A Data Protection Framework for Learning Analytics

Andrew Cormack, Jisc, UK
Andrew.Cormack@jisc.ac.uk

ABSTRACT: Most studies on the use of digital student data adopt an ethical framework derived from human-studies research, based on the informed consent of the experimental subject. However consent gives universities little guidance on the use of learning analytics as a routine part of educational provision: which purposes are legitimate and which analyses involve an unacceptable risk of harm. Obtaining consent when students join a course will not give them meaningful control over their personal data three or more years later. Relying on consent may exclude those most likely to benefit from early interventions.

This paper proposes an alternative framework based on European Data Protection law. Separating the processes of analysis (pattern-finding) and intervention (pattern-matching) gives students and staff continuing protection from inadvertent harm during data analysis; students have a fully informed choice whether or not to accept individual interventions; organisations obtain clear guidance: how to conduct analysis, which analyses should not proceed, and when and how interventions should be offered. The framework provides formal support for practices that are already being adopted and helps with several open questions in learning analytics, including its application to small groups and alumni, automated processing and privacy-sensitive data.

KEYWORDS: learning analytics, privacy, data protection, consent, legitimate interests

1. INTRODUCTION

Learning analytics has been defined as "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, 2011, p.33). Analysing learner data could inform a university's management of finances, resources and enrolment, enhance its course presentation and materials, or enable personalised guidance and intervention for individual students and staff (Leece, 2013). Analytics could improve both the provision of learning to future students and the support and guidance offered to current teachers and students, both at cohort and individual level.

A very wide range of personal data, both historic and current, may be relevant input to analytics processes – "from formal transactions (such as assignment submissions) to involuntary data exhaust (such as building access, system logins, keystrokes and click streams)" (Kay, Korn, & Oppenheim, 2012, p.9) – giving these processes many of the characteristics of "big data". That field has been identified as challenging for existing legal and ethical frameworks. According to Kord Davis, in an interview with O'Reilly Radar, "[b]ig data itself, like all technology, is ethically neutral. The use of big data, however, is

not … The challenge is how to honor those values (transparency, security and accountability) in everyday actions as we go about the business of doing our work" (Wen, 2012). Tickle (2015) reports that in supporting non-traditional students "the timeliness of the university's intervention made far more difference to students than what was actually done" and asks "How comprehensive and intrusive should data collection be?".

To date, learning analytics has largely been conducted within an ethical framework based on medical research, with individuals' informed consent being the foundation for all analysis and intervention. However as learning analytics becomes part of routine university operations, this paper suggests that considering it as a form of human-subject research may no longer produce the most suitable framework. Instead it proposes that examining the full range of legal bases for processing personal data may offer a clearer guide to both organisations and students on how and when analytics should, and should not, be applied. In particular separating the processes of analysis and intervention provides stronger guidance and safeguards for both; examples are given of how this can inform commonly-raised questions. This approach should ensure that learning analytics processes can be trusted by both students and organisations to deliver the greatest benefit for current and future students, for teachers, educational organisations and society.

2. THE NEED FOR A LEARNING ANALYTICS FRAMEWORK

Learning analytics shares many characteristics with the well-established processes of educational data mining (Prinsloo & Slade, 2013) and website personalisation (Pardo & Siemens, 2014). Like them it seeks to "understand and optimize learning and the environment in which it occurs" (Pardo & Siemens, 2014, p.443). However both the nature and scale of data available and the expectations of learners and society are changing to create new opportunities and new risks; this may require a new approach to maintain trust between educational organisations, their staff and students.

Prinsloo and Slade (2013) note that "the increasing digitisation of education, technological advances, the changing nature and availability of data have huge potential for learning analytics to contribute to our understanding of the different variables impacting on the effectiveness of learning, student success and retention" (p.244), in other words to improve the general provision of education; and that "[t]he increasing digitisation of learning has resulted in the availability of real-time data on an unprecedented scale creating new opportunities for harvesting digital trails of students' (non)engagement. Knowing more about students' learning processes and trajectories allows the potential for higher education institutions to offer personalised and customised curricula, assessment and support to improve learning and retention" (Prinsloo & Slade, 2013, p.240), so improving support and guidance to individual students.

