The Big Student Big Data Grab

A. S. Weber

***Abstract*—This contribution addresses a serious emergent policy issue regarding student data privacy that has arisen in the United States the last five years due to the increasingly widespread use of cloud computing services in education and the creation of large datasets–commonly known as 'Big Data'–collected by educational online (hosted) services. Considerable confusion exists around the actual privacy protections offered by laws such as FERPA, PPRA, and COPPA in online environments, and in addition the actual use and extent of the collection of data by hosted services is not transparent. Large datasets have proven immensely valuable to for-profit corporations, and schools generate large amounts of information about students including state and federally-mandated student records. Thus technology giants such as Facebook, Google, Apple, and Microsoft as well as non-profit entities such as inBloom with strong links to for-profit companies, have been competing to gain greater access to student Big Data for the purposes of commercialization. Using two cases studies (Google Apps for Education and inBloom, Inc.), the author demonstrates that new student privacy laws are required in the U.S., and the author suggests the outlines of a federal statute.**

***Index Terms*—Cloud computing–education, big data, educational datasets, student privacy, FERPA, PPRA, COPPA.**

I. Introduction

E-learning even in its basic forms such as email and Learning Management Systems is now ubiquitous in education in developed nations. Since many students own smart phones, and tablets and laptops, electronic learning is now native to many of today's student populations. However, educators and lawmakers must continue to be sensitive to the socio-economic differences among students and provide adequate school-funded electronic access for those who cannot afford it to avoid the creation of a 'digital divide' from an early age. In addition, both developing and developed nations are moving towards Cloud Computing platforms for both teaching purposes and administrative functions. Cloud platforms (defined in Section II) provide reduced costs and reduced complexity, and lower the costs of maintaining in-house institutional datacenters and IT departments to build and maintain them.

With pay-as-you-go models, cloud services for educational institutions can be rapidly scaled up and down according to demand and an institution is therefore not burdened with outdated or unnecessary hardware and software which can be extremely costly to replace. The cloud vendor normally updates software seamlessly for the client and provides bug fixes and security patches without the user even being aware of changes to the system. Since cloud services process and store data 24/7, and shuttle tasks over networks among an array of CPUs by breaking them down into subroutines and processing them in parallel, tasks on network computer arrays are inherently faster and more efficient in logical and energy terms. Power efficiency is becoming an increasing concern in the computer industry since according to a study by Koomey, the electricity used by data centers, which includes the cloud computing industry, increased worldwide by approximately 56% from 2005 to 2010. Thus the total amount of electricity consumed globally in 2010 by data centers "likely accounted for between 1.1% and 1.5% of total electricity use" [1].

However, some cloud vendors, as well as social media sites such as Facebook which educators sometimes adapt for educational purposes, use data-mining techniques to gather Personally Identifiable Information (PII) about users in order to profile their purchasing and general preferences in a practice known as behavioral targeted marketing. Google is the world's largest online advertiser through its AdSense and Double-Click programs, with total revenues from advertising larger than the U.S. newspaper industry. Through the use of http cookies, online firms such as Google can track a user's behavior even after they leave the site that installed the cookie – thus user actions can be tracked across all web activity. Other common web tracking and information gathering technology includes: web bugs or beacons (tracking pixels, 1 × 1 GIF) and browser fingerprinting. Since every week the majority of Internet users will access one of Google's popular services such as YouTube (~20% of North American downstream Internet traffic), Google Search (3 billion searches per day), and Gmail (425 million users; Gmail Android App hit 1 billion downloads in 2014), Google is able to record and store logs of a wide variety of user initiated actions directly on its servers. Google thus possesses not only the metadata of such activity, but actual full text strings such as Gmail email contents and search engine query text. When this data can be identified with an individual device or human agent, it is extremely valuable information which can be analyzed in a myriad of ways to create a web profile or composite that reveals a user's opinions, friendship networks, virtual and real world activities, and consumer purchasing predilections.

Student purchasing trends are of particular interest to advertisers and corporations since spending patterns in youth often predict adult behavior and the corporation is in a unique position to establish 'brand loyalty' at an early age since young people are particularly vulnerable to manipulation (naïvetê).

The student educational market is big business, both due to the educational products used in schools such as textbooks

Manuscript received June 20, 2014; revised September 12, 2014.

