

Policymaker's Guide Webinar
Guide: <https://ferpasherpa.org/policymakersguide/>
4/5/2019

Speakers:

- Utah State Senator [Jake Anderegg](#)
- Rachel Anderson from the [Data Quality Campaign](#)
- Sunny Deye from the [National Conference of State Legislatures](#)
- Amelia Vance and Tyler Park from the [Future of Privacy Forum](#)

1. Why the Policymaker's Guide?

- a. Increasing interest from state legislatures in privacy generally
 - i. There is an interest in consumer privacy, which was first addressed by state legislatures starting with the passage of CCPA last year
 - ii. Another 10 states have introduced consumer privacy legislation
 - iii. Important to reflect back on the 116 student privacy laws passed since 2013 as we see how they relate to other privacy movements in the country
- b. New laws are being introduced that can cause unintended consequences
- c. Few resources have previously been available specifically for policymakers

2. Rachel Anderson on the importance of student data fidelity

- a. Education Data Privacy: Parent and Educator Perspectives and the Policymaker Role
 - i. Big idea at DQC: when students, parents, educators, and partners have the right information to make decisions, students excel
 - ii. A big part of helping people use data is building trust that data is being used in ethical ways that have to do with the purpose of education
 - iii. Part of DQC's work is based on parent/teacher feedback
 1. They have learned that data and privacy matter:
 - a. 95% of parents support teachers' use of data to make sure students are getting all the support they need
 - b. 86% of teachers say data helps communicate with parents about their children's performance
 - c. 93% of parents need data so they can help their children do their best
 - d. 90% of parents say a school's performance rating helps them make decisions related to their child's education
 - e. Teachers use different types of data to improve teaching and learning
 - f. Teachers use data to plan and enhance instruction
 - i. Identify learning goals
 - ii. Know what concepts student learn

- iii. Plan instruction
 - g. Parents increasingly trust educators to use their child's data appropriately
- iv. Four policy priorities to make data work for students
 - 1. Measure what matters
 - 2. Make data use possible
 - 3. Be transparent and earn trust
 - 4. Guarantee access and protect privacy
- b. What is next?
 - i. State policymakers must build trust and provide value:
 - 1. Empower families and educators with access to data
 - a. They are uniquely positioned to make this happen
 - 2. Train and support educators to use data well
 - 3. Make public data more meaningful and useful

3. Senator Anderegg

- a. Tyler: Utah has developed one of the most effective student privacy approaches that we've seen at the state level
- b. Oftentimes, people in Utah have an inherent distrust in government and state agencies
- c. In the era of big data and business, a large part of the distrust comes from a misunderstanding of how you can protect your data while also maximizing its utilization
- d. The guiding structure in student privacy is FERPA, but FERPA has some loopholes
 - i. Ex: Teachers can share PII if they deem it is for an "educational purpose"
- e. When he realized problems with FERPA
 - i. How do you collect only data that is relevant to the educational system and process safely?
 - ii. How do you minimize its exposure? How do you ensure you are getting the highest quality outputs so the policymaking can reflect?
 - iii. If you are trying to measure how effective a policy is, if you have junk data going in, you have junk information coming out that is messing up your policy measurements
 - iv. **FERPA was silent on what data could be collected
 - 1. Utah expanded FERPA on what data could be collected and why
 - 2. They held ~20 meetings over 3 years time about what they wanted to collect, what safeguards they wanted to put in place at the state level, and maximizing security of PII and aggregated data
 - a. Needed a balance that constrained what data was acceptable vs. not to be collected
 - v. If it is not a necessary data element in order to educate the child, parents should have the right to opt-out

- f. With the technology we have today, how will education look in 10/20/30 years?
 - i. You must take the necessary steps to get hands around this issue now

