however, they mentioned that if the system changed to require more personal information or began to share information outside the institute then their attitudes about privacy and LPSS would change.

4.2   Feedback from Users in Remote Usability Testing

Usability evaluation of the LPSS platform was conducted in February 2016 using remote usability software. The users who signed onto lpss.me within the period from December 2014 to December 2015 were invited via email to participate in the usability testing. An invitation email was sent to 150 users of lpss.me, with the reminder email

Table 4. User thoughts about privacy and the LPSS privacy page

Question: Please share your thoughts about privacy and the LPSS privacy page
I have no concern why not write anything of value in this system
I feel I'd like to research the differences
I have to put too much personal information into the system as of yet. I would be cautious if I was asked for more personal information
It could be interesting to have information about: - the location of the data hosting. - the treatment of anonymity -The page is easy to understand and can be commended for its transparency. However, privacy is a tricky issue as the actual risks and benefits are difficult to assess. The fact that LPSS doesn't use browser trackers (unlike, say, SurveyMonkey) does inspire trust. But ensuring privacy can also happen through users having private access to their own data
My general concern is with regard to making my data available outside of the program/organization without my consent or without power to decline consent. The page as it is written seems clear about the nature of usage of my data and allays my concerns
Makes sense - sufficiently lightweight and clear. It might be helpful to clarify what is shared with whom, concretely rather than in these fairly generic terms
If you buy in to the service you buy into the terms -ok - I trust NRC and that's enough for me
I could not accept to participate in the research due to the wording of Terms and Conditions that may imply that you would do data mining on my email account
Sounds more sincere than most commercial privacy statements
My greatest concern concerning data is the linking to my external cloud accounts and online learning accounts such as Coursera

sent a week later. During the study period 16 participants clicked on the study link in the invitation email; out of these 16 people, three users completed the study (P1, P2 and P3). Two other users (P4 and P5) provided some responses to questions but did not complete the study.

The study involved users performing mandatory tasks within lpss.me and answering task-related and general questions on lpss.me use, as well as several demographic questions. The study contained some regular lpss.me tasks that users were asked to complete, for example: access the menu "Resources" and add one source of information. The questions that users were asked to respond to were either within a text box or Likert scale questions with radio buttons.

At the end of the usability study participants were asked a series of general questions about the system, including would they use it, which features they liked the most, and which features are useful for learning or for doing their job, and would they recommend this website to a friend or colleague. The users who were able to do all the tasks provided some useful responses that push the system further towards greater functionality (see Tables 5 and 6 for participants' responses).

Two of the suggestions in the above Table 6, reflecting the user's stage of career and linking to the users' publications or other demonstrations of competencies, point towards making the LPSS system more personal and adaptive to a broader audience. However, the participant P2 states that the LPSS system is not a truly personal environment and since it doesn't have the flexibility that the term personal environment

Table 5. Usability study responses, positive LPSS system attributes

Participant	Would you use it? (LPSS)	Most liked features	Usefulness for learning or job
P1	I agree with the basic premise of taking ownership of my learning and learning record. Still an issue in that ownership is still not mine but the property of NRC	The potential is interesting	Possibly if employers and recruiters could find my profile and offer me employment or at least accept this as a CV
P2	I would, but I would like to have the opportunity to be able to showcase my competencies and abilities	Competencies. Easy to add	I think so. The tool is great to force you to reflect on your career

Note: P3 did not respond to these questions.

Table 6. Usability study responses, issues and suggested improvements

Participant	Less useful features	Useful features and suggestions	Issues with features or navigation
P1	I'm in late career, nothing reflects that context	Link to my publications or similar demonstrations of competencies	Not really, although some brief multimedia tutorials could be helpful
P2	I do not know	No, I have not	No, I did not
P3	idem	Please provide a survey in French	A personal environment, in my opinion, is not built in a platform like LPSS. It is built in a personal space, with all the flexibility that this implies

implies. Even though the users did have some issues with using the LPSS dashboard and understanding the content of some menu tabs, when asked if they would recommend the LPSS system to a friend or a colleague, two of the three responded yes, while the third, the participant who was unable to access their lpss.me account said maybe. The final question asked for additional comments or suggestions, to which one user said they were "looking forward to future developments of LPSS." Another user stated that in order for LPSS to be a truly personal learning environment they felt that LPSS should be on the personal computer of the user and not on a web-based platform that may disappear one day.