A. S. Weber is with the Premedical Department of the Weill Cornell Medical College in Qatar (WCMC-Q), Box 24144, Education City, Doha, State of Qatar (e-mail: alw2010@qatar-med.cornell.edu).

and standardized tests, but also other products that students consume with their disposable income such as music, food, and electronics. As *Bloomberg Business Week* notes: "some children in all 50 states have schoolwork evaluated by data analytics software that tracks their progress on classroom or home computers, a growing part of what the Software & Information Industry Association estimates is an $8 billion market for education software and technology services" [2].

The large consumer data sets collected by data brokers such as Acxiom were the subject of a 2014 report by the Federal Trade Commission (FTC) which studied 9 data brokers in detail and concluded that greater transparency and accountability were needed in that industry. According to the FTC: "Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions….one of the nine data brokers has 3000 data segments for nearly every U.S. consumer" and some of this includes sensitive information that students may wish to keep confidential and private such as "Height, Weight, Cholesterol Focus, Race, Gender, Diabetes Interest, Soon-to-be High School Graduate *et al.*" [3].

White House Counsel John Podesta's 2014 report to the President on the challenges of Big Data in education raised the issue of for-profit educational corporations' collection of data, but did not offer any immediate solutions to the conflicts between current student privacy protection laws and data ownership and accountability [4].

II. Big Data and Cloud Computing: Definitions

A. Big Data

Big Data is not easily defined but in general refers to large sets of data which pose challenges to existing data processing, management or analytical software and relational databases. These datasets have arisen from the continuous recording of sensors and monitors and server logs, as well as a conscious policy of information technology companies such as Microsoft, Apple, Facebook and Google to capture any and all data that it can access, and store it, even if not of immediate use. In fact every digital device outputs data, and virtually every analogue process can be digitized. Google's mission statement reads: "Google's mission is to organize the world's information and make it universally accessible and useful"–reveals the company's global vision to be involved in every aspect of data generated in the modern world [5].

In education, Big Data allows for evidence-based and data-driven policy making and pedagogies. A recent popular account of Big Data by V. Mayer-Schönberger (Professor of Internet Governance and Regulation at the University of Oxford) and K. Cukier (Data Editor of *The Economist*) entitled *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, reviewed some of the applications of big data analytics, such as how the spread of H1N1 virus or other influenzas can potentially be tracked by analyzing search results inputted into such algorithms as Google Flu Trends [6].

Also large datasets are useful in automated learning feedback mechanisms where artificially intelligent agents can measure and track attempts at answering a question, for example, and then tailor subsequent questions to the level and ability of the student. Obviously, to train the agent, a large data set that is linked to a specific individual is critical. On an institutional level, large databases allow comparisons between schools to measure performance and adherence to state and federal legal reporting requirements.

B. Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [7]. There are three general service models: 1) Software as a Service (SaaS) – the consumer accesses applications running on a remote host; 2) Platform as a Service (PaaS) – the consumer can use tools, libraries, programming languages, *et al.* on the host computer; 3) Infrastructure as a Service (IaaS) – the consumer can take control of processing and storage, and make decisions about resources down to the operating system level, although the provider controls the underlying hardware and basic infrastructure of the cloud (which may be unknown to the user).

Mell and Grance identify four basic deployment models of the cloud, and their descriptions are provided below in full since they have important consequences for data privacy and security:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)" [7].

The private cloud provides the most user control, such as implementation of encryption, while the public cloud relies on user trust in the vendor to monitor security, avoid data breach, prevent insider access of data (malicious insider) and to abide by data privacy agreements. However, the public

cloud has been plagued by a number of problems including data breaches, surreptitious data-mining, collection of user behaviors through tracking technologies, and vague and non-transparent privacy policies.

III. Fundamentals of Student Privacy

A. Privacy

Privacy represents a complex social, legal, and philosophical concept. Some theorists believe that privacy is a fundamental, inalienable right in Western democracies. In addition, privacy may be essential to a free society in that individuals should be able to express opinions in private without the fear of consequences; otherwise they will engage in perpetual self-censorship. The Fourth Amendment of the Bill of Rights of the United States Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" [8]. This provision establishes the fundamental legal basis of laws on wiretapping and surveillance and warrants for inspections and seizures of personal documents and goods, including data. Warren and Brandeis established the legal doctrine of "the right to be let alone" in the late 19th century [9]. Privacy directly impacts Big Data and datasets containing PII and Personal Health Information (PHI), since this information can be put to use for beneficial and legitimate purposes, but also promiscuous sharing of data in addition to aggregating disparate anonymized data elements to identify a specific individual, can lead to malicious activity such as identity theft, spear phishing, profiling, cyberbullying and stalking and revelation of health status.