Such uses of personal data may be increasingly accepted, even expected, both by individual learners and by society. According to Kay et al. (2012), "[u]sers, especially born digital generations, appear increasingly to expect personalised services that are responsive to profile, need and interest and are

therefore more likely to be content for their data to be used to those ends" (p.4), while Pardo and Siemens (2014) find "society seems to be evolving toward a situation in which the exchange of personal data is normal" (p.440).

However learning analytics, by consuming increasing quantities of varied and real-time data, also shares characteristics with Big Data, particularly the possibility identified by Mayer-Schönberger and Cukier (2013), quoted in Richards and King (2014), "to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more". This possibility for inquiries to reveal unexpected information from raw data, as opposed to testing prior hypotheses that have already been assessed against ethical rules, "raises important social, legal and ethical questions, among which [are] concerns with regard to the privacy and data protection rights of these individuals", according to the Article 29 Working Party of European data protection authorities (2014b, p.2). For example combining datasets from different sources can result in re-identification of individuals (Ohm, 2010), or a correlation between two factors might suggest a causal link that does not in fact exist. In comparison with big data use in the retail sector (e.g. loyalty cards), Pardo and Siemens (2014) consider that

> Educational institutions pose a new scenario with specific requirements. Students interact very intensively with the university (or its computational platforms) during a concrete time frame, carrying out very specific tasks, and produce highly sensitive data during the process. These special conditions prompt the need for a revision of the privacy principles with respect to analytics and their application in educational settings. (p.448)

On the other hand the much greater shared interest between an educational organisation and its students in improving learning processes creates the possibility of a relationship much stronger and more mutually beneficial than a simple economic bargain exchanging shopping habits for discount vouchers.

It is clear that, as Pardo and Siemens (2014) suggest, in learning analytics "a delicate balance between control and limits needs to be achieved" (p.440). However according to Prinsloo and Slade (2013) "current policy frameworks do not facilitate the provision of an enabling environment for learning analytics to fulfil its promise" (p.240). Present frameworks are largely based on practice in clinical research. Thus Kay et al. (2012) find the Nuremberg Code's principle that "research participants must voluntarily consent to research participation" is "highly relevant" to analytics with "consent regarded as fundamental" (p.20); according to Sclater (2014) "informed consent is recognised as key to the analysis of learner data by many commentators and is a basic principle of scientific research on humans" (p.16); and at the University of South Africa "the Policy on Research Ethics makes informed consent and anonymity non-negotiable" (Prinsloo & Slade, 2013, p.242).

However Kay et al. (2012) note that in other fields different ethical approaches are considered "self-evident good practice" (p.26). For example

> The practice adopted by leading business to consumer players provides a clear and legally grounded approach that is likely to be readily understood by the public in much of the world. In particular, the development of a sense of mutual gain, recognised and shared by a service organisation and its customers, is something to be learned from such as Amazon and Nectar. (Kay et al., 2012, p.24)

They conclude "the challenge is whether the education community, not least in the emerging field of learning analytics, should revise its ethical position on account of the widespread changes of attitude in the digital realm from which learners and researchers are increasingly drawn." (Kay et al., 2012, p.26)

The next two sections of the paper will consider what problems are likely to arise from continuing to rely on "informed consent" as learning analytics techniques transfer from university research to university operations, and whether a more fruitful framework can be derived from European data protection law.

3. LIMITATIONS OF "INFORMED CONSENT"

To date, learning analytics has largely been a subject for educational research. However the techniques are increasingly being adopted as part of the routine operation of universities and colleges (for example (Open University (n.d.))). Such processes may affect all current and future students and staff, not just those who participate in research studies, either through changes to how education is provided in general or through individual interventions. With this significantly increased impact, "informed consent" may no longer provide adequate guidance and protection either for individuals or for organisations.

