LOS ANGELES
Daily Journal
www.dailyjournal.com
THURSDAY, MARCH 3, 2016
PERSPECTIVE

Release of student information raises questions

By Ariana Seldman Hawbecker

Notices sent by school districts last month to parents of California public school children have caused concern regarding the potential disclosure of sensitive student information, including Social Security numbers.

The notices arise of out of a federal lawsuit filed in Sacramento in 2011, *Morgan Hill Concerned Parents Association and Concerned Parents Association v. California Department of Education* (CDE). The plaintiffs are groups of parents of schoolchildren with disabilities who accuse the CDE of violating students with disabilities' rights to receive a "free and appropriate public education" under the Individuals with Disabilities Education Improvement Act (IDEA).

The plaintiffs allege CDE's systematic noncompliance with IDEA. They want the court to order CDE to adopt and implement monitoring, investigative and enforcement systems to measure and ensure that the educational needs of students with special needs are met. CDE claims that its data collection and monitoring systems exceed federal requirements. These allegations trigger a call for the analysis of the CDE's data processes and procedures, implicating data on California public students.

The recent disclosure notices stem from a federal court in Sacramento ordering CDE to produce data. The court rejected CDE's contention that the plaintiffs were not entitled to data covering all of California because the case alleges state-wide, systemic violations rather than particular children's rights. It also rejected CDE's argument that the plaintiffs' right to information should be limited to children with disabilities because the plaintiffs' allegations against CDE include a "failure to locate, identify and refer children with disabilities." While CDE objected to the production as privileged under various privacy laws, the court held that it failed to specify how the information sought violated any of these provisions. The court provided that if CDE could show that these privileges applied through proper factual support, then CDE could renew its objections.

The court entered a separate order regarding information covered by the Family Educational Rights and Privacy Act (FERPA). The order requires CDE to post a notice and objection form on its website and ask special and local education agencies to do the same. This notice provides, in relevant part: "to prove their claims, Plaintiffs have requested that the California Department of Education (CDE) disclose subject to a Protective Order discussed below, information that it stores on databases and network drives that contain protected personal information of children. Examples of information that is stored on CDE's databases and network drives includes name, social security number, home address, … behavior and discipline information … information on suspension and expulsions, and results on state tests."

The notice further explains the right to privacy under the Family and Education Rights and Privacy Act (FERPA) and the IDEA and explains that only the parties, their attorneys, their consultants, and the court may have access to the data, and that it will be returned or destroyed at the end of the lawsuit. The notice clarifies that "[n]o student's identifying records will be disclosed to the public."

The court ruled that any production of sensitive student information must follow the protective order and e-discovery protocol already in place in the case. The protocol details the processes and procedures for production of data by CDE. The protocol recognizes the "highly sensitive" nature of the student data and that a breach could have notice implications costing "millions of dollars." As such, plaintiffs' counsel were required to conduct a "third party risk assessment of their IT infrastructure and protocol for storing, transmitting and using the data."

Following that assessment, the plaintiffs, along with the special master appointed by the court to oversee the discovery, are required to implement safeguards that may include full disk encryption and logging of access to sensitive data. The plaintiffs are also required to maintain a record of each device used to store or access the data, and all persons granted access. Further, all sensitive data transmission must be on a fully encrypted drive with the keys stored and transmitted separately from the hard disk.

In a Feb. 19, 2016, filing, the plaintiffs accuse the CDE of misleading the public in connection with the objection disclosures. They claim that CDE has published a number for parents to call that routes them to CDE employees who have encouraged them to lodge objections with the court. In addition, parents have complained of receiving "robo-calls" from their district warning of the release of information that appear to encourage them to opt out. Also, the plaintiffs complain that news organizations have been led to believe that the Social Security numbers of all California students will be made public. The plaintiffs claim that they do not understand that Social Security numbers will be disclosed and that, even if they were, there are stringent security measures in place to protect the disclosure from the public. However, on their website, the plaintiffs blame CDE for taking inadequate measures to protect sensitive information: "the way CDE has used social security numbers and made them available to thousands of administrators and staff across the state that have little or no training in computer security is inappropriate. We don't want social security numbers, but CDE has embedded them in records that show CDE does not follow federal law."

The fear inspired by these FERPA warnings leads to several questions that need clarification. First, what sensitive student data do schools and school districts keep? Do all schools keep children's Social Security numbers?

Second, what sensitive student data have districts shared with CDE? Does CDE have a requirement that data include children's Social Security numbers (and if so, why)? Third, does the sensitive data that districts have shared with CDE appear in the databases that the plaintiffs want to access? Fourth, will the plaintiffs' discovery be negatively affected if parents of students who clearly do not have any disability object? Finally, what does an objection ensure for a parent? While objectors may believe that their objections will protect their records from disclosure, this does not appear to be the case.

In light of the confusion caused by the disclosure notices, the parties and the court the implications of the planned disclosures must be clarified so parents can ascertain whether their child's information is implicated.

Second, parents who may sympathize with the plaintiffs need a better understanding of whether data regarding their children will aid in discovery in the case. Further, if the plaintiffs want to encourage families not to object they will need to do a better job educating parents on the security measures in place to secure the data that is to be disclosed.

It is clear that parents need to better understand the facts to effectively weigh the risks and benefits associated with any contemplated objection prior to the April 1, 2016, objection deadline.

Recognizing the problems brought out by the contemplated disclosure, and in an apparent compromise, on Monday, the court ordered that CDE undertake specific searches in one of its databases at plaintiffs' behest. Whether this completely averts contemplated disclosures of sensitive student information to plaintiffs remains unclear.

Ariana Seldman Hawbecker *is attorney at Bienert, Miller & Katzman PLC focused on litigation and criminal defense.*

ARIANA HAWBECKER
Bienert, Miller & Katzman