TESTIMONY OF JANE LAUER BARKER, ESQ.
PITTA & GIBLIN LLP

PUBLIC HEARING ON
DISCLOSURE OF PERSONALLY IDENTIFIABLE STUDENT INFORMATION BY SCHOOL DISTRICTS AND STATE EDUCATION DEPARTMENT

BEFORE

NEW YORK STATE ASSEMBLY
COMMITTEE ON EDUCATION
ROOM 513, CAPITOL
ALBANY, NEW YORK 12248

November 20, 2013

Good morning, Madam Chairwoman, and other members of the Committee on Education who are here today. I want to thank you for allowing me the opportunity to speak on the issue of the disclosure of personally identifiable information of students by school districts and the New York State Education Department.

My name is Jane Lauer Barker. I am a partner in the law firm of Pitta & Giblin, LLP and the attorney representing a group of parents and legal guardians who recently filed an Article 78 proceeding against the Commissioner of the State Education Department and the Board of Regents seeking to enjoin the mass disclosure of personal data about their children to inBloom, Inc., a private corporation, as a violation of the New York State Personal Privacy Protection Law, contained in section 96 and related sections of Article 6-A of the Public Officers Law.

My firm is also counsel to Local 372 New York City Board of Education Employees, some of whose members are petitioners in this lawsuit. The members of Local 372 are the hard-working non-teaching employees of the New York City public school system; they are parent coordinators, school aides, school crossing guards and substance abuse prevention and intervention specialists and counselors. They are also parents and legal guardians of New York City public and charter school

students who have deep concerns about the State Education Department's disclosure of sensitive information about their children to inBloom where it will be stored on a virtual cloud and no longer under the control of their local school districts. The President of Local 372, Santos Crespo, and the Union's Executive Board members are strongly in support of privacy protections for their members and their members' children.

The student information that the State Education Department intends to release to inBloom is generally considered to be subject to the strictest privacy protections under federal and state law requiring parental consent for disclosure. With respect to its disclosure of student personal information to inBloom, however, the State Education Department has expressly withheld from parents the right to consent on behalf of their minor children.

What is striking about the State Education Department's position is that it comes at a time that other governmental entities are strengthening restrictions on the disclosure of personal information of children.[1] The dangers of commercial exploitation and worse through digital breaches of

[1] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6508 (2013); Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), http://www.ftc.gov/opa/2012/12/coppa.shtm; Dave Heller, *Florida Moves to Restrict State Database on Public School Students*, 10 News Tampa Bay (Apr. 15, 2013 7:28pm), http://www..wtsp.com/news/education/article/311274/11/FL-moves-to-restrict-state-dadtabase-on-students.

children's privacy rights have become almost universally recognized. Yet, here in New York State, the Education Department has embarked upon a massive student data sharing program with inBloom that will create a substantial risk of exposure of New York State students' personally identifiable information ("PII") to commercial use and identity theft and potentially harm students' future educational and career opportunities.

[The Current System]

Local school districts throughout New York State have, for decades, maintained password-protected, secure student information management systems. The current student data system in New York State is operated with in-house expertise in which local school districts own and control their student data and are required to provide only limited personal data to the State Education Department for purposes of analysis and federal and state reporting requirements. This is implemented through a secure system in which data is extracted and transferred by local school districts to the State controlled Regional Information Centers ("RICs"), including County Boards of Cooperative Education Services ("BOCES"). The State-required data are securely uploaded from the RICs or BOCES to the State's Student Information Repository System or "SIRS". (N.Y. State Educ. Dep't, SIRS Manual for Reporting Data for the 2013-2014 School Year, Version 9.0, at

6-8 (Sept. 30, 2013), http://www. p12.nysed.gov/irs/sirs/; *see also*, N.Y. State Dep't of Educ., Mem. of Ken Slentz to Board of Regents, at 2 (Apr. 11, 2013)). A local school district on Long Island, for example, will transfer student data by electronically instructing its system to extract and load specified data elements to Nassau County BOCES, and Nassau County BOCES will then securely upload that data to SIRS. The State uses SIRS to develop the New York State School Report card required by *No Child Left Behind,* meeting federal reporting requirements and other State needs for individual student data, and informing policy decisions. The SIRS manual and operating procedures incorporate federal and state privacy law compliance protocols.

[The inBloom Plan]

The State Education Department's Service Agreement with inBloom commits the State and its local school districts to outsourcing the storage and processing of all student educational data to inBloom. That company is set to receive from the State Education Department and local school districts up to 400 pieces of student data, including student names, test scores, home addresses, grades, disciplinary and attendance data, economic and racial status, and "program participation," including whether

or not a student is entitled to special education services, English language learner services, or other accommodations or modifications.