Both law and ethics require that for consent to be valid it must be both informed and freely-given (Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L281/281, Article 2(h)). However as Kay et al. (2012) observe, big data approaches, including learning analytics, involve "unpredictability of questions to be answered by the data" (p.7). When using an inductive, data-driven approach, rather than a deductive, hypothesis-driven one it is hard for the organisation to predict even what correlations will emerge from the data, let alone what their impact on the individual will be. Richards and King (2014) see a significant change:

> [b]efore big data, individuals could roughly gauge the expected uses of their personal data and weigh the benefits and the costs at the time they provided their consent. Even if they guessed wrong, they would have some comfort that the receiving party would not be able to make additional use of their personal data. The growing adoption of big data and its ability to make extensive, often unexpected, secondary uses of personal data changes this calculus. (p.414)

While an educational organisation may, and probably should, state that analytics will only be used for the purpose of improving educational provision, this is unlikely to be sufficient for an individual student or teacher to have "an appreciation and understanding of the facts and implications of an action …

includ[ing] also an awareness of the consequences of not consenting to the processing in question", as required by the Article 29 Working Party (2011, p.19) if consent is to be valid.

Furthermore the law increasingly presumes that consent is not freely-given in situations where the party requesting consent has power over the individual granting it. The European Commission's (2012) draft General Data Protection Regulation states explicitly that "[c]onsent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller" (Recital 39). Responding to the Nuremberg Code's requirement that "[s]ubjects must be allowed to discontinue their participation at any time", Kay et al. (2012) note that, in education "[u]nlike in the consumer world, it is perhaps hard to opt out and to ensure that your data will not be collected or used" (p.20). Exercising the option of withdrawing from processing "may involve withdrawing from the wider entity, such as the university" (Kay et al., 2012, p.27). It is hard to see this satisfying the Article 29 Working Party's (2011) test that "[c]onsent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent" (p.12).

Most educational organisations would agree with Richards and King (2014) that "users alone cannot take responsibility for technologies and business practices that they do not themselves create but find themselves increasingly dependent upon" (p.430), and that organisations have a duty to behave responsibly. However using consent as a basis provides little guidance on what responsible behaviour is. The law does require that processing of personal data be "fair" (Data Protection Directive, Art.6(1)(a)) but that is, again, largely a matter of the information and controls provided to individuals (Information Commissioner, n.d.). A consent approach runs the risk of discussions focussing on whether new analytics results are within "the scope of the data subject's consent" (Article 29 WP, 2014a, p.13), rather than whether the inferences may, perhaps, be "inaccurate, discriminatory or otherwise illegitimate" (Article 29 WP, 2013, p.45) and should not be used at all.

Finally, the use of consent may well bias the results of learning analytics, potentially excluding those who have most to gain from the process. Kay et al. (2012) note the practical implications of how consent is obtained: "[a]lthough an opt-in box is much more likely to be held to be consent, (as it requires a definite, positive action), the danger is that the user's inertia means failing to opt-in is a much higher risk" (p.18). With either approach there is a risk of self-selection: that different groups will opt in or out in different proportions. This could skew the results either in favour of or against those groups (Clarke & Cooke, 1983): for example analytics often aspire to help those disengaged from the educational process, but will get little information about this group from data collected on an opt-in basis.

These doubts about the use of consent are not limited to the education context. In discussing the development of big data over the next five years, the European Data Protection Supervisor (2015) sees the focus moving to the behaviour of organisations:

> "Big data that deals with large volumes of personal information implies greater accountability towards the individuals whose data are being processed. People want to understand how

> algorithms can create correlations and assumptions about them, and how their combined personal information can turn into intrusive predictions about their behaviour." (p.10)

Recognising that information may be "knowingly volunteered by the individual, or … observed and inferred without the individual's knowledge" (p.10) he calls for "an end to opaque privacy policies, which encourage people to tick a box and sign away their rights" (p.11). Rather than relying on prior consent individuals should be "properly informed on how and why their information can be used" and have a continuing opportunity to challenge "mistakes in the assumptions and biases [data analytics] can make about individuals" (p.11).

Such an approach seems more suitable for education where, according to Prinsloo and Slade (2013),

> [i]t is accepted that there are certain types of information and analyses (e.g. cohort analyses) that fall within the legitimate scope of business of higher education. There is though an urgent need to approach personal data differently when it is used to categorise learners as at-risk, in need of special support or on different learning trajectories. (p.244)

A framework that recognises the differences between these two uses of personal data, and provides appropriate protections for both, would "enable Further and Higher Education institutions to progress their use of analytics whilst managing risk to the benefit of the individual, the institution and the wider mission of education" (Kay et al., 2012, p.8). The next section suggests how such a framework can be found in European data protection law.

