International **R**eview of **R**esearch in **O**pen and **D**istributed **L**earning
Volume 19, Number 5

November – 2018

User Consent in MOOCs – Micro, Meso, and Macro Perspectives

Mohammad Khalil[1], Paul Prinsloo[2], and Sharon Slade[3]
[1]University of Bergen, Norway, [2]University of South Africa, Unisa, South Africa, [3]The Open University, UK

Abstract

While many strategies for protecting personal privacy rely on regulatory frameworks, consent, and anonymizing data, they are not always effective. Terms and Conditions often lag behind advances in technology, software, and user behaviours, and consent to use data for a range of unclear purposes may be provided unwittingly. As the commercial market for (student) data expands, so does the number of brokers who move, share and sell data across continents and legislative environments. This paper reviews four Massive Open Online Course (MOOC) providers from different geopolitical and regulatory contexts. It explores how consent to collect and use data is described to potential users, and how that consent applies at micro, meso, and macro levels.

This paper proposes a need for greater transparency around the implications of users granting consent at the point of registration. Further, it highlights that though MOOC providers have a responsibility to make clear the potential uses and sharing of user data, users themselves should also be more aware and consider how meaningful student agency can be achieved.

Keywords: consent, massive open online course (MOOC), micro, meso, macro, privacy, policy

Introduction

Within the broader context of discourses surrounding Big Data, educational providers are increasingly collecting, analysing, and using student information (Papamitsiou & Economides, 2014). Data are collected for marketing purposes and operational planning, to personalise the learning experience, and to determine the allocation of resources to individual students based on demographic and behavioural data (Gašević, Dawson, & Siemens, 2015; Leitner, Khalil, & Ebner, 2017; Long & Siemens, 2011b). There are increasing concerns regarding the expanding marketplace for student data (Russell, Reidenberg, Martin, & Norton, 2018) and the ability of big companies (e.g., Facebook) and data brokers to move user data outside the confines of new legislation (Hern, 2018). The introduction of the General Data Protection Regulation (GDPR) has vast implications for users' understanding of the purpose of the collection, analysis and use of their data, and user consent (Slade & Prinsloo, 2013; Khalil, Prinsloo, & Slade, 2018; Prinsloo & Slade, 2015; Sclater, 2018). While giving permission for the use of personal data has long been an issue for both end users and service providers, establishing user consent is complex given changes in international data regulation environments, growing concerns about privacy and the commercialisation of user data, and challenges in overseeing and regulating data exchanges and downstream use by a range of data brokers, collectors, platforms, and markets (Bennett, 2018; Cormack, 2016; Fairfield, 2017; Sclater, 2018; Tene & Polonetsky, 2012).

While student privacy and the use of student data on institutional learning platforms is relatively well-researched, there is little published research on the nature, scope, and implications of user consent in distributed learning environments such as MOOCs (Khalil, Prinsloo, & Slade, 2018; Drachsler & Kalz, 2016). Related research includes research by Young (2014) on the implications of the Family Educational Rights and Privacy Act (FERPA) for educational privacy in online classrooms, and research by Bennett (2018) on the potential of GDPR to be an "instrument for the globalisation of privacy standards" (p. 1). Sclater (2018) provides clear guidelines regarding the scope and practicalities surrounding user consent in the light of GDPR, though does not address its implications for *cross-border transfer* of student data. In online education, privacy can no longer be regarded as a *domestic* problem given "the increasing ease with which personal data might be transmitted across borders" (Bennett, 2018, p. 2), and the potential of data owners to move data beyond the reach of changing legislation (Hern, 2018).

In this paper, we consider the definition and scope of MOOC consent on three levels - the *micro level* of user or student consent; the *meso level* describing agreements between host institution and MOOC provider (e.g., regarding ownership of material, ownership/access to student data); and the *macro level* involving consent relating to external players (e.g., for access to the resources and data of a particular MOOC platform or course by others not directly involved in the MOOC). We critically consider these three different layers of consent by reviewing the practices of four MOOC providers from the United States and Europe, flagging issues for further consideration.

This study attempts to broaden the notion of consent beyond uses of student data for *learning* purposes. We propose that consent also includes uses of student and/or institution-generated *content,* as well as provision for the collection of student behavioural data for purposes outside the original *domestic* context for which consent was provided.

Mapping Consent in the Micro, Meso, and Macro Contexts of MOOCs

User Consent in Higher Education: A Brief Introduction

Collecting, analysing, and using student data has always been a part of (higher) education ranging from, inter alia, using formative and summative assessments as data to inform interventions and/or report on student progress, to automated recommender systems personalising student feedback and support. Traditionally, *user consent* for the collection, analysis and use of data was implied when students accepted the Terms and Conditions of the service provider. As Sclater (2018) indicates, most of the data currently collected, analysed, and used are lawful in terms of the institution's legitimate interests, or "necessary to fulfil your legal contractual obligations with the student" (Sclater, 2018, par. 6). There are two exceptions: Collecting, analysing, and using special category or sensitive data (e.g., ethnic origin) requires explicit, additional consent *before* the data are collected. Consent is also needed when specific interventions will be made to students' learning experience (e.g., additional assessment or alternative courses) based on their analytics (See Sclater, 2018; the European TeSLA project [http://tesla-project.eu/]).