5 Conclusions - Design Considerations for Learner Engagement and Trust

The generation, accumulation, processing, and analysis of digital data is often touted as a potential solution for many prevailing educational or training problems, however research points to important cautions with regards to truth, control, transparency and power in learning analytics and big data which still need to be addressed.

This paper builds on earlier work by the authors related to learning personalization, trust and privacy, and on the results of user surveys and usability studies of the LPSS system related to trust, privacy and user engagement. Of importance is that learner engagement in personalized learning is significantly influenced by trust. Researchers are currently working with massive amounts of data in order to enhance the learning experience and to personalize learning with powerful visualization, dynamic dashboards, and customized drop-down menus with personalized recommendations for learning materials and resources. Usability studies and feedback from LPSS users point to important design considerations with regards to learning personalization, system functionalities, learner engagement and trust.

Discussions around big data ethics have underscored serious methodological concerns related to data cleaning, data selection and interpretation, the invasive potential of data analytics, as well as the potential de-humanizing effects of replacing human communication and engagement with automated machine-learning algorithms and feedback. Keeping too much data, including learner's digital privacy-sensitive data, for too long may actually be harmful and lead to mistrust of the system or institution that has been entrusted to protect personal data. Within LPSS, a literature review informed the development of internal LPSS guidelines for addressing trust issues which comply with relevant privacy laws in Canada and abroad.

Researchers and developers must be mindful of the affordances and limitations of big data, including data mining and predictive learning analytics, in order to construct useful future directions. Working together in teams, whether in industry or academia, should allow researchers to address the inherent fallacies and biases in their work, to tackle the important issues and challenges in big data and data-driven systems in order to add value to the learning and performance support process.

New and emerging technologies in open learning environments and access to an abundance of resources in learning ecosystems, as well as new methods for combining data from personal learning, work, and social environments enable the ability of adaptive learning software to close the loop between learning and performance support; however, important issues and challenges still need to be addressed to improve learner's trust in the learning ecosystem. These remaining issues and challenges pave the way for important future research directions to emerge.

References

1. Lapointe, J.-F., Kondratova, I., Molyneaux, H., Shaikh, K., Vinson, N.G.: A review of personal profile features in personalized learning systems. In: Andre, T. (ed.) AHFE 2017. AISC, vol. 596, pp. 46–55. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60018-5_5

2. Gartner G00300423: Market Guide for Corporate Learning Suites. Gartner report (2016)

3. Gartner G0026299520: Market Guide for Digital Personalization Engines. Gartner report (2016)

4. Rosenberg, M.J., Foreman, S.: Learning and performance ecosystems. Strategy, Technology, Impact, and Challenges. The ELearning Guild, White paper (2014). http://www.elearningguild.com/publications/?id=53

5. Kondratova, I., Molyneaux, H., Lapointe, J-F.: Personal profiles project: literature and market/commercial review, Internal LPSS report (2016)

6. Elmisery, A.M., Seungmin, R., Botvich, D.: Collaborative privacy framework for minimizing privacy risks in an IPTV social recommender service. Multimed. Tools Appl. **75**, 14927–14957 (2016)

7. Pardo, A., Siemens, G.: Ethical and privacy principles for learning analytics. Br. Educ. Res. Assoc. **45**(3), 438–450 (2014)

8. Siemens, G.: Learning analytics: the emergence of a discipline. Am. Behav. Sci. **57**(10), 1380–1400 (2013)

9. Kondratova, I.: Trusted environments for learning: design guidelines. Internal LPSS report (2015)

10. Vinson, N.: Privacy laws applicable to LPSS. Internal LPSS report (2014)

11. The Aspen Institute Task Force on Learning and the Internet: Report on the Learner at the Center of a Networked World (2014). www.aspentaskforce.org