4. A DATA PROTECTION FRAMEWORK

While research gives consent a unique position in authorising the use of data about human subjects, under data protection law it is one of six justifications for processing personal data, set out in Article 7 of the Data Protection Directive and Schedule 2 of the UK Data Protection Act 1998. Each justification has equal status (at least under UK and EU law (Article 29 WP, 2011)) and each has its own additional requirements to protect the interests of data subjects. The Article 29 Working Party (2011) describe how a single transaction may involve processing under several different justifications. The Information Commissioner (2014) suggests that for big data analytics, the most relevant justifications are "consent, whether processing is necessary for the performance of a contract, and the legitimate interests of the data controller or other parties" (para.55) (respectively Articles 7(a), 7(b) and 7(f) of the Directive and clauses 1, 2 and 6 of the Act's Schedule 2).

Kay et al. (2012) divide processing into two categories: "Data used for institutional purposes" and "Data used for personal purposes" (p.10). In discussing Big Data, the Article 29 Working Party (2013) make the same distinction between processing to "detect trends and correlations in the information" versus situations where "an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions'

that are taken with regard to those customers" (p.46). In the former, according to the Working Party (2013) "functional separation is likely to play a key role" (p.46) in protecting individuals: in the latter opt-in consent will normally be required. The Open University give examples of each category: "modules may be redesigned to take account of topics seen to cause particular issues of understanding"; analytics may "identify points on the study path where individuals or groups may need additional support" (Open University, n.d.).

Using different justifications for the two categories – primarily legitimate interests for trends and consent for individual support – offers a much better framework for using learning analytics in university operations. In particular, stronger protection for individuals is obtained by considering the learning analytics process as two separate stages:

- the discovery of significant patterns ("analysis") treated as a legitimate interest of the organisation, which must include safeguards for individuals' interests and rights; and
- the application of those patterns to meet the needs of particular individuals ("intervention"), which requires their informed consent or, perhaps in future, a contractual agreement.

The following sections examine the implications of this separation.

4.1 Analysis

Like most other processing of personal data, the "legitimate interests" justification requires that the individual be informed what data will be processed, by whom and for what purpose(s) (Data Protection Directive, Art.10; Data Protection Act 1998, Sch.1 Part II 2(3))) The purpose of the processing must be a legitimate interest of the organisation, and the processing must be necessary to achieve that interest: in other words no "less invasive means are available to serve the same end" (Article 29 WP, 2014a, p29). Unlike the "consent" justification, however, the individual's agreement does not need to be obtained (Article 29 WP, 2014a): instead individuals are protected by the requirement that the organisation's interest must not be overridden by the individual's interests or fundamental rights (Data Protection Directive, Art.7(f)) (the UK Data Protection Act transposes this as "prejudice to the rights and freedoms or legitimate interests of the data subject" (Sch.2 6(1))). An individual with "compelling legitimate grounds relating to his particular situation" may object to processing if a different balance of interests applies in his case (Data Protection Directive, Art.14(a)).

The Article 29 Working Party (2014a) describe the legitimate interests justification as involving "an additional balancing test, which requires the legitimate interests of the controller … to be weighed against the interests or fundamental rights of the data subjects" (p.48). The Working Party (2014a) recognise that a "broad range" (p.24) of interests may be legitimate, including "the benefit that the controller derives - or that society might derive - from the processing" (p.24), so long as it "corresponds with current activities or benefits that are expected in the very near future" (p.24). But, as the Information Commissioner (2014) confirms, organisations do "need to be able to articulate at the outset

why they need to collect and process particular datasets. They need to be clear about what they expect to learn or be able to do by processing that data" (para 73). Since the Working Party (2014a) quote as legitimate a business's "interest in getting to know their customers' preferences so as to enable them to … offer products and services that better meet the needs and desires of the customers" (p.26), there seems little doubt that the interests of a university or college in improving its educational provision would qualify as legitimate. That these interests are shared by society and current and future students is recognised as "adding weight" to the interest (p.35). For example a university might wish to make one module a pre-requisite for another if analytics indicated that this combination produced better learning outcomes. However legitimate interests do not give *carte blanche* for any kind of analysis: the Working Party (2014a) warn against "creat[ing] … complex profiles of the customers' personalities and preferences without their knowledge" (p.26), since this interference with individuals' rights could not be justified.