4. Questions

- a. Do you feel like you struck the right balance in Utah and what are you thinking of doing moving forward?
 - i. Every year, they tweak the student data privacy amendment bill
 - ii. This year, they passed one dealing with special needs data
 - iii. What we have now is a lot better than what we had 5 years ago
- b. What stakeholder participation was involved initially and throughout the legislation?
 - i. State BoE, local LEAs (especially legal), 3-4 school districts on board, partners like United Way
 - ii. We self regulate, so we had to have a system that was workable through the educational process to ensure quality and compliance
 - iii. Had to be an element of auditing, training and funding

5. What does the policymaker's guide do?

- a. Provide an overview of federal laws
 - i. FERPA
 - 1. Requires information to be released only with consent
 - 2. Subject to several safeguards
 - 3. Studentprivacy.ed.gov is a great resource
 - ii. COPPA
 - 1. Information collected from children under 13 from online services
 - iii. PPRA
 - 1. Deals with surveys given to students
 - 2. Gives parents the ability to opt-out
 - iv. IDEA
 - 1. Mirrors FERPA protections but extends further for children with disabilities
 - v. HIPAA
 - 1. Medical information in student records is exempted
 - 2. Not usually applicable to students
 - vi. CIPA
 - 1. Schools that receive E-rate funds must monitor their systems and prevent obscene and other objectionable content
- b. Provide an overview of the state landscape, which is even more diverse and complicated
 - i. 40 states have passed 116 laws since 2013
 - ii. 10 states have not passed a student privacy law yet
- c. Potential issues to consider
 - i. How can states build upon what exists in FERPA and allow for local control
 - ii. School safety and surveillance

- iii. Vendors and third-party data use
 - 1. SOPIPA, passed in 2014 in California, was the first law directly regulating edtech vendors
 - a. This law has been adopted in more than 20 states
- iv. Transparency
- v. Parental rights
 - 1. Parents should be able to make decisions about how their child's information is shared without jeopardizing what teachers can do in the classroom
 - 2. This is an area ripe for unintended consequences; for example, Louisiana required that parents opt-in to most data sharing, and had to backtrack because that was unworkable.
- vi. Data governance and security
- vii. Training
 - 1. Fairly limited in state laws, but is the most important thing
- viii. How to approach higher education - is it the same as K12?
 - 1. Most states haven't passed laws regulating higher ed privacy.
- d. Important stakeholder groups
 - i. Students and parents
 - ii. Educators
 - iii. District, state, and federal education offices

6. Sunny Deye

- a. NCSL: membership organization for state legislators and their staff
 - i. Provide policy research and analysis, training for legislatures
- b. Trends in state legislation from 2013-2018
 - i. Key policy questions
 - 1. Purpose of privacy policy
 - 2. What data is collected and by whom
 - 3. District capacity/resources to protect student data
 - a. Some state have helped districts create data security plans
 - 4. Requirements for private companies
 - a. What would be the remedy when they breached those requirements?
 - 5. Who is responsible
 - ii. Volume of legislation shows legislators prioritize student privacy that requires updates and provisions
 - 1. Data use: state efforts to improve educational outcomes
 - iii. 2019 outlook
 - 1. At least 35 bills introduced to date
 - 2. Often build on previous state legislation
 - 3. Continuing concerns
 - a. Third party vendors
 - b. Enforcement provisions

- c. Transparency and accountability
 - d. Coordination and governance
- 4. New and emerging concerns
 - a. School safety
 - b. Social media
 - c. Personal device use
 - i. CT had a bill in 2018 concerning students right to privacy on their electronic devices
 - d. Storage and retention policies
 - i. NH bill in 2018 established a statewide protocol for collecting and retaining data

7. Questions

- a. Is student safety via video surveillance an emerging issue?
 - i. It is not a new issue- has been around since the 90s
 - ii. We have seen a push to build on that video surveillance and add tech like AI over video surveillance
 - iii. Legislation that would require that districts share video information with law enforcement on an ongoing basis has raised serious privacy concerns.