Anonymisation and Synthetic data approaches to minimise privacy risks in highly scaled LA intervention driven infrastructure

Alan Mark Berg
University of Amsterdam
a.m.berg@uva.nl

Jarno Vrolijk
University of Amsterdam
j.vrolijk@uva.nl

Stefan T. Mol
University of Amsterdam
s.t.mol@uva.nl

Ashley Fisher
University of Amsterdam
a.j.fisher@uva.nl

ABSTRACT: Higher Education's response to COVID included an accelerated rush to scale online learning and related services. Online services generate digital traces that once processed trigger Learning Analytic Interventions. There are numerous reasons to anonymise or pseudo-anonymise the traces. For example, synthetic or anonymised data may be used to mininse ethical, legal, and privacy risks associated with the release of data to infrastructure developers, LA practitioners, and Lecturers. During this hackathon we will review best practices, algorithms, and architectural design patterns. Furthermore, we will discuss trade-offs, such as traceability of individuals and usability for analysis.

Keywords: Anonymisation,Intervention, Infrastructure, xAPI, Caliper,PII, Scalability

1 Background

A review of the demand for realistic synthetic data to minimise risks in the practicalities of deploying Learning Analytics (Berg, Mol, Kismihók, & Sclater, 2016) also indirectly highlights the needs for generic, scalable, well designed, and reusable anonymisation and/ or pseudonymisation services. Highly scaled Infrastructures such as those developed by JISC (Sclater, Berg, & Webb, 2015) depend on standardizations at the protocol level, for example, xAPI for the collection of digital traces. However, there is confusion in the market over similarly targeted protocols such as Caliper. This confusion has previously led to a call known as the *Edinburgh Statement* by LA researchers for standards bodies to work more closely together and converge their specifications. Both the xAPI and Caliper protocols are related to particular architectural components such as a queryable digital trace collection and storage points often known as Learning Record Stores (LRS). Learning Management Systems (LMS) such as The University of Amsterdam's Canvas and the Hogeschool van Amsterdam's Brightspace environments contain a myriad of information relating to utilisation of these platforms by both learners and teachers alike. The use of this LMS data within an LRS provides insight to empower an individual in their learning, in addition to providing teachers the ability to adapt to the needs of their students or enact an intervention. Over the course of time technology has improved and the feature sets, terminology, and usability of commercial LRS's have also progressively increased. An LRS has the ability to be deployed in the cloud, on premise, or in a hybrid fashion. The data stored is related to the individual and the results of querying and degree of disclosure should depend on the role of the agent conducting the queries, as seemingly harmless information can be repurposed for de-anonymization by cross-referencing the data with other data-sources to re-identify individuals (Sweeney, 2002). Further, depending upon the context such as a student looking at a dashboard or an Infrastructure specialist wanting to test their designs, the data the audience requires is either synthetic, fully disclosed, pseudonymised, or anonymised at the group or other aggregation level (albeit by suppression, generalization and/ or perturbation). As in accordance with the European Union's General Data Protection Regulation (GDPR), which demands that stored data on people is either anonymised or pseudonymised. In the era of LA interventions, a standardised, plugable, minimiser of sensitive- and/ or quasi-sensitive identifiers based on either generalization, suppression and/ or perturbation methods can help lowering scalability risks for online learning by protecting identities and attributes from being disclosed (Li, Li & Venkatasubramanian, 2007).

2 Research Question

The research question provided next is deliberately open ended so that the teams have a wide permit to evaluate. The focus is on processes, methods, algorithms, design patterns, advice, architectural artifacts such as extra components to support the filtering of data as an LRS is queried, and requirement analysis aimed at tackling privacy related obstacles in the collection, curation, storage, and analysis of data that are relevant to learning analytics.

How do we minimise privacy sensitive information within the context of a standardized, highly scaled LA infrastructure?

3 Expected outcome

We will work within teams and agree on the specific focus depending on a review of the opportunities at the beginning of the workshop. Data, python code, and a reading list reflecting the current state of the art will be provided via a public Github repository. Outputs generated will be placed in the repository and publicly available with annotations.

We open our arms to any interested party. Please bring along your own problems, infrastructure, data, and code. The more intractable the issue the better. Early communication with the organisers (email at top of proposal) are most welcome.

REFERENCES

Berg, A. M., Mol, S. T., Kismihók, G., & Sclater, N. (2016). The Role of a Reference Synthetic Data Generator within the Field of Learning Analytics. *Journal of Learning Analytics*, *3*(1), 107–128. https://doi.org/10.18608/jla.2016.31.7

Edinburgh Statement for Learning Analytics Interoperability (2016) https://docs.google.com/document/d/18VJ9hVcfk9sOzs2MEeZ59Q5RSz1jZnUHzSWFSednEXg/edit#heading=h.votza0o0t5xa

Li, N., Li, T., & Venkatasubramanian, S. (2007). t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering* (pp. 106-115). IEEE.

Sclater, N., Berg, A., & Webb, M. (2015). Developing an open architecture for learning analytics. Proceedings of the EUNIS 2015 Congress. https://doi.org/ISSN. pp. 2409–1340.

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 571-588.