B. The Family Education Rights Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) or the "Buckley Amendment" was passed in 1974. The law gave parents or students over the age of 18 the right to review and amend their educational records. As originally formulated, FERPA forbade student records, with some exceptions such as "directory information," to be released to third parties.

Beginning with the *Gonzaga University v. Doe* case (2002), FERPA has been continually weakened as a means of protecting student privacy, both through judicial neglect and a change in its definitions in 2008 and 2011 by the U.S. Department of Education, as described below.

To further protect the privacy and safety of children online from data abuses, Congress passed the Children's Online Privacy Protection Act (COPPA) in 1998. The act limits the amount and kind of PII that a website can collect about a child under the age of 13. Although student privacy protections concerning data in electronic records under FERPA jurisdiction have eroded in the last two decades, COPPA protections were extended and tightened under new rules placed in effect in 2013 by the Federal Trade Commission (FTC) who oversees and administers the law. A "persistent identifier" (information used for tracking users) was included as part of a child's PII which would be subject to COPPA rules. Due to advances in face recognition software which can identify users by analyzing biometric information in images, photographs and videos were also added to the list of personally identifiable data. Since all children under the age of 13 must legally attend school in the U.S., they are thus students. However, COPPA affords more privacy protection to student data than a law (FERPA) designed to protect student records, and the laws appear to conflict if one extends the definition of educational record to cover informal learning and edutainment activities outside of school. This situation demonstrates the patchwork of sometimes conflicting laws that govern student privacy at the current time.

In addition, the Protection of Pupil Rights Amendment (PPRA) or "Hatch Amendment" protects private information that might be gathered in surveys and questionnaires from minor students in U.S. Department of Education-funded programs. Schools and contractors must obtain written parental consent to information gathering practices that might reveal data about a student's: "Political affiliations; Mental and psychological problems potentially embarrassing to the student and his/her family; Sex behavior and attitudes; Illegal, anti-social, self-incriminating and demeaning behavior…" [10].

However, the PPRA contains one clause that allows for collection of student PII without consent or opt-out provisions for educational products and services: "PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. 20 U.S.C. §1232h(c)(4)(A)" [11]. While this provision would seemingly benefit students, teachers and schools (better classroom materials), under this provision PII can be released to for-profit entities without consent; thus this loophole does not fully protect student data and additionally raises the question of why one for-profit sector (educational marketers) and not others are allowed access to this data.

The use of online educational resources and their relationship to FERPA is therefore complex. The Privacy Technical Assistance Center set up by the U.S. Department of Education as a privacy resource notes that: "Schools and districts will typically need to evaluate the use of online educational services on a case-by-case basis to determine if FERPA-protected information (i.e., PII from education records) is implicated" [12].

C. Changes to FERPA Regulations in 2008 and 2011

In 2008 and 2011, the U.S. Department of Education (ED), who is tasked by Congress to oversee and administrate FERPA, made significant changes to the law's definitions which effectively weakened the provisions of the original bill which was intended to grant parents and students control over who sees their school records. The changes were implemented in part by ED due to the "need for clarity surrounding privacy protections and data security [that]

continues to grow as statewide longitudinal data systems (SLDS) are built and more education records are digitized and shared electronically" [13]. Specifically, the definition of "directory information," "authorized representative," and "education program" were modified. The new definition of "authorized representative" allowed the release of student records without consent to any outside party contracted by the school. These parties could include data consultant companies building student records databases.

Many consumer and civil rights organizations – the ACLU, American Association of Collegiate Registrars and Admissions Officers, and the World Privacy Forum–criticized these new amendments as effectively repealing the original FERPA law, and allowing the exposure of sensitive student educational data to for-profit entities [14]. The Electronic Privacy Information Center (EPIC) launched a lawsuit in 2011 against the Department of Education regulations stating that the department did not have authority to reinterpret the law in this way against the original intent of Congress and that the changes rested on a misinterpretation of the law. The suit was dismissed in 2013 on technical grounds that the plaintiffs did not have standing to bring claims against the U.S. Department of Education.