With the increasing move towards online learning across borders and the proliferation of data brokers, service providers, and inter-institutional agreements, as well as an increasingly expanding market for student data (Russell et al., 2018), the consent students provide at the point of first registration has potentially far-reaching and unforeseen consequences.

User Consent as Layered

Until the emergence of learning analytics as a deliberate process to inform pedagogy at a student and faculty level, aggregated student data were used to inform functions such as funding, quality assurance, and policy, in what became known as *academic analytics* (for a full discussion see Long & Siemens, 2011b). Another way to distinguish between the uses and audiences of learning analytics is to reference three levels - namely *micro* (individual user actions); *meso* (institution-wide application and use); and *macro* (region/state/national/international) levels (Buckingham Shum, 2012). The micro level correlates with the definition by Long and Siemens' (2011b) that learning analytics is distinct from academic analytics, in that the latter is used by management for reporting and strategic planning purposes. In contrast to academic analytics, learning analytics is of "primary interest to *learners themselves*, and *those responsible for their success*, since it can provide the *finest level of detail*, ideally as *rapidly as possible* [emphasis added]" (Buckingham Shum, 2012, p. 3). At the meso level, Buckingham Shum (2012) defines academic analytics as learning analytics used alongside business intelligence, primarily to inform and optimise workflows and business processes. Macro-level analytics apply at an inter-institutional level and can be used for "'maturity surveys of current institutional practices or improving state-wide data access to standardised assessment data over students' lifetimes" (p. 3).

User Consent in MOOCs

Khalil, Taraghi, and Ebner (2016) argued that the use of learning analytics in MOOCs drives questions related to privacy, transparency, and consent. With a central focus on consent, this paper suggests implications for the scope and nature of consent for each of the levels of learning analytics, illustrated by the consent that students provide when registering for a MOOC (micro level). We consider how this consent is affected by the agreements of the content provider (e.g., a higher education institution) with

the MOOC platform (e.g., FutureLearn; meso level). And finally, the implications of the initial consent provided by students on the scope and nature of the sharing of personal data between the MOOC platform provider and other data stakeholders are explored in the context of the stipulations and guarantees (or lack of) in the MOOC's privacy or data-sharing documents (macro level).

Figure 1 illustrates the range of stakeholders and some of the actions taken at each of the micro, meso, and macro levels (A-C). Point A illustrates the stage (micro level) at which students enter into an agreement with an educational provider by accepting the Terms and Conditions. Students consent not only to have their *data* collected, analysed, and used, but may also cede the copyright and ownership of the *content* they produce on these platforms. The Terms and Conditions are, in turn, influenced both by factors in a given geopolitical context and regulatory environment, and by the purpose of the collection, analysis, and use of user data by the learning platform provider (e.g., FutureLearn).

Point B illustrates the boundary between the higher education institution as the MOOC *content and teaching* provider, and the MOOC *platform* provider (meso level). At this point, there is consent from the content and teaching provider to have *content* and *teaching* hosted on the platform. Additionally, there may also be agreement that allows the platform to harvest information from the instructors and for the teaching institution to cede the copyright of the materials. On a meso level, we may also find other complexities – for example, where the providing institution and the platform provider are in different geopolitical contexts governed by different regulatory frameworks and legislation.

The macro level (Point C) maps how the *initial* student consent at micro-level (Point A) may play out in the nexus between the MOOC *platform* provider and other data stakeholders. While third-party use is often included in the Terms and Conditions of MOOCs (Prinsloo & Slade, 2015), there are increasing concerns about the range of actors, whether human or algorithmic, having access to the content and data on these platforms, and who analyses and uses the data, often outside the scope and declared purpose of the initial consent provided by students at the point of registration (Point A).

In the light of this layered "lattice of information networking" (Solove, 2004, p. 3), it is important then to investigate the nature and scope of user consent at the initial point of contact (Point A), and how that notion of consent changes from micro and meso to the macro level.

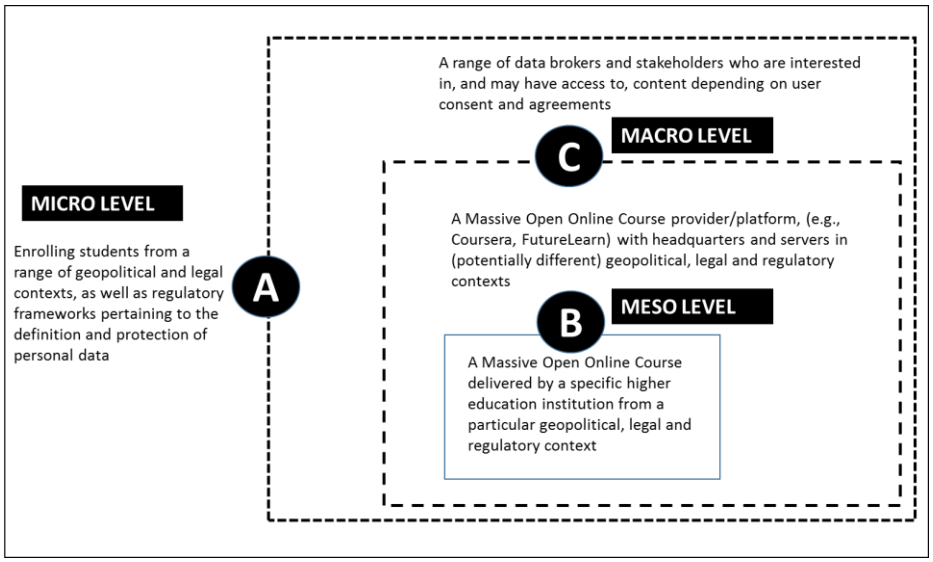

Figure 1. Mapping the micro, meso, and macro-levels of consent in MOOCs.

