K-12 Student Privacy Working Group Meeting Notes

(open to all education privacy working groups and the FPF Advisory Board)

Friday, February 10, 2017
11:30am-12:30pm
Topic: Education privacy and federal government data requests from companies
70 Attendees (see list of organizations at the end of the notes)

Amelia Vance (FPF) on Student Privacy Legislation Updates

- To date, 96 bills have been introduced in 30 states.
    - The trend of bills modeled on SOPIPA continues (11). Several bills are governance-focused and modeled after Oklahoma's Student DATA Act.
    - Most bills target K-12 (78), followed by higher-ed (18), and early education (2).
    - Most bills are directed to local education agencies (45), followed by state education agencies (27), and vendors (24).

Jake Sommer, Melissa Maalouf, and Kandi Parsons (Zwillgen PLLC) on Law Applicable to Government Requests for Student Data from Companies

Key Points:

- The Electronic Communications Privacy Act (ECPA), especially Title II of ECPA, the Stored Communications Act (SCA), governs law enforcement access to electronic records. These Acts may provide more stringent protections than FERPA with respect to student data held by vendors.
- ECPA and SCA require various types of legal process for law enforcement to request data from vendors, ranging from a subpoena to a warrant. Before responding to such a request, a company should ensure it is valid, and give only the data that is required by that type of order.
    - ECPA includes a private right of action for anyone harmed by improper disclosures to law enforcement and third parties generally.
- School districts should minimize the data collected from students and retained to minimize what the district or a school vendor may be asked to produce.
- Contracts between vendors and schools should include when and by what mechanisms requests for data should be made.
- Vendors should adopt standard policies that provide for notification of both subscribers (school districts) and students and parents upon receipt of a government request for student records.

What is the Electronic Communications Privacy Act (ECPA)? What is the Stored Communications Act (SCA)?

- ECPA: Passed in 1986, ECPA modernized the Wiretap Act. Its provisions govern when law enforcement can get records from you about your users.
- SCA: Part of ECPA, the SCA governs data held by covered entities—electronic communications services (e.g. email) and remote computing services (e.g. cloud drive).

The Act provides rules for covered entities regarding what data they may give to the government and when they may do so.

Who is a "covered entity" under the SCA?

- A covered entity is an electronic communications services (ECS) or a remote computing services (RCS) that is offered to the public. An entity may be both an ECS and RCS.
- Most vendors are likely to be a covered RCS because, as a business, the services are broadly offered to the public.
- School districts may be covered entities, but only when a service they provide is offered to the public.
    - A schoolwide email service accessible only to staff within a .edu domain is likely not an ECS because it is not publicly accessible.
    - A vendor-provided email service accessible to the entire school community (staff, students, parents, etc.) may be a covered ECS if the group is large enough to be considered "public."

What information is protected and how?

- ECPA protects wire, oral, and electronic communications while being made, while in transit, and when stored.
- Three basic principles:
    - Content (i.e. message text) is more protected than non-content (i.e. message metadata).
        - Content data requires a more burdensome probable-cause warrant.
        - Non-content data requires a court-issued § 2703(d) order based on a finding of specific, articulable facts that there are reasonable grounds to believe the information is relevant to an ongoing criminal investigation.
    - Messages in transit are more protected than stored files.
        - Messages in transit require a more burdensome wiretap order.
        - Stored files require a probable-cause warrant.
    - Transactional information (i.e. metadata) is more protected than subscriber basic identity information (i.e. name and address).
        - Transactional information requires at least a § 2703(d) order.
        - Basic subscriber information requires only a subpoena.

How should I (a vendor) respond to a government request?

- If you receive a preservation request, you must preserve the identified data for an initial period of 90 days, with the possibility of one 90-day extension. During this time, law enforcement may return with other orders.
- If you receive a subpoena, respond only with basic subscriber information (name, address, phone, email, service details). For vendors, the subscriber is most likely the school system, but it depends on contract language.
- If you receive a § 2703(d) order, ensure the order is proper. These orders are valid for requested non-content metadata.

- If you receive a warrant, ensure the warrant is proper. Warrants are valid for the requested content information.

Can/should I notify my users and subscribers?

- Vendors should adopt standard policies that provide for notification of both subscribers (school districts) and students and parents upon receipt of a government request for student records.
- School districts should also think about ECPA when writing terms of service. Subscribers are likely to be both parents and students for valid consent.
- You may issue notification unless the government presents a confidentiality request as part of a warrant or non-disclosure order.
    - If the request is a subpoena, you may issue notification. Even if the subpoena requests you to keep the process confidential, this is not binding. A best practice response is: "We have a standard policy to notify users in the event of a record request. Would you like to withdraw this subpoena or return with a non-disclosure order?"
    - If the request is a warrant, you may only issue notification if there is no accompanying request for confidentiality.
    - Non-disclosure orders are binding. Some companies (e.g. Microsoft) have been issued indefinite non-disclosure orders and are challenging the constitutionality.

Am I subject to liability for disclosures to law enforcement?

- ECPA includes a private right of action for anyone harmed by improper disclosures to law enforcement and third parties generally.
- Two immunity defenses:
    - It is a complete defense (available in a motion to dismiss) if you provide information in response to valid court order with proper process.
    - It is an incomplete defense if you demonstrated good faith reliance on a process that had a slight defect.

