



NEW YORK STATE SENATOR

Jack M. Martins

## From the Desk of Senator Jack M. Martins

JACK M. MARTINS January 23, 2014

| ISSUE: **EDUCATION, LOCAL GOVERNMENT**

| COMMITTEE: **LOCAL GOVERNMENT**

### **Making “Targets” of our children**

No doubt you’ve seen the full page ads that Target recently placed in major newspapers around the nation. The massive retailer was apologizing to the 110 million customers who likely had their credit information stolen in one of the largest security breaches in retail history. If you shopped at Target before Christmas (unnamed members of my family practically lived there) then you may have been affected. By Target’s own admission, the hackers may have stolen credit and debit information from 40 million shoppers and personal data from another 70 million. Under pressure from the U.S. Attorney General’s office, they’re even offering a year of free credit monitoring to all of their customers in the hopes of mitigating the situation. Yet none of that, however well-intentioned, will fix the damage now.

This incident makes it abundantly clear that everyone is vulnerable, even billion-dollar corporations that spend millions of dollars on cyber-security and assign droves of people to the task. Unfortunately, it’s the world we live in, but it should make all of us more vigilant about sharing sensitive data. That’s why I cringe when I think of New York Education Commissioner Dr. John King’s plan to share our children’s personal data.

By way of background, as part of the ever less-popular Common Core initiative, Dr. King signed an agreement with InBloom, a nonprofit corporation in Atlanta. Their job is to collect student information from school districts and store it in a data cloud, supposedly making

educator access easier so that it might be more effectively used for the students' benefit, while protecting it with hopefully hack-proof encryption. The problem is they can't and won't promise us that it's safe. In fact, their contract specifically states that they cannot be held liable for any data breaches.

And what data it is! The number of fields tops a mind-boggling 400. There are obvious things like attendance, grades, courses, learning disabilities and the like. But the New York Times reports that it includes fields that are, in my opinion, absolutely intrusive like: family relationships ("foster parent" or "father's significant other") and enrollment changes ("withdrawn due to illness" or "leaving school as a victim of a serious violent incident"). There are even disciplinary fields like "perpetrator," "victim" and "principal watch list." Controversial labels to be sure. And while a parent may want educators to know these details, why would an unaccountable, third-party, commercial vendor who has no direct contact with their children have it?

You guessed it. Somewhere, somehow, someone is making a buck. InBloom's plan is to sell access to this enormous stockpile of data to vendors who would then design and market customized education software, apps for smart phones, and even video games to those very same schools, parents and children. They claim that data-driven education will eventually be a help to our children – and that may be so – but at what cost? Is our children's privacy worth it?

Parents everywhere, myself included, are up in arms. In fact, of the nine states that signed onto this plan, only three remain: Colorado, Illinois, and unfortunately, New York. Worse still, our state education department has already sent along the data for most of our 2.7 million students. Keep in mind that most local school districts have no privacy policy in place regarding this data sharing or even an opt-out for concerned parents. That's because the federal law that previously required schools to obtain parents' permission when sharing data

was conveniently changed. They no longer have to alert parents if sharing it with a company with whom they have a contract. I can't help but recall the words of our forefather James Madison to be wary of "the abridgment of freedom of the people by gradual and silent encroachments by those in power."

To be sure, districts already share data for very specific tasks but in no way should that be interpreted as blanket authorization to turn such specific data over to a private vendor. It's wrong. As I've told my daughters time and again – once something is posted online, it's out there forever, period.

Unfortunately, nowhere in this process do we, as parents, have a voice. Commissioner King's anemic response was to suspend implementation of the program until March. This does nothing to address our privacy concerns but is a disingenuous attempt to delay action with the hope that it will all blow over. It won't.

We are charged with protecting the welfare of our children and we will. That's why I'm co-sponsoring a bill in the Senate that will make it illegal for New York school districts to share this data without first obtaining parental consent. I encourage you to stay informed and engaged and together we'll prevent our kids from becoming the next "Target".