In response to data security concerns, many states are considering ways to allow individuals to remove their personal information from certain statewide data collections or data products. Such "opt out" measures were included in 81 state student-privacy bills in 2015, 13 of which were signed into law.[1] Additionally, the federal Family Educational Rights and Privacy Act (FERPA) grants families some control over the release of specific student information, and additional measures related to student privacy are being discussed at the federal level. These regulations—and the variety of data-related activities they can cover—present challenges for statewide longitudinal data system (SLDS) teams, who need to ensure that personal data are collected and used appropriately.

This brief provides an overview of the data collections and data uses that are often part of opt-out measures. It also examines strategies that states are developing to handle opt-out preferences in their SLDSs and ensure that data are properly managed.

What Does It Mean to Opt Out?

The term "opt out" has become common in state and nationwide discussions about a range of situations in which schools and education agencies gather and use student data. A state's technical and administrative solutions for handling opted-out records depend on the specific data collection, process, or reporting activity from which students and families are opting out. Discussions about opting out often focus on the following data collections and uses.

Directory information
Directory information is typically collected at the school level. The data categorized as directory information vary by school but commonly include a student's name, address, telephone number, date and place of birth, any honors and awards, and dates of attendance at the school. In addition to being used for school operations, in many states the collection of directory information is required to support the federal Elementary and Secondary Education Act (ESEA) and American Reinvestment and Recovery Act (ARRA) grants.

Schools may want to release this type of information to publish directories, publicize student activities and athletic teams, or work with third-party vendors like yearbook or

Directory Information and FERPA

The federal Family Educational Rights and Privacy Act (FERPA) allows schools to collect and disclose student data categorized as "directory information" without consent, unless parents or eligible students have opted out of this disclosure. Eligible students are those who are over the age of 18 or who are enrolled in an educational institution beyond high school. Under FERPA, schools must notify families annually about what data are considered directory information and allow them to opt out of having such information disclosed. Additionally, schools must allow parents and eligible students to review the student's directory information and correct any errors.

IES NATIONAL CENTER FOR EDUCATION STATISTICS
Institute of Education Sciences

[1] Data Quality Campaign. (2015). *Student Data Privacy Legislation: What Happened in 2015, and What Is Next?* Retrieved November 18, 2015, from *http://dataqualitycampaign.org/find-resources/student-data-privacy-legislation-2015/*

class ring providers. At the federal level, FERPA includes provisions for schools' use of directory information and for families to opt out of the release of this information. Some states have adopted policies that further regulate the use of directory information, including the circumstances in which schools can disclose student information, what processes are required for schools to notify families, and when families can opt out of disclosure.

Directory information should not be confused with data needed by school officials to educate children. These data are not subject to FERPA's opt-out provision for directory information. However, FERPA requires school districts to define for parents who is considered a school official with "a legitimate educational interest" in student data. Although parental notification is required, FERPA does not allow parents and eligible students to opt out of data needed by school officials.

State assessments
Concerns about standardized testing have led many families to opt out of allowing their students to take statewide standardized assessments that are used for state and federal accountability reporting. Schools were required to conduct and report assessment results to the U.S. Department of Education as part of the No Child Left Behind Act, and state assessment results are also a factor for the Every Student Succeeds Act (ESSA) passed in 2015. Additionally, assessment results are used to inform instructional decisions at the state, district, and school levels.

State and federal reporting
Many types of student data are collected at the school level and then reported to the state education agency for programmatic purposes and inclusion in the SLDS, and as aggregated datasets to the U.S. Department of Education

---

Federal Reporting and School Funding

A number of federal education programs provide money for schools to better serve specific populations of students or to meet specific outcomes. These programs require schools to report some student information for accountability purposes. Incomplete student information can affect the federal funding that schools receive.

Federal programs that require reporting include

- Individuals with Disabilities Education Act (IDEA) programs; and
- Elementary and Secondary Education Act (ESEA) Title programs, including those supporting low-income, limited-English proficient, migrant, and homeless students.

---

for funding and accountability for federal programs. Some states are considering legislation that would allow parents to opt out of including their students' data in the SLDS beyond what is needed for specific purposes, such as to establish a student's educational record or to meet federal reporting requirements.