At the micro level (Point A), the issue of consent pertains specifically to the collection, analysis, and use of student data in learning analytics.

Learning analytics was initially defined as "the use of intelligent data, learner-produced data, and analysis models to discover information and social connections, and to predict and advise on learning" (Siemens, 2010, as cited in Ferguson, 2012, p. 9). Later, the Society for Learning Analytics Research (SoLAR) refined this to "the measurement, collection, analysis, and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs" (Long & Siemens, 2011a). In the context of the collection, analysis, and use of student data, the issue of consent is a constant, however relatively, marginal issue (Prinsloo & Slade, 2017; Sclater, 2017a; Slade & Prinsloo, 2013).

Much of the current research on student consent refers to the context of higher education, and specifically, institutional learning management systems (Siemens, 2013). Consent in the context of MOOCs is less researched (Young, 2014). Typically, MOOCs are open to a broad set of students enrolling from a range of geopolitical, legal, and regulatory frameworks. Students from these different contexts and regulatory frameworks will have different epistemologies and cultural capital. The assumptions underpinning their understanding of "consent," privacy, and risk, will therefore vary. On a meso level (Point B) we need also consider the potentially different geopolitical, legal, and regulatory frameworks within which the content-provider (e.g., a university) and the host MOOC platform (e.g., Coursera, FutureLearn) operate. Consent here not only implies agreement related to educational content, but also to copyright, and responsibilities to ensure that course outcomes and materials are updated and of good quality. There may also be issues with how the behavioural data of course instructors are regarded by MOOC platform providers.

At a macro level (point C), MOOC platform providers may wish to share data (and content) on their servers with official entities (e.g., legal enforcement agencies and government), and with (un)specified data brokers and commercial entities. The macro level could also refer to a learner (micro level) enrolment in an institution's offering (meso level) via a social media account (macro level). In such cases,

with data flows between the social media platform (e.g., Facebook), the MOOC platform provider and the institution offering the course, consent becomes a potential minefield.

Consent at the Micro Level

Given increasing concerns around privacy and surveillance, coupled with changes in international legal and regulatory environments, the issue of user consent is of clear interest (e.g., Ball, Haggerty, & Lyon, 2012; Bellman, Johnson, & Lohse, 2001; Solove, 2013). While it falls beyond the scope of this paper to comprehensively map the many issues pertaining to user consent, the following broad issues apply here:

- Regulatory and legal frameworks often lag technological developments and, so reliance on regulatory and legal frameworks can only be part of the solution. The success of laws and frameworks depend largely on the ability of various institutions to oversee and enforce the regulations (Lane, Stodden, Bender, & Nissenbaum, 2015; Pasquale, 2015; Solove, 2004, 2013)

- Digital promiscuity appears to be an increasing phenomenon. While there is growing protection of individuals' right to privacy, and a general awareness of privacy and the collection, analysis, and use of personal data, there remains evidence of irrational sharing of (often) highly personal information in environments that may not be secure (Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Payne, 2014)

- When individuals opt to share information, their decisions are based, inter alia, on how much trust they have in the online service provider to protect their information, how much control users have to change or delete their information. The relationship between trust, privacy and control, and perceived benefits is known as the "privacy calculus" (Krasnova, Veltri, & Günther, 2012).

- The length and inaccessibility of Terms and Conditions (Miltgen & Smith, 2015; Miyazaki & Fernandez, 2000) also impacts on user understanding and acceptance of the scope and purpose of the collection, analysis, and use of their data.

- While users may engage with the immediate implications of the collection, analysis, and use of their data, there are increasing concerns pertaining to the downstream use of data by a plethora of users; data brokers; individual, commercial, and legal entities; and platforms (Lane et al, 2015; Solove, 2004, 2013)

- The increasing role of algorithmic decision-making systems and concerns about, inter alia, the lack of human oversight and regulation (Pasquale, 2015). Interestingly, GDPR specifically addresses the issue of automated decision-making "that has legal or similarly significant effects on them" (Sclater, 2018, par. 24), requiring that "humans are involved in decisions with significant consequences" on data subjects (Sclater, 2018, par. 25).

Given that GDPR is flagged as an "instrument for the globalisation of privacy standards" (Bennett, 2018, p.1), Sclater (2018) stipulates a number of requirements at micro level (point A, Figure 1), namely:

1. Consent requests should be kept separate from other terms and conditions.

2. Clear and specific information must be given to the students about what they are consenting to.

3. Students should be informed of any third-party data controllers who will rely on the consent.

4. The consequences of both providing and withholding consent must be made clear.

5. Clear, affirmative action is required by the student; the use of pre-ticked boxes would not be acceptable.

6. Mechanisms must be put in place to enable students to easily withdraw their consent at any time–with the consequent removal of their Special Category Data from all databases or withholding of any interventions.