IV. INBLOOM

The development and eventual closure of inBloom, Inc., the kind of statewide longitudinal educational data system (SLDS) company mentioned in the U.S. Department of Education's justifications for its 2011 amendments to FERPA, clarifies the possible original purpose of the FERPA modifications. inBloom, Inc. (formerly the Shared Learning Collaborative) began as a non-profit data company collaboration between the Council of Chief State School Officers and the Bill and Melinda Gates foundation, with funding from Gates and the Carnegie Foundation and Carnegie Corporation. inBloom contracted with several U.S. state education departments to implement SLDSs aligned with Common Core standards.

The data fields included in the inBloom databases sometimes contained as many as 400 unique pieces of information, going beyond the scope of the traditional data collected on students in student and administrative records. A broad coalition of educational stakeholders began questioning the propriety of gathering such an enormous amount of data on students, coupled with the new looser FERPA regulations regarding data sharing with third parties. In addition, opponents questioned the robustness of inBloom's privacy and security practices, which were not transparent.

In early 2014, New York State ended its relationship with inBloom after objections from local school boards and privacy activists. The Class Size Matters website among other parents and teachers groups had led campaigns against the project. On April 21, 2014, inBloom announced that it would be shutting down operations. In addition, eight U.S. states have passed laws in 2014 forbidding the sharing of student data with marketing firms.

At approximately the same time that New York State withdrew from participation with inBloom, it passed student data privacy provisions in Budget Bill A08556D signed into law on March 31, 2014. The bill states: "the Commissioner and the Department [New York State Education Department] are hereby prohibited from providing any student information to a SLISP and the commissioner and the department shall take actions to immediately insure that any student information provided to any SLISP shall be deleted from such SLISP and destroyed in a secure manner" [15]. A SLISP is defined in the bill as "any entity that collects, stores, organizes, or aggregates student information and contracts with or enters into an agreement with the department for the purposes of providing student information to a data dashboard operator for use in a data dashboard" which clearly refers to inBloom's SLDS developed for New York State, although not by name [15]. The bill further provides for the appointment of a Chief Privacy Office in the Department of Education. Also, the bill specifies that "personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold or used for marketing purposes" [15].

V. GOOGLE APPS FOR EDUCATION

In order to capture the growing educational markets for software, Google introduced its Google Apps for Education and Microsoft Corporation developed its Office 365 Education. Both suites of applications are web-based and offer functionality such as spreadsheets, calendars, instant messaging, word-processing, emails, and document-sharing which before the availability of cloud-based applications (SaaS or Software as a Service) were supplied by purchased software programs running on a local client computer. Google Apps for Education bundles several stand-alone current and former Google products such as Gmail and Google Docs.

Google Apps for Education is built on a familiar business model – businesses pay subscription fees to use the App suites, while use is free for educational organizations. Students become familiar with these applications and Google expects that they will continue to use them in their adult working lives, creating customer loyalty. Apple Corporation used a similar strategy in marketing the Apple II computer in the 1980s by offering large discounts to secondary educational institutions in the hope that students would become dedicated Apple users.

Through service level agreements as well as through misleading statements by Google spokespersons, many educational users believed that Google Apps for Education were exempted from scanning and data-mining. These technologies are employed by Google in order to return targeted advertisements to the user's computer based on key-word analysis of Gmail text aggregated with other user behaviors from the use of Google services (aggregation). In documents filed in a class-action suit against Google for allegedly violating federal wiretap laws, Google admitted to scanning student emails even when users or institutions elect not to participate in the targeted advertisement program. According to a Google spokesman, Google "'scans and indexes' the emails of all Apps for Education users for a

variety of purposes, including potential advertising, via automated processes that cannot be turned off — even for Apps for Education customers who elect not to receive ads" [16].

On April 30, 2014, Bram Bout, Director of Google for Education, announced on the Google Official Enterprise Blog that: "We've permanently removed all ads scanning in Gmail for Apps for Education, which means Google cannot collect or use student data in Apps for Education services for advertising purposes" [17]. Bout also promised that scanning would be turned off in the future in other Google Apps enterprise suites for Business and Government. The decision may have been in response to the wiretap lawsuit, or due to mounting criticism of Google's student privacy practices.