The inBloom agreement allows inBloom to load and store the students' information on a cloud hosted and managed by inBloom or by vendors of inBloom, including Amazon.

The State is using Race to the Top Funds to require that local school districts access that data uploaded to inBloom through one of three "data dashboards" offered by third-party vendors. (EngageNY Portal FAQ (revised Oct. 30, 2013), http://www.engageny.org/resource/engageny-portal-faq#one). However, as a result of the inBloom Agreement, *all* local school districts, including those not receiving Race to the Top grant money will lose the right to control the storage and disclosure of their students' personal data. (EngageNY Portal FAQ) ("If your district does not participate in RTTT, the statewide data set will still be provided to inBloom for contract purposes . . . .").

[Current Legal Framework]

Both federal law and state law contain provisions that protect student personal information from disclosure. The Family Educational Rights and Privacy Act ("FERPA") provides parents with some degree of control over the disclosure of information from their children's educational records, and

generally prohibits the nonconsensual disclosure of student personal educational records. 20 U.S.C. § 1232g (2013). FERPA does not permit the release of education records or PII contained therein unless enumerated statutory exceptions are met. § 1232g(b). In 2011, the U.S. Department of Education unfortunately loosened the privacy protections provided under FERPA by expanding the exception for nonconsensual disclosure of PII to include any entity designated by a State or local school district, even entities that are not under their direct control, to conduct any audit, evaluation, compliance or enforcement activity. While there is considerable question whether the State's agreement with inBloom can pass muster under FERPA, the only remedy for a violation of FERPA is the withholding of federal funds by the U. S. Department of Education to a state or local educational agency. We can find no examples of the U.S. Department of Education ever having done so.

New York State has its own comprehensive personal privacy law which applies to any person about whom personal information has been collected by any governmental entity. Enacted in 1983, Article 6-A of the Public Officers Law, also known as the Personal Privacy Protection Law ("PPPL"), governs the management of records maintained by State agencies and to protect the privacy rights of persons to whom those

records pertain. N.Y. Pub. Off. Law, Art. 6-A. The legislative memoranda in support of that law pointed to the "inherent danger in permitting unchecked use of high speed data systems which contain the personal information about millions of New York State citizens." (Memorandum in Support of S. 6936, N.Y. State Senate, 652-53 (1983)).

Section 96 of the PPPL specifically governs the circumstances under which personal information may be disclosed. [2] Under the PPPL, no agency may disclose any record or personal information unless such disclosure is (a) pursuant to . . . the voluntary written consent of the data subject . . . . or (b) if such disclosure is necessary to the performance of their official duties pursuant to a purpose of the agency required to be accomplished by statute or executive order or necessary to operate a program specifically authorized by law[.] § 96(1)(a), (b). The PPPL allows an aggrieved party to challenge an agency's action in an Article 78 proceeding pursuant to Section 97 of the PPPL and places the burden of proof on the party defending the action. §§ 97(1), 97(2).

It is the contention of the parents and legal guardians in our lawsuit that because the State Education Department failed to obtain consent for the extensive disclosure of PII to inBloom and because such disclosure is

[2] The PPPL uses the term "personal information," while the inBloom Service Agreement and standard industry practice use the term "personally identifiable information" ("PII"). These terms essentially are interchangeable.

not necessary to the operation of any educational program authorized by law, the agreement with inBloom must be declared null and void and any disclosure to inBloom and any other vendors of the personal information of New York State schoolchildren enjoined.

The State Education Department has, however, taken that position that consent is unnecessary because private information is given up when parents register children for school and that, were parents allowed this right, it would be "impossible—or extraordinarily more expensive—to conduct much of the day-to-day management work of schools." (EngageNY Portal Fact Sheet, http://usny.nysed.gov/rttt/ data/enyp-parent-fact-sheet.pdf (updated Nov. 3, 2013)).

However, the State is ignoring the fact that "day-to-day management work of schools," as well as collection and maintenance of student data, has on the whole been left to the individual school districts themselves, and that parents always have had the right to control the manner in which information about their children—and themselves—is utilized. Their privacy interests surely outweigh any justifications relating to school management.

