The College Transparency Act

The College Transparency Act would both repeal the ban on a federal student unit record data system and specify requirements related to the establishment of such a system. NAICU has generally opposed the creation of a student unit record data system because we believe the benefits of such a system do not outweigh the risks to student privacy. Currently, the bill has multiple sponsors in both the House and the Senate.

For over four decades, federal law has guaranteed that students are the ones who control their own personal and academic information. Under the Family Educational Rights and Privacy Act (FERPA), institutions of higher education are subject to strict privacy requirements in their role as *temporary custodians of student records*, but it is students who generally determine what may be done with their personal information. A federal student unit record data system, however, would fundamentally alter FERPA's promise to ensure that students are the ones who determine who has access to their personal and academic information. In particular, the College Transparency Act raises several privacy concerns, which are discussed below.

Notice and Consent

Two of the most fundamental privacy principles are notice and consent. In general, individuals should be given notice when their personal information is being collected. Such notice is essential to maintain a data system that is both transparent and that conforms to basic tenets of privacy.

The College Transparency Act would require the Commissioner of the National Center for Education Statistics (NCES) to ensure that the new data system complies with the Privacy Act, which requires federal agencies that maintain a system of records to provide notice to individuals whom they ask to provide information. However, under the Act, institutions, not students, would be the entity supplying information to the Department of Education, thus raising questions about who— the institution or the department — would provide notice to students.

Individuals should also be given an opportunity to consent to the collection of their personal information. The bill does not provide such an opportunity.

Access

Access is another basic privacy principle. To construct a data system that adheres to generally accepted privacy principles, access for individuals whose information is being collected should be available, and access by the data collector and third parties should be limited.

Specifically, individuals should be granted access to inspect their personal information and correct inaccuracies. It appears that this right would be available to individual students pursuant to the Privacy Act provisions that would govern a federal student unit record data system. We are concerned, however, that institutions, which would be responsible for transmitting de-identified student data to the federal government, do not appear to have the same right under the bill.

In addition, agency access to data should be limited only to those who need the information to fulfill the intended purpose of the information collection. Access by third parties should be subject to the same

constraint. Thus, it is critical to limit who a student unit record data system is intended to serve and to what end. Although the bill would require the Commissioner to impose access controls and would prohibit the sale of data to third parties, it does not specify the conditions, if any, under which third parties such as contractors, other government officials, or researchers would have access to the system.

Additionally, the bill would require the Commissioner to make de-identified student-level data available for "research and evaluation purposes approved by the Commissioner." Because there is no definition of what constitutes research or evaluation and because the Commissioner would have broad approval authority, the de-identified student data could become widely available.

Purpose and Content

In order to maximize privacy protections, it is essential to clearly identify the purposes for which the individualized information is to be used and to limit the collection of data only to that which is strictly necessary to achieve the underlying purpose. Framed another way, it is important to ask what problem the creation of a federal student unit record data system is intended to address.

Under the College Transparency Act, the stated purposes of a federal student unit record data system are quite broad, including the need to "assist with transparency," provide "customizable information for students and families," and "reduce the reporting burden" on educational institutions. Other commentators have suggested that such a data system would provide outcome metrics that could be used to hold institutions accountable. However, it is not clear how the bill would serve these purposes. For example, it is by no means certain that the information collected would be useful to students and their families or that institutional reporting burdens would be lessened, especially since it does not appear that the bill eliminates and institution's obligation to report IPEDS data or comply with other reporting requirements contained elsewhere in the Higher Education Act. Likewise, it is not clear that the various outcome metrics would be a valid and reliable measure of the problem they are intended to solve.

In order to promote privacy, it is also critical to place limitations on the content of the data collected, both in terms of the types of information gathered and the individuals whose information is being collected. Notably, the bill would not limit the number of data elements that would be included in the system. The bill specifies certain elements that must be included, but the Commissioner would have unlimited authority to add additional elements. In other words, the bill sets a floor but not a ceiling on the information that the government would collect. A provision authorizing reevaluation of the required data elements provides an additional opportunity to continue to collect additional information. In addition, although the bill would prohibit the collection of certain information, it's not clear why certain categories of information are protected. For example, the bill would prohibit the collection of student addresses, but such information is generally not a form of protected information under FERPA.

The bill also lacks limits on the population of students whose information could be gathered. Currently, the federal government does maintain a student unit record data system called the National Student Loan Data System. However, the information contained in the system is there because students have voluntarily turned in their FAFSA application to the federal government. Creating a student tracking system for those who are not in the NSLDS database raises several concerns. In general, such students fall into two broad categories: (1) those who do not wish to apply for federal aid either for economic or privacy reasons, and (2) those who are not eligible for aid, primarily because of citizenship status. These students would now be trackable in a federal database simply because they enrolled in a college course

at some point in their lives. Although the bill would ostensibly prohibit the collection of information about citizenship status, requirements to match data with other federal agencies could make unauthorized students vulnerable to exposure.

Ultimately, it is not clear what policy problems a federal student unit record data system are intended to solve. Is it to gather information about part-time and transfer students? If so, IPEDS has added a survey to collect this information in an aggregate form that will not require students to turn over their personal information to the federal government. Is it to gather data about student employment earnings? If so, it is not clear that students' personal career choices are a valid indicator of the quality of their education. In general, in order to maintain good privacy practices, data systems should not rely on individually identifiable information when statistically reliable aggregate information is available.

Collection and Maintenance

Once a data system is created, it is critical to ensure the integrity and security of the personal information collected by creating standards related to the collection and maintenance of the data contained therein. The bill does contain several provisions that address these issues, including provisions that would incorporate Privacy Act protections and that would require the Commissioner to issue guidance specifying audit capabilities, access controls, and requirements related to data security and reliability, as well as other protections consistent with federal standards developed by the National Institute of Standards and Technology.

However, the bill would also call for institutions to turn over personal files on all their enrolled students. Under other proposals, the institution de-identifies the files before they turn them over to the governmental entity. In this way, there are protections against re-identification of individual students. Cohorts that are too small to report without risk of identifying an individual are never submitted in the first place. We are deeply concerned about a federal system that begins with each student's personal, identifiable file.

Another essential component of a secure data system are limits on data retention, including provisions related to the de-identification or destruction of personal information. Although the bill would require the Commissioner to ensure that data linkages "do not result in the creation of a single Federal database at the Department of Education that maintains the information reported across other Federal agencies," it is not entirely clear how the Commissioner would comply with this provision, given that the data system would theoretically need to be updated regularly. For example, the department would necessarily need to maintain a database in order to conduct data matches with other federal agencies and perform the required calculations. Even if the individualized information were deleted at some point, there necessarily would need to be a database that existed for some period of time. Likewise, if the purpose of the data system is to track individual earnings over a student's lifetime, it is not clear whether the personal information would be destroyed after an appropriate interval.

Finally, the bill would require the Commissioner to make aggregate information publicly available. Although the bill language emphasizes that this aggregate data shall not include personally identifiable information, this would be very difficult to achieve with smaller institutions at the level of disaggregation required by the bill. In addition, much of the information subject to public disclosure appears to currently be available via IPEDS.