VI. Conclusion

As data storage and computing power continue to drop in price, and Cloud Computing becomes more efficient, the amount of data that is captured, analyzed and stored will continue to increase. Algorithms for extracting useful information from this data will additionally become more sophisticated as this emerging area of mathematics and logic is well funded with support from governments, the military, and private corporations. The old adage that knowledge is power, and the corollary that power is money, holds true with respect to Big Data sets, which reveal numerous facets about individual lives. However, several specific dangers lie in so much aggregated data, particularly if one actor holds more information than another: this allows the data holder to exercise considerable economic, social and political power over the less knowledgeable actor.

Clearly the technological developments in Cloud Computing and big data collection will not stop and large multi-billion dollar technology firms have built business models on the collection and sale of personally identifiable information. The PII contained in student records simply represents another potential source of revenue for them. The U.S. has in the past relied on a data collection industry self-policing regulatory environment with little government intervention [18]. In the author's view, the only solution to the responsible and ethical use of this sensitive data, however, is comprehensive legal protection for data holders with an enforcement mechanism. Two recent frameworks for student data privacy rights have recently been proposed: Weber's Principles for a Proposed Student Privacy Law based on medical ethics human subjects protection regulations and EPIC's "Student Privacy Bill of Rights" (Appendices I and II). Weber's proposed principles for a federal omnibus student privacy law entitled "Proposed Omnibus Federal Student Data Privacy Protection Law" were based on medical ethics principles embodied in the 1979 Belmont Report [19].

Clearly, since using student PII for commercial purposes without user consent or opt-out options fundamentally conflicts with laws designed to protect student data and student records, some form of enforceable legislation needs to be introduced. A federal law is preferable, due to the many unique state laws now in force, which often were passed in response to a specific case of data abuse and therefore lack general applicability.

Appendix

A. Student Privacy Bill of Rights

The following "Student Privacy Bill of Rights" was suggested by Khaliah Barnes in an article in the *Washington Post* [20]:

1) Access and Amendment: Students have the right to access and amend their erroneous, misleading, or otherwise inappropriate records, regardless of who collects or maintains the information.
2) Focused collection: Students have the right to reasonably limit student data that companies and schools collect and retain.
3) Respect for Context: Students have the right to expect that companies and schools will collect, use, and disclose student information solely in ways that are compatible with the context in which students provide data.
4) Security: Students have the right to secure and responsible data practices.
5) Transparency: Students have the right to clear and accessible information privacy and security practices.
6) Accountability: Students should have the right to hold schools and private companies handling student data accountable for adhering to the Student Privacy Bill of Rights.

B. Appendix II: Weber's Proposed Privacy Statute Principles

Appendix II: Weber's Proposed Privacy Statute Principles

Medical Ethics Principle	**Principles for Proposed Student Privacy Law**
Respect for persons	individuals should be allowed to make decisions about their data and those with diminished autonomy should be protected (i.e. under-13s as per COPPA)
Beneficence	individuals should not be harmed by usage of their data; harms should be minimized and benefits maximized
Justice	individuals should receive adequate compensation for use of their data commensurate with the benefits accruing to the user of the data
Informed consent	data subjects should be clearly informed at the point in time of collection in plain language policies about how their data will be collected and used, including potential reuse and re-identification
Information	subjects should know of anticipated risks and benefits, have the opportunity to ask questions, and be able to opt-in, or withdraw data (opt-out) if misuse occurs
Comprehension	subjects must fully understand the implications of usage of their data by second and third parties
Voluntariness	data cannot be gathered under duress or conditions of deceit
Additional Principles	**Principles for Proposed Student Privacy Law**
Enforcement	privacy infractions by data holders should carry substantive penalties, such as a percentage of annual revenue, as proposed in European regulations, and be adjudicated by law
Context	subjects should be informed when data is used outside of the original context in which it was gathered
Correction	data subjects should have the right to examine their PII upon request and correct it

ACKNOWLEDGMENT

The author would like to thank the Weill Cornell Medical College in Qatar, Qatar National Research Fund and Qatar Foundation for Education, Science and Community Development for providing funding and travel monies for presentation of this research. Cornell Statement of Research Compliance: The author reports that he has no financial, research or personal conflicts of interest related to this research. The following is original work not published elsewhere. No human or animal subjects were used in the course of this research. The views expressed are those of the author and not necessarily those of Weill Cornell Medical College in Qatar, Cornell University or Qatar Foundation for Education, Science and Community Development.