7. Records should be kept of any granting, withholding, or withdrawal of consent by students (par. 18).

The above requirements echo pointers expressed in one of the earliest published explorations of the ethical implication in learning analytics. One of the six principles proposed by Slade and Prinsloo (2013) refers to the issue of "transparency," which they later expand into a set of questions including "Who benefits and under what conditions?" (p. 1521) and how to deal with issues pertaining to consent, de-identification, and opting out.

Though GDPR provides much clarity on the scope, nature, and nuances of consent at the micro level, there are concerns that

> data protection law does not halt surveillance, it manages it. It may produce a fairer and more efficient use of and management of personal data, but it cannot effectively control the voracious and inherent appetite of modern organisations for more and more increasingly refined personal information, especially when those data are central to the business models of the platform economy. (Bennett, 2018, p. 8)

Research by Russell et al. (2018) confirms that even though GDPR may provide some safeguards and increase user understanding of the scope and nature of consent, it will not necessarily curtail the market value for personal data. The extent to which GDPR will impact on stemming the growth in the market for student data remains to be seen.

Consent at the Meso Level

Privacy is no longer a "domestic issue" (Bennett, 2018, p. 2) with data shared across platforms, and different geopolitical, legal, and regulatory frameworks within which the content-provider (e.g., a university) and the host MOOC platform (e.g., Coursera, FutureLearn) operate. There is, as far as we could establish, no published research on the implications of GDPR for data exchanges between the offering institution, the hosting platform provider (and its legal and regulatory environment), and the legal and regulatory environment of students. MOOCs may be designed and delivered on a platform based in a particular geopolitical and regulatory environment. The offering institution may then be in a different geopolitical and regulatory context, regulated by different rules and provisions. This raises complex new areas for exploration. Bennett (2018) states that "adherence to privacy standards is now regarded as a necessary condition for the international, networked economy" and that there "are certainly no geographical barriers to diffusion" (p. 7). He continues to warn that the existence of legislation and regulation does not, necessarily, ensure its effective implementation and that many laws

"are totally symbolic" (p. 8). In line with Bennett (2018) and Russell et al (2018), the existence of GDPR and its impact on transnational flows of data will have to be seen.

In research carried out by Prinsloo and Slade (2016) on student consent in the context of three MOOC providers, several issues were flagged which illustrate the complexity of consent on the meso level. For example, the authors note that "personal data" is defined differently on different platforms, or not defined at all, and that the scope and type of data collection methods are not always declared or defined. Although students had the option to disable selected installed cookies, such action will impact on the functionality of the services provided.

Khalil, Prinsloo and Slade (2018) refer to this as the "unbearable lightness of consent" in the context of later research on MOOC providers from different geopolitical contexts, noting that uses of personal data unrelated to the course of study were unclear and in general, that the scope, and implications of consent "remain(s) largely unsatisfactory."

Consent at the Macro Level

The implementation in 2018 of GDPR has dramatically changed the playing field. GDPR addresses the different complexities in the collection, analysis and use of data by a range of stakeholders, including, but not limited to, commercial providers and enterprises, governments, (independent) algorithmic agents, and in the context of education, providers of formal, informal, and post-formal education. Various authors explore the sharing, selling, remixing, and re-identification of user data outside the original consent provided by the user (Crawford & Schultz, 2013; Lane et al., 2015; Solove, 2004, 2013). Lane et al. (2015) claim that "privacy and big data are simply incompatible, and the time has come to reconfigure choices that we made decades ago to enforce constraints" (p. xii).

Within the context of developments in international privacy protection and regulation of data flows, we should not overlook the complexities that arise when stakeholders (e.g., students, content providers, and MOOC platform) are based in different geopolitical locations (Bennett, 2018; Khalil, Prinsloo & Slade, 2018; Sclater, 2017a, 2017b). For example, students from different geopolitical and regulatory contexts may enrol for a course offered by a specific institution, possibly in different geopolitical and regulatory context, offered on a platform in yet another geopolitical and regulatory context, who would then share user data with data brokers, third-party providers, and other stakeholders in other geopolitical and regulatory contexts. This is further complicated if we consider that the MOOC platform provider may provide access to user data to data brokers, third-party providers, and other stakeholders in other contexts.

In the next section, we review the approaches taken to user consent from four MOOC providers based in different geopolitical contexts, and identify issues related to the micro, meso, and macro levels.

Methodology

The methodology adopted for this study is a multiple-case study of the Terms of Use and the Privacy Policies of four MOOC providers with the aim of mapping the scope and content of user consent on micro, meso, and macro levels. The purpose of this multiple-case study is to explore and map how

consent, which has been provided to collect and use data, is a) described to potential users and b) how that consent applies at each level.

The research design entailed a qualitative, interpretive study entailing a directed content analysis (Bos & Tarnai, 1999) whereby authors transmit the meaning of a text through interpretive reading. Using a *deductive*, directed content analysis approach entails identifying key concepts of variables as initial coding categories, defined by theoretical frameworks and published research (Elo & Kyngäs, 2007).