12. Diaz, V., Golas, J., Gautsch, S.: Privacy considerations in cloud-based teaching and learning environments. EDUCAUSE ELI Paper, 3 (2010)

13. Albrechtslund, A.: Ethics and technology design. Ethics Inf. Technol. **9**(1), 63–72 (2007)

14. Gartner G00314732: Hype cycle for artificial intelligence. Gartner report (2017)

15. Griffiths, D., Drachsler, H., Kickmeier-Rust, M., Hoel, T., Greller, W.: Is Privacy a Show-stopper for Learning Analytics? A Review of Current Issues and Solutions. Learning Analytics Review 6, LACE (2016)

16. Slade, S., Prinsloo, P.: Learning analytics: ethical issues and dilemmas. Am. Behav. Sci. **57** (10), 1509–1528 (2013)

17. Welsh, S., Mckinny, S.: Clearing the fog: a learning analytics code of practice. In: Reiners, T., von Konsky, B.R., Gibson, D., Chang, V., Irving, L., Clarke, K. (eds.) Globally Connected, Digitally Enabled, Proceedings of the Ascilite 2015 in Perth, pp. 241– 245 (2015)

18. Ashman, H., Brailsford, T., Cristea, A.I., Sheng, Q.Z., Stewart, C., Toms, E.G., Wade, V.: The ethical and social implications of personalization technologies for e-learning. Inf. Manag. **51**(6), 819–832 (2014)

19. Drachsler, H., Greller, W.: Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In: Proceedings of the Sixth International Conference on Learning Analytics & Knowledge, pp. 89–98. ACM (2016)

20. Buckingham Shum, S., Crick, R.D.: Learning analytics for 21st century competencies. J. Learn. Anal. **3**(2), 6–21 (2016)

21. Fournier, H., Kop, R.: MOOC learning experience design: issues and challenges. Int. J. E-Learn. **14**(3), 289–304 (2015)

22. Fournier, H., Kop, R., Durand, G.: Challenges to research in MOOCs. J. Online Learn. Teach. **10**(1) (2014). http://jolt.merlot.org/vol10no1/fournier_0314.pdf
23. Boyd, D.: Privacy and Publicity in the Context of Big Data. WWW. Raleigh, North Carolina, 29 April 2010. Accessed http://www.danah.org/papers/talks/2010/WWW2010.html
24. Cavoukian, A., Jonas, J.: Privacy by design in the age of big data (2012). Accessed https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf
25. Oblinger, D.G.: Analytics: What we're Hearing. Educause (2012). Accessed http://er.educause.edu/articles/2012/11/analytics-what-were-hearing
26. Berland, M., Baker, R.S., Blikstein, P.: Educational data mining and learning analytics: applications to constructionist research. Tech. Know Learn. **19**, 206–222 (2014)
27. Cormack, A.: A Data Protection Framework for Learning Analytics. Community.jisc.ac.uk (2015). Accessed http://bit.ly/1OdIIKZ
28. European Data Protection Supervisor: Leading by Example: the EDPS Strategy 2015–2019 (2015). https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Strategy2015
29. Boyd, D., Crawford, K.: Critical equations for big data. Inf. Commun. Soc. **15**(5), 662–679 (2012). https://doi.org/10.1080/1369118x.2012.678878
30. Yuste, R., Goering, S.: Four ethical priorities for neurotechnologies and AI. Nature **551**, 159–163 (2017)
31. Kitchin, R.: Foreword: education in code/space. In: Williamson, B. (ed.) Coding/Learning, Software and Digital Data in Education. University of Stirling, Stirling (2015). Accessed http://bit.ly/1NdHVbw
32. Fenwick, T.: Professional responsibility in a future of data analytics. In: Williamson, B. (ed.) Coding/Learning, Software and Digital Data in Education. University of Stirling, Stirling (2015). Accessed http://bit.ly/1NdHVbw
33. Kondratova, I., Molyneaux, H., Fournier, H.: Design considerations for competency functionality within a learning ecosystem. In: Zaphiris, P., Ioannou, A. (eds.) LCT 2017. LNCS, vol. 10295, pp. 124–136. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58509-3_12