Based upon its public pronouncements, it appears that the State Education Department seeks to implement transfer of student PII to inBloom—and bypass obtaining parental consent for such use—on the

grounds that the disclosure is "necessary to operate a program specifically authorized by law." As such, the State intends to join issue in our lawsuit, making it clear that it does not consider itself constrained by current state law from disclosing any and all student personal information to inBloom.

Based on our examination of the issues, however, nothing in federal or state education law necessitates the State's use of inBloom for any purpose, and the State Education Department as of yet has not offered any reasoning or justification for why broad disclosure to inBloom is, as the law requires, necessary to the operation of any program. The State Education Department does claim that use of inBloom is part and parcel of a data infrastructure requirement of the U.S. Department of Education's Race to the Top program. However, based on our examination, there is nothing in Race to the Top regulations, or in New York State's application for Race to the Top funding, or in any other federal law or regulation, that mandates either the use of inBloom to fulfill the program's requirements, or the mass transfer of PII to a third party such as inBloom, and its vendors, for storage and processing.

Federal law does require that state recipients of education grants establish a "statewide education longitudinal data system" (LDS) to track student progress through the school system. America COMPETES Act, 20

U.S.C. § 9871(e)(2) (2013) ("Competes Act"). However, the Race to the Top grants merely requires that a state's LDS include twelve data points that are set forth in the Competes Act. Neither the Competes Act nor Race to the Top requires the State to utilize inBloom—or any third-party data host or processing vendor for that matter. Further, the Competes Act sets a floor of the minimum data elements that school districts must disclose to state education agencies. Here, the State has taken it upon itself to disclose data well above and beyond such requirements. The State Education Department seeks to provide inBloom and potentially other third party vendors with ***everything*** from disciplinary records to attendance records to economic status to whether students get free lunch, and much more. Thus, the State has reached far beyond federal requirements in disclosing data to inBloom, and cannot justify doing so based on federal laws and programs.

Furthermore, conspicuously lacking from New York's Race to the Top application was any mention of the State's intent to upload all student PII into a private, third party database. Indeed, the State Education Department represented to the federal government in its application that the State would "continue to develop the capacity and infrastructure of our regional data networks" and that SED would "pull relevant data from

regional networks on a periodic and as-needed basis." Thus, the State, at least at some point, fully intended to keep its current infrastructure of data management in place, not outsource the storage and processing of PII to inBloom. As noted, many school districts already have their own student information management systems which they populate with data stored on their premises; other districts input student data directly into governmentally controlled Regional Information Centers ("RICs") and other established governmental entities to upload data to SIRS. Thus, as the State Education Department well knows, many school districts already meet the stated Race to the Top requirement to ensure implementation of "data systems to support instruction." The practices of these districts demonstrate that uploading information to inBloom for subsequent download back to data dashboards is completely superfluous and unnecessary.[3]

In addition to the simple fact that the State Education Department is not required to disclose student PII generally to inBloom, some of the information SED looks to disclose is of a highly sensitive nature. Never has

[3] Even a data dashboard manufacturer has stated that inBloom is not necessary to populate data into data dashboards. Jefferson County, Colorado—one of the last inBloom pilot school districts—is planning to invest in a data dashboard being built by LoudCloud Systems. LoudCloud's CEO stated that inBloom is not necessary for the dashboard to work—and that LoudCloud "might be perfectly fine working with these school districts directly[,]" because the system could pull information directly from the existing data storage system. Notably, on November 7, 2013, the Jefferson County school board voted to sever ties with inBloom due to parental concerns regarding safety and security of student PII.

such information been accessible to any and everyone, even within a given school itself. For example, a student with a disability may have an "individualized education plan" ("IEP"). Currently, IEPs are closely held, and the only people with access are parents and essential staff and faculty. Yet when the State begins using inBloom to hold and process data and to populate data dashboards, that limitation will end. Disciplinary history is another example of information not normally widely disclosed. With use of inBloom, both these and other sensitive bits of information will now be one or two clicks away from access. Parents are rightly concerned with the ramifications of such availability. A student with an IEP may be stigmatized, or detrimental harm may come to a student's educational opportunities if a college or program got hold of certain information. Further, since a given student's PII may contain medical information, broad disclosure may also run afoul of § 96(2)(b) which absolutely prohibits the disclosure of medical information unless required by law. The State never disclosed this information in the past because of its sensitive nature and because of the harm that could come to students, and it has failed to explain how such disclosure is now reasonably related to its goals of analyzing educational data, implementing actions to improve student education, and increasing efficiency. Neither vague policy goals nor

obsessive focus on statistical assessments can justify such a radical intrusion into students' privacy.