Four cases were considered involving MOOC providers from the United States and Europe (see Table 1). Coursera (http://coursera.org) and edX (http://edx.org) represent the largest US MOOC providers with student enrolments of over 25 million (Coursera) and 10 million (edX) respectively, and FutureLearn (http://futurelearn.com) and iversity (http://iversity.org) represent the European MOOC providers with student enrolments of 7 million (FutureLearn) and 1 million (iversity), respectively. At the time of the study, the providers had offered a variety of MOOCs: Coursera (2,000), edX (1,750), FutureLearn (640), and iversity (110). The geopolitical locations of the studied MOOC platforms provided an opportunity to examine the ways in which European and U.S. legislation shape and approach user consent.

Table 1

Background Information of the MOOC Providers

Description	**edX**	**Coursera**	**iversity**	**FutureLearn**
Country	USA	USA	Germany	UK
Launch year	2012	2012	2013	2012
Enrolments	10,000,000	25,000,000	1,000,000	7,100,000
Documents analysed (effective and last update)	Terms of Service (Jan. 2016) Privacy Policy (Oct. 2014)	Terms of Use (April 2015) Privacy Policy (Oct.2015) Privacy Shield Policy (June 2017)	Terms of Use (n.d.) Privacy Policy (Feb. 2016)	Terms and Conditions (n.d.) Privacy Policy (n.d.)

The units of analysis included were the four providers' publicly available Terms of Use and the Privacy Policy. Each MOOC provider affords conditions which users must accept to use their service. Coursera and iversity describe this as the Terms of Use, edX as the Terms of Service, and FutureLearn as Terms and Conditions. The text of these documents was copied from the MOOC provider websites on (September 13, 2017). The analysis was performed in (February 2018). It is worth noting that the privacy policy of the MOOC providers was updated to reflect changes relating to the ways in which individuals' data will be handled and stored to be GDPR compliant. This study is based on an examination of documents obtained in September 2017.

The privacy policies and terms of use (or terms and conditions) for each provider were copied and pasted into separate text files using UTF-8 character encoding. Each file was labelled for identification purposes. In total, there were eight text files, totalling 120 pages and 36,965 words.

The text material was examined thoroughly with a view to reflecting issues relating to consent at the three levels (i.e., micro, meso, and macro) as informed by published literature, and specifically the framework of Buckingham Shum (2012).

Methodological Norms

The dialogical model proposed by Rule and John (2011) in which theory and research interact dialogically throughout the research process was adopted:

> Such an approach acknowledges that theory infuses research in all its aspects, including the identification and selection of the case, the formulation of research purposes and questions, the survey of literature, the collection and analysis of data, and the presentation and interpretation of findings. (p. 100)

We addressed the validity, reliability, and trustworthiness in the directed content analysis by transparency regarding the process including the selection of analytical constructs from the literature review, coding, member checking of the codes, constructs, and analyses (Elo & Kyngäs, 2007; Zhang & Wildemuth, 2009).

The researchers held regular virtual meetings and took responsibility for peer cross-checking of terms, levels, and analysis. An audit trail was kept of member comments and changes. As such, the suggestions by Rule and John (2011) of steps to ensure the *trustworthiness* (as an alternative to reliability and validity) of the analysis and findings were followed. In doing so, it is accepted that it is not only the final product that needs to be judged for quality, but also the process of inquiry. Thomas (2011) states that:

> Conclusions drawn from case study research become less pronounced when we realise that, to a greater or lesser extent, all forms of inquiry, especially social inquiry, produce knowledge that is provisional – in other words, good until we find out something else which explains things better. (p. 216)

Limitations

This research study covered four MOOC providers from the United States and Europe at a given date. We did not review the content of the privacy policy nor the terms of use from a legal perspective. This study attempts to examine the micro, meso, and macro perspectives of user consent in the studied MOOC platforms from a lay-person's dimension.

Results and Discussions

The analysis sought to establish and distil substantial points from the terms and conditions as well as the privacy policy of each MOOC provider at each of the three levels. The results of the analysis are presented below within three tables, which attempt to describe and categorise how consent is characterised in the policies of the four MOOCs at the micro, meso, and macro levels. It is worth noting that the context of the different levels occasionally overlap so that some issues are not exclusive to one level.

Micro Level

The micro level represents a narrow view within a limited direction of data usage between teacher(s) and student(s), that is, at a course level. This level typically involves student consent that their data are collected, processed, analysed, and interpreted to create interventions that affect learners and/or teachers. Many students would assume that the granting of consent would relate primarily to this level, that is, that data gathered about students would be used directly to support their own learning (Sclater 2017a, 2017b, Slade & Prinsloo, 2013). Table 2 shows the categorization of issues captured from policy documents at a micro level.

Table 2

The Micro Level of Consent in the Studied MOOC Providers

MOOC provider	Terms
edX	• Permission to copy, host, and modify user postings. • Consent to use the data for recommendation and personalization. • Receive newsletters and subscriptions. • Consent to collect and analyse online traces and learning patterns.
Coursera	• Permission to copy, host, and modify user content. • Consent to use the data to improve the education experience. • Consent for archiving, newsletters, and communication. • Verify identification. • Use and share of personal identifiable information and learner performance data with the instructor(s), teaching assistant(s), and the institution(s) with which they are affiliated.
FutureLearn	• Permission to exploit, host, and modify learner content. • Consent to collect entry data and traces for personalization and recommendation. • Receive newsletters and subscriptions.
iversity	• Permission to adapt and undertake user content (exploitation is prohibited). • Consent to collect and use data from: logfiles, cookies, web analytics for security reasons, and system optimization. • To receive newsletters and subscriptions, communication, and contact. • Consent to pass content data to instructor(s) and cloud-based teaching assistant(s).