The balancing test requires that the organisation's interest be weighed against possible harm to "all relevant interests" (Article 29 WP, 2014a, p.29) of individuals including, but not limited to, their fundamental rights. The Working Party's guidance on this is particularly helpful for conducting the analysis stage of learning analytics.

First, there must be a clear "functional separation" between the analysis and intervention processes: "data used for statistical purposes or other research purposes should not be available to 'support measures or decisions' that are taken with regard to the individual data subjects concerned (unless specifically authorized by the individuals concerned)" (Article 29 WP, 2014a, p.30). This is likely to involve both technical and organisational measures (for example confidentiality agreements and guidance to staff with access to raw data) to protect users' privacy during the analysis process.

The quantity of data collected, and access to that data, must be limited to that required to achieve the stated purpose. The Working Party (2014a) note that this "is particularly relevant … to ensure that processing of data based on legitimate interests will not lead to an unduly broad interpretation of the necessity to process data" (p.29).

Technical measures should be used to reduce the risk to individual users. Anonymised or statistical data should normally be used for analysis; where full anonymisation is not possible, directly identifying information such as names or student numbers should be replaced with key-codes, with the index linking keys to individuals stored separately and, preferably, under separate control (Article 29 WP, 2013). The Working Party (2014a) note that "The use of less risky forms of personal data processing (e.g. personal data that is encrypted while in storage or transit, or personal data that are less directly and less readily identifiable) should generally mean that the likelihood of data subjects' interests or fundamental rights and freedoms being interfered with is reduced" (p.42). Safeguards that "unquestionably and significantly reduce the impacts on data subjects" may "chang[e] the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden" (Article 29 WP, 2014a, p.31), thus allowing processing to proceed.

For example, successful combinations of modules cannot be identified using fully anonymised data as this analysis requires each student's performance to be linked across modules. However the sequences of modules and results can be constructed and analysed using key-coded data, or even one-way hashed identifiers so that there is no index that would allow an identifier to be associated with a student. Combined with organisational controls to prevent re-identification, this investigation should easily satisfy the balancing test. If the organisation wishes to intervene with individuals who have chosen a combination likely to be unsuccessful, this should be a separate process from the analysis, conducted after obtaining consent as described in the next section.

Another factor that may tip the balance is whether processing matches users' reasonable expectations of how their data will be used: "the more clearly acknowledged and expected it is in the community and by data subjects that the controller can take action and process data in pursuit of these interests, the more heavily this legitimate interest weighs in the balance" (Article 29 WP, 2014a, p.35). For a university or college to use analytics to improve the educational services it provides, benefitting both the students whose data are analysed and their successors, should not be unexpected. Indeed, as noted by Kay et al. (2012), current students may positively expect that the services they receive will respond to use, so long as this protects their interests and rights. In a Jisc workshop to identify appropriate uses of analytics students proposed personalised suggestions for those who were having difficulty engaging with course material (Sclater, 2015).

Although universities assessing the balance of rights and interests are allowed to take into account both positive and negative impacts on individuals, their close relationship with students and employees creates particular risks of harm from inappropriate processing (Article 29 WP, 2014a). Rather than run these risks, where actions may directly affect individuals it is normally better to seek those individuals' consent.

4.2 Intervention

The analysis stage itself provides much useful information for educational provision. Improvements to university facilities and processes, recruitment, courses and teaching materials are most likely to be based on aggregated or anonymised data. However learning analytics can also be used to provide support and guidance to individual students or staff. Students might, for example, be offered personalised reading lists based on how their progress compares with others' (Sclater, 2015). Here the university's aim is to affect the individual (in a positive way) so the legitimate interests justification, which requires that any impact be minimised, is no longer appropriate. Instead, intervention will normally be based on the individual's consent (the possibility of intervention being a requirement of a contract or a legal duty is discussed further below). Again, the legal requirements for consent provide helpful guidance for how this should be done.

Consent will only be valid, according to the Article 29 Working Party (2011), if there is "no risk of … coercion or significant negative consequences if [the student] does not consent" (p.12). Since a

university or college, ultimately, has the power to grant or withhold its students' qualifications, there is a risk that students will feel compelled to accept. Interventions should therefore be offered as a choice between receiving personalised support or standard educational provision. Such a choice should avoid "significant negative consequences" and thereby provide valid consent.