Question & Answer

Question: How is this applicable to a vendor holding a full student record - what data can be disclosed?

Answer: Where a vendor is holding a full student record (for example, in a cloud folder), the record should be treated as content. The vendor should insist on a warrant.

Question: If the contract between the LEA and vendor establishes the vendor as a "School Official" does this change your response to question #1?

Answer: No. This remains protected content. The vendor should still insist on a warrant.

Question: Can you provide an example of ECPA language that should be included in vendor contracts and student Acceptable Use Policies?

Answer: Contract language will heavily depend on the nature of the service.

- Generally, schools should spell out to all users (students, parents, and staff) exactly who has access to communications and obtain consent for that access.
- For vendor contracts, schools should require notice and an opportunity to respond if the vendor should be served with legal process for account information.

Question: Is it up to the recipient of the warrant to ensure it is valid and appropriate?

Answer: The recipient should review the basic elements. For example, it must say "warrant," it must include a statement of probable cause, it must specify particular items requested, and it must be signed by a judge. If there is a defect in one of those elements, you should insist on a proper warrant to avoid liability.

Question: Should schools be worried about the government circumventing them by going to vendors?

Answer: Due to the SCA, student data is likely *harder* to get from vendors. It is much easier for law enforcement to get records from the schools themselves. However, if the school is the custodian of the data (or can access the data), the simple fact that the school uses a vendor does not make the data harder for law enforcement to obtain.

Question: What if the school wants to push back by asking the government to make the request to the vendor?

Answer: This will be difficult to do since the data is likely in the control or custody of the school. While the school may need technical assistance from the vendor, FERPA's exception for disclosure to law enforcement likely applies. The best practice for schools seeking to avoid government data requests is to, minimize what you collect and retain.

Question: What policies govern data retention by vendors?

Answer: Many countries have generalized data retention mandates, but the US does not. Retention is thus managed under the policies of the vendor.

Question: Does "government" = "law enforcement"?

Answer: ECPA refers to a "governmental entity," not specifically "law enforcement."

- A "government entity" means any department or agency of the U.S. or a political subdivision.
- Whether your school district is considered a "government entity" may depend on the organization of your school board. If the school board is elected, it is likely subject to ECPA requirements when requesting data from vendors.

Question: If a request for confidentiality is not binding, what is the advantage of pushing back on the subpoena? Wouldn't one be able to notify the subject upon receipt and/or while the agency decides to withdraw or send a binding confidentiality notice?

Answer: While taking that course of action is possible, it is not recommended. Law enforcement is typically conducting a serious investigation. A vendor or school could blow the investigation this way, leading to other negative consequences down the road.

Question: Can the call touch on the proposed amendment to CalECPA (link here) which would exempt law enforcement from following the warrant-for-content requirement when requesting

data from "a local educational agency or an individual acting for or on behalf of a local educational agency":

Answer: The legal argument against this amendment is that the Fourth Amendment requires a warrant anyway, not just CalECPA. However, it is typically difficult for a third party like a vendor to assert the Fourth Amendment rights of its users.

Question: Should a request for information about a student/user that is made by an individual teacher or administrator be legally treated in the same manner as a request from law enforcement or a request from a School Board, etc.?

Answer: Vendors should resist such a request unless it was specifically contracted that that individual would have access in that manner. Otherwise, the vendor should ask the individual to go through the contracting party. Generally, contracts between vendors and schools should cover when and how requests for data should be made.

Question: How does this relate to/play out for data from a US resident customer/user of a US Inc., held outside the US, eg in Europe? Would this have to be served by the Inc. through (internal, international) company channels, or would it have to go externally though assistance treaties feeding into the overseas entity holding the data?

Answer: This is a complicated reference to the Microsoft-Ireland case (brief summary on *Lawfare* here). That case involved a foreign user of a U.S. company's services whose data was located on servers abroad. This question asks about a U.S. user and a U.S. company, so it would likely be harder to fight. A court would likely try to make this data available, but it remains an open question.

Question: Same as above but for a non-US resident?

Answer: That scenario is closer to the Microsoft Ireland case, and therefore may be easier to fight so long as the data is also overseas.

Attending Organizations

Please email Amelia Vance at avance@fpf.org if you were on the call and your organization name is not listed below.

1. Amplify
2. AT&T
3. Butler County Schools, Alabama
4. California Department of Education
5. Cambridge Public Schools, Massachusetts
6. Colorado Department of Education
7. Data Law Group LLC
8. Data Quality Campaign
9. Edelman
10. Edmodo
11. Ellevation
12. Enhancing Insights, LLC

13. Fairfax County Public Schools
14. Foresight Law + Policy
15. Georgia Institute of Technology
16. Global Information Infrastructure Commission
17. GoGuardian
18. Institute for Higher Education
19. Khan Academy
20. Lifetouch
21. LinkedIn
22. Louisiana Department of Education
23. Microsoft
24. New America
25. Netflix
26. New York City Department of Education
27. Nixon Peabody
28. North Dakota EduTech
29. Oregon Office of State CIO
30. Pearson
31. PlayWell, LLC
32. PRIVO
33. Quantcast
34. Santa Clara County Office of Education, California
35. SETDA
36. Software and Information Industry Association
37. TomTomUSA
38. TRUSTe
39. UCLA
40. U.S. Department of Education
41. Ventura County Office of Education, California