The above analysis points to aspects to consider further in the light of published research on user consent. For example, when students enrol in edX, they provide consent for collection and analysis of online traces and learning patterns for recommendation and personalization. However, there is no further information regarding the specific criteria or data points used to identify learning behaviour, nor information on how students' learning journeys may change when their data are used to personalise their learning. Coursera shares personal identifiable information of learners with instructor(s), teaching assistant(s), and the institution(s) with which they are affiliated but does not provide an exact scope of what "personal identifiable information" may mean. It is also clear from Table 2 that users cede the right to the content they produce on these platforms. For example, users on Coursera consent that the provider may copy, host, and modify their content, while FutureLearn states that it will *exploit* student content. In stark contrast, iversity states explicitly that exploitation of student content is prohibited.

In considering suggestions by Sclater (2017a, 2017b), the initial consent provided by students does not, necessarily, cover agreement to having a learning journey changed or personalised. It seems that MOOC providers are inherently relying on students' trust that the provider will not abuse their data nor use it to their detriment (Prinsloo & Slade, 2015). Without knowing its exact parameters, consent may be, as Bellman, Johnson, and Lohse (2001) described "unbearably light."

Meso Level

The meso level operates at the institutional level (i.e., at the level of the whole MOOC platform). Consent for data collection and usage at this level often relates to building insight for accreditation, enhancing the online experience, and general website improvement. Table 3 demonstrates the categorization of the examined documents within the meso level. It would perhaps not surprise some students if their data were being used for some of these activities.

Table 3

The Meso Level of Consent in the Studied MOOC Providers

MOOC provider	Terms
edX	• To improve courses, do research, maintain security, archiving communication for future contact, etc.
Coursera	• For business purposes. • For demographic statistics, research, and to improve courses and online experience. • Transfer and process personal information on servers located outside the US. • Partner sites may share user's data with Coursera for improving Coursera's services. • Users have the option to log in to the Coursera website using their Facebook login details. This provides Coursera then with access to their Facebook data
FutureLearn	• Collect data for accreditation purposes and website improvement.

	• Consent to share data to the holding company and its subsidiaries.
iversity	• User consent, if logging using Facebook Connect, to allow iversity to collect, process, and use of all Facebook data (likes, profile picture, email, name of friends, cover photo, etc.).

At the meso level, the effects of the initial consent provided by students increase in complexity and potential impact. For example, Coursera explicitly states that it transfers personal information to servers located outside the United States. Coursera and iversity also record that they receive personal information when a user accesses or logs onto their sites using login details from a third-party site, for example, Facebook. A student accessing their site in this way also then provides access to his or her Facebook data. This has immense implications for students' understanding of the impact of the initial acceptance of the terms and conditions of the provider. Considering the recent public outcry regarding Facebook's data practices and its sharing of data with, among others, Cambridge Analytica, users should seriously (re)consider the scope and impact of their consent to providers' terms and conditions (Bennett, 2018; see also Meyer, 2018).

At a meso level, we get a glimpse of the unfolding and implications of the initial consent users provide. As the next section regarding the macro level illustrates, the scope and impact of the initial consent increases on macro level.

Macro Level

The macro level represents a broader view of sharing of data, analysis, and curricula with a wider community and with other stakeholders of similar disciplines (such as regional and international MOOC platforms or academic research institutions) and with (not obviously connected) stakeholders (such as governments, recruitment companies, and other third parties). Table 4 shows the categorization of the examined documents within the macro level.

Table 4

The Macro Level of Consent in the Studied MOOC Providers

MOOC provider	Terms
edX	• The collection, use, transfer, disclosure, and retention of information in and outside of the United States. • To transfer personal data between edX and third parties, affiliates, and subsidiaries. • To transfer applicable personal information to a jurisdiction which may provide a different level of privacy protection. • Third party payment processor when buying a certificate. • To use data for subpoenas, court orders, or other legal process; to investigate, or prevent, or take action regarding illegal activities. • To use anonymized data with public/third parties.

Coursera	• To transfer and distribute user content to share with partners or research purposes. • To share personal information with government authorities in response to subpoenas, court orders, or other legal processes. • Third Party Credit Card Processing.
FutureLearn	• To transfer and distribute learner content to display on the website or online content and courses. • Share data with third parties to provide services that one requested. • To an exchange of data in case of protecting FutureLearn against fraud. • To share data with partners for research and course improvement.
iversity	• To use anonymized personal data for research purposes with academic institutions. • To pass content data (profile and course data) to other platform users or other platforms (opt out is available). • Governmental and regulatory use. • Share content and inventory data with recruiting companies. • To allow third party tools like "conversion tracking tools" from Facebook and Google to track the effects of marketing measures.