According to the *Data Protection Directive* consent is "any freely given specific and informed indication … by which the data subject signifies his agreement to personal data relating to him being processed" (Article 29 WP, 2011, p.5). The Working Party (2011) explain that "[informed] implies that all the necessary information must be given at the moment the consent is requested, and that this should address the substantive aspects of the processing that the consent is intended to legitimise" (p.9); and that to be specific, consent "should refer clearly and precisely to the scope and the consequences of the data processing" (Article 29 WP, 2011, p.17). These requirements are actually easier to meet after analysis has identified a pattern that may suggest a particular intervention. Students can now be given detailed and precise information on the purpose of the intervention and the implications of either granting or withholding consent for it. The Working Party (2011) recognise that consent requested "'downstream', when the purpose of the processing changes" allows information to be provided that "focus[es] on what is needed in the specific context" (p.19), rather than more general information available when data collection began. Thus, rather than obtaining general consent for "appropriate support" when a course begins, waiting until analysis of a student's performance has identified their most effective learning style lets them give fully informed consent to a particular kind of help.

Since the Working Party (2011) consider that "[t]he notion of 'indication' is wide, but it seems to imply a need for action" (p.12), some positive action by the student is required for their consent to be valid. Normally students should be invited to opt-in to an intervention but if circumstances require an opt-out approach then it might be argued that consent was obtained earlier – for example when the student signed up to the module – and that an offer to withdraw that consent was being made at the time of the intervention. This would, however, require the module description to state clearly that personalised interventions would be made. Interventions on this basis could only use personal data that were either stated or obviously relevant at the time of signing up: the information provided to the student must be such that joining "lead[s] to an unmistakable conclusion that consent is given" (Article 29 WP, 2011, p.23). A course might, for example, state that skills would first be assessed and appropriate topics then chosen to address those needing improvement.

The Working Party (2011) place no specific limit on how long consent given at the start of a module or course may be presumed to last: "[i]t should be sufficient in principle for data controllers to obtain consent only once for different operations if they fall within the reasonable expectations of the data subject" (p.17) but "as a matter of good practice, data controllers should endeavor to review, after a certain time, an individual's choices, for example, by informing them of their current choice and offering the possibility to either confirm or withdraw. The relevant period would of course depend on the context and the circumstances of the case" (p.20). However since "withdrawal … should, as a principle, prevent any further processing of the individual's data by the controller" (p.9), a student who actively

opts out of an intervention (as opposed to one who does not opt in) should not be offered further interventions, at least within the same module.

If an organisation plans to use learning analytics to intervene with individual members of staff, rather than students, then consent may not be an appropriate legal basis. If an employee "might fear that he could be treated differently if he does not consent to the data processing" (Article 29 WP, 2011, p.13) then consent will not be freely given so is not valid. Interventions with staff should therefore be limited to those that are necessary for the purpose of the (employment) contract or those where there are sufficient safeguards that, despite the strong presumption to the contrary, genuinely free consent can in fact be obtained from the employee (Article 29 WP, 2011).

Finally, intervention might possibly be required for the university to comply with a legal duty. Here any use of personal data must be limited to that strictly necessary for that purpose.

5. APPLYING THE FRAMEWORK

The framework proposed here – particularly the balancing test required by the legitimate interests justification – appears to match the responses of participants in learning analytics studies. For example Pardo and Siemens (2014) found that "the concerns of users about privacy vary significantly depending on what is being observed, the context and the perceived value when granting access to personal information" (p.440). Furthermore the balancing test protects all the rights and interests of individuals, not just privacy: the Article 29 Working Party (2014a) note, for example, that "[t]he chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration" (p.37). This section considers how the framework might inform some specific questions raised by learning analytics practitioners: historic data, small groups, fully-automated processing and sensitive data.