The trampling of privacy rights of millions of children and their parents through mass disclosure of students' PII to inBloom is made even worse because of the manner in which SED has agreed to allow inBloom to maintain data once it is transferred to inBloom—namely, through use of cloud computing. The cloud has become an increasingly popular way for companies to store data and information. However, the cloud has many well-known susceptibilities that make it clear that the PII of millions of children should not be in such a vulnerable location. There have been numerous instances in recent years of PII exposure, whether because of malicious attacks or through inadvertent exposure. For example, in 2009, Google inadvertently shared user documents with user contacts that did not have access to them. In 2011, over 100 million Sony customers had their accounts exposed when Amazon.com's cloud system, which Sony used to host its accounts, was hacked. Most recently, Adobe Systems, Inc. had nearly 3 million credit card numbers exposed through a malicious attack. These systems all have in common the use of cloud computing to store sensitive information. Google, Amazon, and Adobe, three web and software giants, certainly have stringent security policies in place to protect

user accounts and private information. However, not even the technological savvy of these three market leaders could stop the disclosure of sensitive information to the world. Why parents should feel secure that inBloom has security measures on par with them is unclear.

Additionally, while I believe that parental consent must be the touchstone of any law or regulation in the area of student privacy, I also note that the State's agreement with inBloom is simply inadequate and defective under the PPPL. It, for example, does not contain an enforceable data privacy and security policy detailing the requirements inBloom must meet to protect PII from disclosure of any kind. Its Service Agreement does not commit inBloom to any liability for security breaches, other than requiring notification to SED that a breach has occurred. InBloom is not even required to notify parents of a breach. InBloom's Service Agreement places the onus of disclosure of PII by a third party upon the State itself, and does not require inBloom to ensure that third-party vendors comply with privacy and security laws. Yet parents and guardians are supposed to accept that their children's PII will be secure simply because inBloom says it will be.

Cyberattacks and inadvertent disclosures are so malicious precisely because they cannot be predicted and cannot necessarily be avoided. The

State Education Department's claim that storing all students' PII in one central cloud location is secure is naïve at best. Yet it is telling that New York is the only remaining state centralizing all public and charter school student PII with inBloom. The Education Department has attempted to deflect attention from these issues by stating that Social Security numbers will not be provided to inBloom for storage on its cloud. However, it does not address protection of the multitude of other identifiable information that will be provided to inBloom. The information collected by school districts about children and their families is extensive—information that may be much more valuable to third parties, whatever their intent. It is impossible to remove private information about oneself from the Internet, from collective memory, or from the hands of a malicious party.

The State Education Department's willingness to trust the most highly-sensitive information about New York State students to a still-unreliable technological form, when more secure methods exist, is ill-conceived and unwarranted. The Department has claimed that the current "hodge podge of security measures from every school district across the State . . . weakens security." However, it ignores one glaring point, reinforced by the myriad public reports of data breaches: centralization of data makes a security breach that much more serious. Because data will

be centralized on inBloom's cloud, even the most minor breach—whether malicious or otherwise—has the potential to affect millions.

Furthermore, contrary to the PPPL, the State has not established or made public a data retention policy, which § 94(1)(i) of the PPPL requires it to do. The PPPL states that "[e]ach agency that maintains a system of records shall . . . (i) establish rules governing retention and timely disposal of records in accordance with law[.]" *Id.* To date, the State has not made public any enforceable data retention and destruction policies related to PII to be disclosed to inBloom. It is unclear what happens to a student's information if, say, he or she graduates, moves out of state, or transfers to private school. Alternatively, suppose a student is arrested for a crime, though his or her criminal record ultimately is expunged. Does the criminal activity remain in his or her educational file on inBloom? Does the Department modify the educational record and have inBloom's data updated? Perhaps the State Education Department will request that inBloom delete the PII of a student upon such events. However, at this time, parents have no way of knowing whether or not their children's PII is secure—meaning deleted—once they are no longer part of the State's educational regime. For all intents and purposes, a student's PII could live

on the inBloom cloud forever, which could have lifelong ramifications for them.

Thank you again for the opportunity to speak today. I commend the Assembly Committee on Education for convening this hearing to renew attention to the very serious concerns of parents, legal guardians and their children about the privacy of their personal information and the disclosure of that information by the State Education Department to a private contractor. It is imperative that the Legislature not wait until the data breaches occur before examining the current student data system, the wisdom of the State Education Department's agreement with inBloom, and enacting appropriate legislation to ensure that student personal information is fully protected.

* * * * *