The tables above demonstrate that consent is considered by MOOCs at all three levels. What might be surprising to users is the way that consent is employed to predominantly provide benefit to the MOOC providers. A huge amount of data is collected, much of which is not obviously associated with a learning experience. It is evident from Tables 2, 3, and 4 that the terms of use and privacy policies of the four reviewed MOOC providers emphasise issues far beyond student learning and insights for content providers. Even where it is stated that data will be used to improve learners' experience, it is not clear how this is done, how often, nor how learning analytics is employed for optimization purposes (i.e., interventions, recommendations, personalisation).

This largely confirms Sclater's (2017a) view that consent remains an issue when learning analytics is operationalised within education. In reviewing and mapping the policy documents, ambiguity was also an identified feature.

Despite the generous provision of "free learning," it seems clear from the reviewed policies that user consent is employed to gain significant insight into individuals' personal data.

(In)conclusions

User consent, and in the case of online education platforms, student consent, is often considered in the specific context of the providing institution. With the advent and continuing growth of MOOCs, this paper suggests that the initial consent provided by students at the point of registration has considerable potential for misinterpretation. This study highlights a need to more explicitly consider consent issues when data is used and shared on meso and macro levels in learning analytics. Given the range of uses to which data is put, consent needs to be more clearly seen for what it is—as allowing data to be used, re-used, and shared with a range of stakeholders and for a range of purposes well outside the original assumptions and understanding of those accepting the Terms and Conditions.

The implications of this study are far-reaching, for students, for higher education institutions offering courses on MOOC platforms, and for MOOC platforms themselves. MOOC platform providers should be more transparent about their definitions of personal data; the ways in which data are collected and the purposes for which data are collected and analysed; and who data will be shared with and under what circumstances. While it falls outside the scope of this paper to map the legal implications of GDPR for MOOC platform providers, students and higher education institutions should have a clear(er) understanding of how the initial consent of students (Figure 1, Point A) has vast implications for the downstream use of a range of data-collectors, users, and brokers.

Studies provide ample evidence that users do not engage with Terms and Conditions in any context, educational or otherwise. Given that higher education institutions have a fiduciary duty towards students, they should find ways to make Terms and Conditions pertaining to consent more understandable and accessible. For instance, MOOC providers can show a banner where students can opt in or out of certain personal data collection and processing prior to enrolment.

We believe that students can no longer afford to claim ignorance or have limited choices in accepting Terms and Conditions of any online service, including MOOCs. This also applies to situations when students are registering for what may appear to be free educational services. Student bodies and consumer organisations should scale up their efforts to increase student agency and literacy regarding the scope, nature, and implications of their consent.

Acknowledgement

The authors express gratitude to the reviewers whose comments, suggestions, and critique greatly enhanced the resubmitted article.

References

Ball, K., Haggerty, K.D., & Lyon, D. (2012). *Routledge handbook of surveillance studies*. Abingdon, UK: Routledge.

Bellman, S., Johnson, E.J., & Lohse, G.L. (2001). On site: to opt in or opt-out?: It depends on the question. *Communications of the ACM*, *44*(2), 25-27. Retrieved from http://dl.acm.org/citation.cfm?id=359241

Bennett, C. J. (2018). The European general data protection regulation: An instrument for the globalization of privacy standards? *Information Polity*, (Preprint), 1-8. Retrieved from https://pdfs.semanticscholar.org/3813/041fc44467933d64c54c3e39a467c2be63c3.pdf

Bos, W., & Tarnai, C. (1999). Content analysis in empirical social research. *International Journal of Educational Research*, *31*(8), 659-671. http://doi.org/10.1016/S0883-0355(99)00032-4

Buckingham Shum, S. (2012). Learning analytics. *UNESCO Institute for Information Technologies in Education*. Retrieved from http://iite.unesco.org/files/policy_briefs/pdf/en/learning_analytics.pdf

Cormack, A.N. (2016). Downstream consent: A better legal framework for Big Data. *Journal of Information Rights, Policy and Practice, 1*(1). https://doi.org/10.21039/irpandp.v1i1.9

Crawford, K., & Schultz, J. (2013). Big data and due process: Towards a framework to redress predictive privacy harms. *Boston College Law Review,* 55(1). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784

Drachsler, H., & Kalz, M. (2016). The MOOC and learning analytics innovation cycle (MOLAC): A reflective summary of ongoing research and its challenges. *Journal of Computer Assisted Learning, 32*(3), 281-290. http://doi.org/10.1111/jcal.12135

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107-115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Fairfield, J.A.T. (2017). *Owned: Property, privacy, and the new digital serfdom*. Cambridge, United Kingdom: Cambridge University Press.