Pardo and Siemens (2014) identify issues with historic data: "How long will the data be kept? Will the data be used after students graduate?" (p.446). They consider long-term information "will be helpful for the university to refine its analytics models, track the development of student performance over multiple years and cohorts or simply for internal or external quality assurance processes", but retaining too much, or for too long, may well damage trust. Applying the framework: the likelihood of direct personal benefit to a student decreases once they have completed their module or course, long-term retention increases the risk of information becoming out of date or suffering a security breach. The university must demonstrate that continued processing generates sufficient benefit to balance the increased risk and decreased benefit to the individual's rights and interests; in particular, according to the Information Commissioner (2014) "[i]f organisations wish to retain data for long periods for reasons of big data analytics they should be able to articulate and foresee the potential uses and benefits to some extent, even if the specifics are unclear" (para.75). They may also need to implement additional safeguards, for example anonymisation rather than pseudonymisation (Information Commissioner, 2012). Thus processing of historic data should still be possible, given a sufficiently clear and strong

justification, but the range of acceptable purposes is likely to be narrower than for current students. Where universities wish to continue to collect data from former students – for example for the Higher Education Statistics Agency's (2015) Destination of Leavers from Higher Education survey – this relies in any case on voluntary participation so free, informed consent to continued processing of relevant historic data could be obtained at the same time.

Kay et al. (2012) note that patterns derived from small numbers of individuals represent an increased risk of accidental or deliberate re-identification. They suggest a minimum group size of twenty though the boundary between data protection and freedom of information laws has sometimes been drawn as low as five (Information Commissioner, 2012). The legitimate interests balancing test can take account of the various factors affecting the risk of harmful re-identification and ensure that all groups retain a level of protection appropriate to the risk and benefit of the processing. In most cases there will be a threshold group size below which the risk outweighs the benefits: this should indicate that such fine-grained processing should not continue.

One paradox highlighted by the balancing test is that where there is a clear benefit to the individual and a negligible risk, automated processing may invade privacy less than revealing personal data to a human mediator. Re-ordering the choice of modules based on a student's performance in previous courses might be an example of this kind of intervention. Under data protection law individuals are entitled to know of any fully-automated processing that may affect them and the logic used (Data Protection Directive, Art.12(a)); they also have the right to object to such processing (Data Protection Directive, Art.15(1)). Although the law only requires these "profiling" safeguards where there is no human mediation (European Commission, 2012, Art.20), by seeking consent at the time of intervention the framework encourages their use in both mediated and automated processes.

Pardo and Siemens (2014) consider the risks of using privacy-sensitive data in learning analytics: "[f]or example, in a hypothetical scenario, is the improvement of the overall learning environment a valid reason to record the exact location of students within the institution and share it with peers to facilitate collaborative learning?" (p.439). Location data can be processed on the basis of legitimate interests, however the e-Privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 Article 9) warns of significant privacy risks so clear benefit and strong safeguards would be needed to satisfy the framework's balancing test. Anonymised location data might, for example, be used to improve the design of learning spaces or make more efficient use of rooms, provided there was strong protection against re-identification of individuals. However Pardo and Siemens' example of collaborative learning directly affects individuals so the framework, like Art.9(1) of the e-Privacy Directive, would require individuals' free, informed consent. If information is categorised by the Data Protection Directive (Art.8(1)) as Sensitive Personal Data – for example race or religion (but not location) – then legitimate interests cannot be used even if there is no effect on the individual (Data Protection Act 1998, Sch.3(4)). A university that wished to use these categories in analysis would have to obtain the informed consent of each individual before data were collected. Such information could then only be processed for purposes and in ways envisaged at that time. Also, consent for processing

Sensitive Personal Data must be explicit and cannot be inferred from some other action (Data Protection Act, Sch.3(1)).

6. CONCLUSIONS

As learning analytics moves from a research context to become a key tool in university operations, the use of consent as the main ethical and legal guide appears inappropriate. The Article 29 Working Party (2011) warn that "[t]he use of consent 'in the right context' is crucial. If it is used in circumstances where it is not appropriate, because the elements that constitute valid consent are unlikely to be present, this would lead to great vulnerability and … would weaken the position of data subjects in practice" (p.10). Instead, following the Working Party's (2014a) guidance that it may provide "a valid alternative to inappropriate use of, for instance, the ground of 'consent' or 'necessary for the performance of a contract'" (p.49), this paper proposes a two-stage framework using the legitimate interests of the university as the legal basis for the analysis of data and informed consent as the basis for any subsequent interventions with individual students or staff. Legitimate interests provides "complementary safeguards" (Article 29 WP, 2014a, p.49) ensuring that the university's interests are continually tested against the interests and rights of individuals, that interference with those interests and rights must be minimised, and that processing must cease if they cannot be adequately protected.