Public reports and third-party data sharing
Some states are adopting or considering measures that affirm the need to collect and report student data to state and federal education agencies but allow families to opt out of releasing their students' information beyond these purposes. Under such measures, a student's data can be included in the SLDS but must be removed from datasets that are used for public reports, shared with non-state researchers, or provided to vendors.

Strategies for Managing and Recording Opt Out

Implementing any type of opt-out policy requires both administrative processes to record and report opt-out preferences and technical solutions to ensure that those preferences are reflected within the data system. The administrative and technical components will depend on the specific data and data activities affected by a state's opt-out policy. Most opt-out strategies will be informed by the following considerations:

- *Location of opt out.* Identify the agency or agencies responsible for collecting opt-out preferences from individuals or families and for implementing provisions of the policy. If parents are opting out of releasing student directory information, that preference is recorded by the student's school and the school is responsible for ensuring that the information is not released without consent. If state policy allows student data to be included in the SLDS but excluded from external reporting and research, the school, state education agency, or SLDS program might be responsible for gathering and recording opt-out preferences. Responsibility for including or excluding specific student data from datasets will lie with the SLDS program.
- *Communication of opt-out preferences between data systems.* Decide how opt-out preferences will be recorded in the source data system and then reflected when records are submitted to additional data systems, including to the SLDS. For example, if opt-out preferences are recorded at the school level, records for students whose families have opted out of certain data uses need to include indicators of that preference when integrated into district-level or state-level data systems, or those records need to be stripped of affected data elements before being shared outside the school.

- *Duration of opt out.* Determine over what period of time an individual's records will be affected by opt-out preferences. Will individuals or parents be required to opt out of data collections or uses on an annual basis, or does a one-time opt-out choice apply as long as a student remains in a school or district?

Depending on the requirements of the opt-out policy and the affected data, SLDS teams could use a number of approaches to managing opted-out records, including the following.

Limit the data shared between source systems and the SLDS
Opt-out measures may require that some data collected at the school or district level not be released beyond the collecting agency. In these cases, data-sharing processes, such as integrating school or district records into the SLDS, must be designed so that data for opted-out students is fully or partially excluded. Personnel at the collecting agency must be trained so that opt-out preferences are recorded appropriately for each individual and so that the affected data are not shared outside the agency.

Flag opted-out records
When individuals' data can be included in the SLDS but cannot be used for purposes such as public-facing reports or external research, the data system will need an indicator—or "flag"—to identify the affected records. Queries and reports designed to fulfill any purpose covered by opt-out measures must be designed to exclude records containing that flag.

Additional Considerations

When individual records are missing data, or when data must be suppressed from specific uses due to opt-out policies, datasets and reports created from those records are necessarily incomplete. Any report, evaluation, or other data product created from records affected by opt-out measures must address the missing data. It is important to determine in advance how to communicate to users the opt-out policy's impact on data products. This might be accomplished through a disclaimer outlining the policy, the number or percentage of records affected, and how the excluded data might affect conclusions drawn from the product.

Communications and transparency can also assist SLDS efforts more broadly. For instance, if the SLDS's output includes only properly de-identified data or aggregated data, this fact should be clearly stated in publications and messaging around the SLDS. Consider creating a frequently asked questions (FAQ) page or a short video about the SLDS that explains the security and privacy protections on personally identifiable student data.

State Example

The **Virginia Longitudinal Data System** (VLDS) program created a short video explaining the privacy and security measures in place to protect individual data in Virginia:

https://www.youtube.com/watch?v=Wpda6eP-rcI

State Opt-Out Challenges

Most states considering opt-out regulations and policies are in the early stages of planning potential approaches and solutions. Even so, some SLDS teams are actively involved in discussions about opt-out procedures in their states. By engaging in privacy conversations, they hope to ensure that future policies adequately address concerns while maintaining the integrity of data tools, reports, and research.

Minnesota: An Agency-Driven Opt-Out Policy
In 2015, leaders of Minnesota's Statewide Longitudinal Education Data Systems (SLEDS) began drafting an opt-out policy at the suggestion of a legislative committee chair following a hearing on data privacy. Although state law does not require such a policy, the SLEDS team realized that developing one would add to its existing measures to ensure individual rights and privacy as well as help protect the program politically in similar conversations in the future.