Ferguson, R. (2012). Learning analytics: Drivers, developments and challenges. *International Journal of Technology Enhanced Learning*, *4*(5/6) 304–317. Retrieved from http://oro.open.ac.uk/36374/1/IJTEL40501_Ferguson%20Jan%202013.pdf

Gašević, D., Dawson, S., & Siemens, G. (2015). Let's not forget: Learning analytics are about learning. *TechTrends, 59*(1), 64-71. https://doi.org/10.1007/s11528-014-0822-x

Hern, A. (2018, April 19). Facebook moves 1.5bn users out of reach of new European privacy law [Blog post]. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635. https://doi.org/10.1111/isj.12062

Khalil, M., Prinsloo, P., & Slade, S. (2018, June 26-28). The unbearable lightness of consent: Mapping MOOC providers' response to consent. In *Proceedings of the fifth annual ACM conference on learning at scale*. London, United Kingdom: ACM. Retrieved from https://dl.acm.org/citation.cfm?id=3231659

Khalil, M., Taraghi, B., & Ebner, M. (2016). Engaging learning analytics in MOOCs: The good, the bad, and the ugly. In *Proceedings of the International Conference on Education and New Developments (END 2016;* pp. 3-7). Ljubljana, Slovenia.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127-135. https://doi.org/10.1007/s12599-012-0216-6

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (Eds.). (2015). *Privacy, big data, and the public good*. New York: Cambridge University Press.

Leitner, P., Khalil, M., & Ebner, M. (2017). Learning analytics in higher education—a literature review. In A. Peña-Ayala (Ed.), *Learning analytics: Fundamentals, applications, and trends* (pp. 1-23). Springer, Cham.

Long, P., & Siemens, G. (2011a). Message from the LAK 2011 general & program chairs. Proceedings of the *1st international conference on learning analytics & knowledge*. Alberta, Canada: ACM. Retrieved from https://portalparts.acm.org/2100000/2090116/fm/frontmatter.pdf?ip=129.177.96.37

Long, P., & Siemens, G. (2011b). Penetrating the fog: Analytics in learning and education. *EDUCAUSE Review*, *46*(5), 30-32. Retrieved from https://er.educause.edu/articles/2011/9/penetrating-the-fog-analytics-in-learning-and-education

Meyer, R. (2018, March 20). The Cambridge Analytica scandal, in three paragraphs [Blog post]. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behaviour. *Information & Management, 52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006

Miyazaki, D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*(1), 54–61. https://doi.org/10.1509/jppm.19.1.54.16942

Pasquale, F. (2015). *The black box society. The secret algorithms that control money and information*. London: Harvard University Press.

Papamitsiou, Z., & Economides, A. A. (2014). Learning analytics and educational data mining in practice: A systematic literature review of empirical evidence. *Journal of Educational Technology & Society*, *17*(4), 49-64. Retrieved from https://www.jstor.org/stable/pdf/jeductechsoci.17.4.49.pdf

Payne, R. (2014). Frictionless sharing and digital promiscuity. *Communication and Critical/Cultural Studies 11*(2), 85–102. Retrieved from https://doi.org/10.1080/14791420.2013.873942

Prinsloo, P., & Slade, S. (2015, March). Student privacy self-management: Implications for learning analytics. In *Proceedings of the fifth international conference on learning analytics and knowledge* (pp. 83-92). ACM. Retrieved from https://dl.acm.org/citation.cfm?doid=2723576.2723585

Prinsloo, P., & Slade, S. (2017). Ethics and learning analytics: charting the (un)charted. In C. Lang, G. Siemens, A. Wise, & D. Gašević (Eds.), *Learning analytics handbook* (pp. 49-57). Edmonton, AB, Canada: Society of Learning Analytics.

Rule, P., & John, V. (2011). *Case study research*. Pretoria: Van Schaik Publishers.

Russell, N.C., Reidenberg, J.R., Martin, E., & Norton, T.B. (June 6, 2018). Transparency and the marketplace for student data. *Virginia Journal of Law and Technology, Forthcoming*. http://dx.doi.org/10.2139/ssrn.3191436

Sclater, N. (2017a, February 16). Consent for learning analytics: some practical guidance for institutions [Blog post]. *Jisc.* Retrieved from https://analytics.jiscinvolve.org/wp/2017/02/16/consent-for-learning-analytics-some-practical-guidance-for-institutions/

Sclater, N. (2017b, June 30). Consent and the GDPR: What approaches are universities taking? [Blog post]. *Jisc.* Retrieved from https://analytics.jiscinvolve.org/wp/2017/06/30/consent-and-the-gdpr-what-approaches-are-universities-taking/

Sclater, N. (2018, June 1). GDPR and learning analytics – Frequently asked questions [Blog post]. *Jisc.* Retrieved from https://analytics.jiscinvolve.org/wp/2018/06/01/gdpr-and-learning-analytics-frequently-asked-questions/

Siemens, G. (2013). Learning analytics: The emergence of a discipline. *American Behavioral Scientist, 57*(10), 1380-1400. https://doi.org/10.1177/0002764213498851

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist 57*(10), 1509–1528. https://doi.org/10.1177/0002764213479366

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York, USA: New York University Press.

Solove, D.J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review 126*(7), 1880–1904.

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 239*, 1–36. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/nwteintp11&id=265&collection=journals&index=

Thomas, G. (2011). *How to do your case study: A guide for students and researchers.* Thousand Oaks, CA: Sage Publications.

Young, E. (2014). Educational privacy in the online classroom: FERPA, MOOCs, and the big data conundrum. *Harvard Journal of Law & Technology*, *28*(2), 549-592. Retrieved from http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech549.pdf

Zhang, Y., & Wildemuth, B.M. (2009) Qualitative analysis of content. In B. Wildemuth (Ed.), *Applications of social research methods to questions in Information and library science* (pp. 308-319). Westport, CT: Libraries Unlimited.