This approach lets universities plan and provide their educational activities using complete relevant data, avoiding the risk of self-selection bias. It also provides strong protection for individual students and staff, providing both clear guidance on the conduct of current and new analyses and detailed, specific information when individual interventions are offered. The framework reduces the significance of the sharp legal boundary between (protected) personal data and (unprotected) non-personal data, ensuring that all processing includes safeguards appropriate to the level of risks to privacy and other interests and rights. Finally the framework should promote discussion of ethically important questions concerning appropriate topics and methods of analysis and appropriate forms of intervention, rather than a focus on legal formalities.

REFERENCES

Article 29 Working Party (2011). *Opinion 15/2011 on the definition of consent* (01197/11/EN WP187). Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Article 29 Working Party. (2013). *Opinion 03/2013 on Purpose Limitation* (00569/13/EN WP203). Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Working Party. (2014a). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (844/14/EN WP 217). Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Article 29 Working Party. (2014b). *Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (14/EN WP221). Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Clarke, G. & Cooke, D. (1983). *A Basic Course on Statistics* (London: Edward Arnold)

European Commission (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* COM(2012)11 Final

European Data Protection Supervisor (2015). *Leading by Example: the EDPS strategy 2015-2019*. Retrieved from https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Strategy2015

Higher Education Statistics Authority (2015). *Destinations of Leavers from Higher Education in the United Kingdom for the Academic Year 2013/2014*. Retrieved from https://www.hesa.ac.uk/sfr217

Information Commissioner (n.d.). *Processing personal data fairly and lawfully (Principle 1)*. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/#fair-processing

Information Commissioner (2012). *Anonymisation: managing data protection risk code of practice*. Retrieved from https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Information Commissioner (2014). *Big data and data protection*. Retrieved from https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf

Kay, D., Korn, N. & Oppenheim, C. (2012). Legal, Risk and Ethical Aspects of Analytics in Higher Education. *Cetis Analytics Series* 1(6)

Leece, R. (2013, July). *Analytics: An exploration of the nomenclature in the student experience*. Paper presented at 16th Annual FYHE Conference, Wellington. Retrieved from http://fyhe.com.au/past_papers/papers13/14E.pdf

Long, P. & Siemens, G. (2011). Penetrating the Fog: Analytics in Learning and Education. *Educause Review*, 46(5), 31-40

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701-1777

Open University (n.d.). *Using Information to Support Student Learning*. Retrieved July 9 2015 from http://www.open.ac.uk/students/charter/sites/www.open.ac.uk.students.charter/files/files/ecms/web-content/using-information-to-support-student-learning.pdf

Pardo, A. & Siemens, G. (2014). Ethical and Privacy Principles for Learning Analytics. *British Journal of Educational Technology*, 45(3), 438-450

Prinsloo, P. & Slade, S. (2013). An evaluation of policy frameworks for addressing ethical considerations in learning analytics. In *Third Conference on Learning Analytics and Knowledge (LAK 2013)* (pp. 240-244). Leuven: ACM

Richards, N. & King, J. (2014). Big Data Ethics. *Wake Forest Law Review*, 49, 393-432

Sclater, N. (2014). *Code of Practice for Learning Analytics: A literature review of the ethical and legal issues*. Retrieved July 9 2015 from http://repository.jisc.ac.uk/5661/1/Learning_Analytics_A-_Literature_Review.pdf

Sclater, N. (2015). *What do students want from a learning analytics app?* Retrieved July 9 2015 from http://analytics.jiscinvolve.org/wp/2015/04/29/what-do-students-want-from-a-learning-analytics-app/

Tickle, L. (2015, June 30). How universities are using data to stop students dropping out. *Guardian*. Retrieved from http://www.theguardian.com/guardian-professional/2015/jun/30/how-universities-are-using-data-to-stop-students-dropping-out

Wen, H. (2012, June 11). *Big Ethics for Big Data*. Retrieved from http://radar.oreilly.com/2012/06/ethics-big-data-business-decisions.html