February 1, 2019

What's trending on NP Privacy Partner

DOE seeks to improve FERPA enforcement and proposed North Carolina legislation intends to strengthen the state's data protection laws. Here's what's trending in data privacy and cybersecurity.

Education Privacy

DOE seeks to improve FERPA enforcement

The United States Department of Education ("Department") has modified its investigatory practices to address and resolve complaints and violations of the Family Educational Rights and Privacy Act ("FERPA"), as stated in its guidance document titled "Improving the Effectiveness and Efficiency of FERPA Enforcement." FERPA applies to all educational agencies (e.g., school districts) and institutions (i.e., public elementary and secondary schools and postsecondary institutions) that receive funds under any program administered by the Secretary of Education. The Secretary must take appropriate actions to enforce FERPA and to investigate violations.

Typically, under the FERPA regulations, the Department has "formally" investigated all timely FERPA complaints that it receives from parents and eligible students. However, final determinations often take months or even years to complete. In some instances, the investigation continues after the underlying issue has been resolved or the student no longer attends the educational agency or institution. The Department has recognized that investigations should entail a shorter period of time, and it shall make a case-by-case determination on the best mechanism to address a timely FERPA complaint.

Going forward, the Department will not formally investigate every FERPA complaint. Formal investigations will still occur in matters deemed to required them because of their significance. In lieu of a formal investigation, the Department will weigh the feasibility and propriety of acting as an intermediary or providing resolution assistance. In determining when to conduct a formal investigation, the Department will prioritize the highest risk complaints based upon "the severity of risk to student privacy, the number of students affected, [and] other relevant factors." The Department will also continue to conduct self-initiated investigations in the absence of a filed complaint.

As an example of where the Department envisions acting as an intermediary, it cites complaints implicating a parent's or eligible student's right to access or amend the student's education records, which are typically time-sensitive matters and frequently arise out of misunderstandings regarding FERPA's requirements. Also, a large number of complaints involve isolated incidents of inadvertent

or accidental disclosures of student education records or personal identifying information within the records. The appropriate response may entail assisting the educational agency or institution in improving its policies, practices and security controls to prevent future incidents. If a complaint cannot be resolved through resolution assistance, the Department will determine—on a case-by-case basis—whether additional action is required.

The Department's guidance should come as welcome news to agencies and institutions subject to FERPA, as data management and privacy pose often vexing challenges particularly with electronic records. The Department seeks to undertake a more interactive and cooperative resolution of FERPA complaints, without subjecting the funding recipient in every instance to the potential stigma, costs and impacts of a prolonged formal investigation. *–Steven M. Richard*

Consumer Privacy

Proposed North Carolina legislation intends to expand regulation of data breaches and strengthen consumer data protection

On January 17, 2019, North Carolina Attorney General Josh Stein and North Carolina Representative Jason Saine announced proposed legislation intended to strengthen the state's data protection laws.

The existing North Carolina Identity Theft Protection Act (ITPA) is similar to data breach laws in other states, and requires businesses to protect the sensitive information (e.g., social security numbers) of state residents. Businesses must implement policies governing the secure destruction of personal information and train employees accordingly. In the event of a data breach, the ITPA requires notification to impacted individuals without unreasonable delay.

In 2018, Attorney General Stein and Representative Saine introduced legislation to strengthen the ITPA, expanding the definition of a data breach to include a ransomware attack and requiring incident notification within fifteen (15) days. This legislation was not enacted. The 2019 version reflects certain modifications to last year's proposal. In particular, the new proposed legislation gives entities up to thirty (30) days to report a data breach to those impacted North Carolina residents and the North Carolina Attorney General.

According to a fact sheet, the proposed legislation goes beyond most breach reporting laws by requiring entities that determine an incident did not result in harm to document that determination for review by the North Carolina Attorney General. If enacted, this will bring greater scrutiny to data hacks, ransomware events and other incidents that may not necessarily result in reportable breaches under the federal HIPAA regulations or other state or federal laws.

Attorney General Stein also released a report summarizing the 1,057 data breaches reported to his office last year. According to the report, these breaches impacted more than 1.9 million North Carolina residents, which is a 63% decrease from 2017 when breaches impacted approximately 5.3 million residents. As to the causes of these breaches, the report indicates that phishing schemes comprised 26% of the breaches, with hacking breaches decreasing slightly as compared to 2017. – *Valerie Breslin Montague*

For more information, please contact:

— Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020

— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4487

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team