Minnesota's draft opt-out policy would allow individuals—or parents in the case of students who have not yet graduated high school—to exclude their data from research performed by local education agencies, other SLEDS partners, or external researchers. Individuals cannot exclude their data from collection or linkage within SLEDS, nor from state and federal reporting.

Opt-out requests would be collected via an online form on a new SLEDS data privacy webpage, which would also include general information about SLEDS privacy policies. Individuals would be asked to submit their first, middle, and last names and date of birth, and they have the option to submit prior last names, Social Security numbers, and state K12 identification numbers for greater accuracy in identifying their personal records. Data collected through the form would be stored in an "Opt-Out Collection" table within SLEDS and incorporated into the system's probabilistic matching algorithm process. If the data provided meet a 91 percent matching threshold with existing SLEDS records, those records will be identified with an opt-out flag and excluded from research datasets in the future. The opt-out flag is time limited, and individuals would need to re-submit the form on a defined schedule to continue excluding their data from SLEDS research.

The SLEDS team developed this draft policy to give individuals control over how their SLEDS data are used while minimizing disruptions to SLEDS operations and data use. Collecting opt-out requests within the SLEDS platform avoids increased administrative burden or potential errors from having the state education agency, schools, colleges and universities, or employers enter that information manually. Because the opt-out policy will affect the data available to schools, universities, and other users, the SLEDS team plans to discuss with its stakeholders the policy's implications for data products. It also hopes to quantify the impact of the policy with metrics from the opt-out collection form. The opt-out policy will require amendments and revisions to existing SLEDS documentation, such as memoranda of understanding, data sharing agreements, and possibly data classifications, as well as additional public outreach.

SLEDS leaders plan to present the draft opt-out policy to their executive team and then add details about the required administrative and IT processes based on the executives' feedback. Afterward, the draft policy will be presented to SLEDS's advisory committee and external stakeholders for review and feedback. In addition to the technical challenges of collecting and storing opt-out preferences, SLEDS leaders anticipate questions and concerns about the need to collect significant amounts of personally identifiable and sensitive data in order to accurately identify individuals' SLEDS records. The team hopes to finalize a formal opt-out policy by the end of 2016.

Alaska: Communicating the Impact of Opt Out
Individuals in Alaska currently cannot opt out of having their data collected and used through the state's P-20W SLDS—known as the Alaska Navigator: Statewide Workforce and Education-Related Statistics (ANSWERS)—nor do the ANSWERS partners plan to implement an opt-out policy. However, recent conversations among state legislators have prompted the ANSWERS team to consider and communicate the impact that different opt-out approaches would have on the program.

ANSWERS leaders believe that an opt-out regulation would dilute the accuracy and value of reports and products created with ANSWERS data, thereby undermining confidence in the system. They also recognize that the number and demographics of the individuals choosing to opt out may not be uniform across the state. That inconsistency could create bias in data products and prevent ANSWERS from providing high-quality information to policymakers, specific schools or districts, and the public. In addition, accurately identifying individual records to opt out of data uses would require individuals to provide considerable amounts of personally identifiable information to the state first. This last concern has so far resonated with Alaska lawmakers.

If state law or public privacy concerns do require Alaska to implement an opt-out policy in the future, the ANSWERS team would design the policy and procedures to limit the impact on its data products as much as possible. This approach could involve allowing individuals or parents of students to opt out of having their unit-level data shared for research, but not for reporting or data products that use aggregated data.

Some conversations about data privacy at the state level have raised concerns about using Social Security numbers to identify individual records. Although Social Security numbers are not collected by all ANSWERS data providers, they are used to match records across data sources. The data-linking process would need revision if those identifiers were no longer available. The ANSWERS team is addressing concerns by clearly documenting and communicating that although Social Security numbers may be used for matching purposes, they are never stored in the ANSWERS data warehouse.

By pointing out the potential impact of opt-out measures on individuals as well as data users, ANSWERS leaders want to drive any future discussions or regulations rather than merely reacting to them.

Additional Resources

Alaska Navigator: Statewide Workforce and Education-Related Statistics (ANSWERS)
http://answersresults.alaska.gov/

Family Educational Rights and Privacy Act (FERPA)
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Minnesota Statewide Longitudinal Education Data Systems (SLEDS)
http://sleds.mn.gov/

Privacy Technical Assistance Center (PTAC)
http://ptac.ed.gov/