NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

February 22, 2019

What's trending on NP Privacy Partner

The DOE's new FAQs provide guidance to school officials on balancing student safety and privacy and German anti-trust regulators restrict Facebook's expansive data collection policy. Here's what's trending in data privacy and cybersecurity.

Education Privacy

DOE answers frequently asked questions about balancing FERPA rights and school safety concerns

The United States Department of Education has issued an important and comprehensive set of frequently asked questions (FAQs) on schools' and districts' responsibilities under the Family Educational Rights and Privacy Act (FERPA) in the context of school safety. School administrators often face vexing challenges in understanding and balancing protecting the privacy rights of students while taking the fullest measures to ensure their safety.

In December, the Federal Commission on School Safety released a detailed report, which observed that "substantial misunderstanding remains at the local level among officials and educators concerning (FERPA), and in particular its application to school-based threats." In response, the DOE's FAQ document titled *School Resource Officers, School Law Enforcement Units and the Family and Educational Rights and Privacy Act (FERPA)* consolidates previously issued guidance and technical assistance into a single comprehensive resource to assist schools' and districts' understanding of when their privacy and safety obligations intersect.

The document contains 37 FAQs regarding responsibilities under FERPA relating to disclosures of student data to school resource officers, law enforcement agencies and other stakeholders. DOE also reminds that there may be other federal or state laws, such as civil rights and privacy statutes or regulations, that are relevant to decision-making regarding when and with whom schools and districts may disclose, without appropriate consent, student information.

Among the important FERPA questions addressed are the following:

· Who qualifies as a "school official" under FERPA and to whom may schools and districts disclose education records under the school official exception to FERPA's general written consent requirement?

· Can law enforcement unit officials who are off-duty police officers or SRO's be considered school officials under FERPA and, therefore, have access to students' education records?

· What is a threat assessment team?

· When is it permissible for schools and districts to disclose, without appropriate consent, student education records (or PII contained in these records) under FERPA's health or safety emergency exception?

· May a school make disclosures under FERPA's health or safety emergency exception for emergency preparedness exercises?

· Does FERPA permit schools to disclose any and all education records on a student to another school where the student seeks or intends to enroll?

· Does FERPA permit the disclosure of PII from education records to officials of a state's juvenile justice system?

· Does FERPA permit school officials to release information that they personally observed or of which they have personal knowledge?

As we are reminded too often, we are living in a challenging time where school safety concerns arise daily throughout our nation's schools. The FAQs are a must read for school administrators in understanding how they may permissibly disclose information when confronting ever-growing safety challenges. *–Steven M. Richard*

Cybersecurity

German anti-trust regulators restrict Facebook's expansive data collection policy

Last week, Germany's anti-trust regulatory agency, the Federal Cartel Office (the "FCO") issued a decision intended to sharply curtail Facebook's ability to collect and aggregate data about its users. The decision was the culmination of an investigation that began in March 2016. In its ruling, the agency stated that Facebook's take-it-or-leave-it terms of use, which allowed the company to compile detailed profiles of its users, abused the company's position in the German market. Because the alternative would be not to use Facebook services at all, the FCO argued that Facebook effectively coerced users into giving up personal data.

Facebook's terms of use required users to consent to the company's collection of personal data across all Facebook-owned services, including Instagram and WhatsApp, and on millions of third-party websites with embedded Facebook features and analytics. These data collection practices allowed Facebook to bundle numerous data points into comprehensive user profiles, which are the cornerstone of the company's lucrative advertising model.

The FCO advanced a novel argument to establish that Facebook's activities violated anti-trust principles. Regulators argued that Facebook's overwhelming market power coerced users into accepting the website's terms of use. Instead of a financial harm, Facebook users suffered a loss of control over their personal information, which was combined with data from other sources in a manner that would be unforeseeable to most users.

The FCO's action against Facebook was an administrative proceeding, intended to compel the company to change its practices, rather than merely extracting a financial penalty. However, Facebook

has already announced plans to appeal the decision, in a process that begins next month. – *Aya M. Hoffman*

For more information, please contact:

- Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020
- Aya M. Hoffman at **ahoffman@nixonpeabody.com** or 585-263-1535

NP PRIVACY PARTNER BLOG

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