REFERENCES

[1] J. G. Koomey, *Growth in Data Center Electricity Use 2005-2010*, Stanford, CA: Analytics Press, 2011.
[2] O. Kharif. Privacy fears over student data tracking lead to inBloom's shutdown. *Bloomberg Business Week.* [Online]. Available: http://www.businessweek.com/articles/2014-05-01/inbloom-shuts-down-amid-privacy-fears-over-student-data-tracking
[3] Federal Trade Commission (FTC), *Data Brokers: A Call for Transparency and Accountability*, Washington, D.C., FTC, 2014, pp. 24-25.
[4] J. Podest *et al*., *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, Washington, D.C., 2014, pp. 24-27.
[5] Google. Company Overview. [Online]. Available: http://www.google.com/about/company/
[6] V. Mayer-Schönberger and K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston: Houghton, Mifflin, Harcourt, 2013.
[7] P. Mell and P. Grance, *The NIST Definition of Cloud Computing, Special Publication 800-145*, Washington, D.C.: The National Institute of Standards and Technology (NIST), 2011.
[8] U.S. Constitution. 4th Amendment. Cornell University Law School Legal Information Institute. [Online]. Available: http://www.law.cornell.edu/constitution/fourth_amendment
[9] S. Warren and L. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193-220, 1890.
[10] U.S. Department of Education (ED). Protection of Pupil Rights Amendment (PPRA). [Online]. Available: http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html
[11] U.S. Department of Education (ED), *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, Privacy Assistance Technical Center, 2014, p. 6.
[12] U.S. Department of Education (ED), *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, Privacy Assistance Technical Center, 2014, p. 3.
[13] *Federal Register*, vol. 76, no. 232, Friday, December 2, 2011.
[14] E. Bennet and A. S. Weber, "Current climate of cloud computing in New York State: Concerns of student PII (data) & private vendor platforms, applications and services," *Forthcoming*.
[15] *State of New York Senate-Assembly*, S. 6356—D/A. 8556—D., January 21, 2014.
[16] B. Herold, "Google under fire for data-mining student email messages," *Ed. Week*, vol. 33, no. 26, p. 1, 19, 22-23, March 2014.
[17] B. Bout. (2014). Protecting students with Google apps for education. Google Official Enterprise Blog. [Online]. Available: http://googleenterprise.blogspot.ca/2014/04/protecting-students-with-google-apps.html
[18] A. Weber, "Cloud computing in education," in E. Sampson *et al*., eds., *Ubiquitous and Mobile Learning in the Digital Age*, New York, Springer, 2013, pp. 19-36.
[19] A. Weber, "Suggested legal framework for student data privacy in the age of big data and smart devices," *Forthcoming*, 2014.
[20] V. Strauss. (March 2014). Why a 'student privacy bill of rights' is desperately needed. [Online]. Available: http://m.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/

A. S. Weber is an associate professor of English. He teaches the first-year writing seminar in humanities in the pre-medical program at Weill Cornell Medical College in Qatar (WCMC-Q). The Weill Cornell Medical College in Qatar is a branch campus of the Weill Cornell Medical College in New York City, New York and offers an American M.D. degree in the Middle East. WCMC-Q is a member of Education City sponsored and built by Qatar Foundation for Education, Science and Community Development in Doha, Qatar, a consortium of programs affiliated with internationally ranked American, British, and French universities.

Dr. Weber previously taught literature, writing, and the history of science and medicine at Cornell University, Ithaca, The Pennsylvania State University, and Elmira College. His research interests include language, history, and the social and cultural dimensions of science and medicine. He is the editor of *19th Century Science* (2000), and *Because It's There: A Celebration of Mountaineering Literature* (2001), and is the author of specialized publications on Shakespeare, women in medicine, and 17th century medicine. His current research interests include education, e-learning and the sociology of Arabian Gulf.