The Privacy Implications of Self-Sovereign Identity in Education

Education information systems that are built upon concepts of self-sovereign identity (SSI) have the potential to transform how students manage and disclose their academic records by increasing control, access, and transparency. These systems may also reduce the burden on school districts, colleges, and various other education providers across the country. They would also provide parents and students with powerful new ways to control and leverage their education data while ensuring privacy and security in compliance with existing and emerging privacy laws. This white paper reviews key privacy topics and considerations for information systems leveraging the principles and approaches of SSI.

SSI in Education: An Example

Jordan found her career passion through her high school shop class. After high school graduation, she apprenticed at a local machine shop and attended trade school. She was soon hired by a popular motorsport team.

She has excelled in her profession and quickly rose through the ranks to a supervisory role as head machinist. She has now set her sights on a higher leadership position in the company. While she is talented and well-respected, she realizes that she needs more business and management skills.

Jordan decides to enroll in classes after hours at a local community college. However, she feels overwhelmed by her busy schedule and the prospect of applying for college, given it has been so many years since she graduated trade school. She is interested to learn that her state has implemented a digital transcript system that will allow her to easily review her records and transcripts electronically, and then share those records with the community college during the application process.

The process is simple:

1. Jordan finds the system through the State Department of Education website.
2. She provides the required identification to enroll and downloads a mobile application that enables her to search for and identify her education records from high school and trade school.

3. She uploads additional professional certificates and several digital badges, awards, and proof of participation in vocational training she attended throughout her career. These documents are hosted in the application's digital wallet.
4. She searches for the community college to which she wants to send her credentials. Having successfully authenticated herself by logging into the system and providing her consent to share her data with the college, her application is complete.
5. Shortly thereafter, she receives a call from the admissions counselor welcoming her to the college's school of business.

While this experience is a welcome contrast to her effort to apply to trade school, it also seems surprisingly easy. She wonders how secure the information she submitted to the application is, and what privacy protections the system offers.

What is SSI?

Individuals generally have many identifying credentials for the various systems and services they interact with online. The number and disparate nature of these credentials can make them difficult to manage. SSI is a set of principles that work to support and enable individual control over this identifying information, including their online credentials.

Instead of a password or simple knowledge factor, a verifiable digital identity adopts principles of SSI that create trust and assurance. In doing so, they create an infrastructure in which all participants can trust data, including individuals, schools, credential issuers, and authorities. The underlying SSI principles mean that technology is used to increase transparency and allow students to make smart decisions regarding what and how much data will be shared, minimize the risk of unwanted data sharing, and empower the individual to make critical decisions regarding who gets access to sensitive personal information—and to what extent they can access it.

The Ten Principles of Self-Sovereign Identity (Allen, 2016)

Principle	Explanation
Existence	Users must have an independent existence
Control	Users must control their identities
Access	Users must have access to their own data
Transparency	Systems and algorithms must be transparent
Persistence	Identities must be long-lived
Portability	Information and services about identity must be transportable
Interoperability	Identities should be as widely used as possible
Consent	Users must agree to the use of their identity
Minimization	Disclosure of claims must be minimized
Protection	Rights of the users must be protected

Currently, students face real challenges when using existing education credentialing and verification systems. Systems that are aligned with the principles of SSI place the individual student at the center of any credentialing process so that the student becomes the source of his or her identity. The technology systems built according to principles of SSI support improved mobility as students move through key life events. For example, interconnected education information systems aligned with SSI could help students verify their education credentials with new education institutions digitally as they move schools with little to no cost or delay. It could also serve students later in life by providing verifiable proofs to future schools, training programs, or even employers.

For Jordan, accessing a system aligned to the principles of SSI would enable her to remove friction from the credentialing processes and reduce the burden on both students and educational institutions. She would benefit from a system that aligns with the principles of SSI, enabling her to more efficiently explore her education records with access to more data that can be converted to credit towards her new degree, saving her time and money. This exchange can occur more quickly and seamlessly than the process of requesting that physical records be mailed to a future school; requires less effort for both Jordan and the schools involved; and, thanks to modern data security controls such as encryption, blockchain, and digital signatures, can be more secure than currently used methods.

Verifiable credentials are statements given to individuals by issuers that assert something about that individual. From our example, a verifiable credential might be a digital diploma from a school. Individuals keep credentials in a digital wallet for use when verifiers need to prove the individual's claims. Governance authorities add context and rules to these transactions; such as deciding which issuers are trusted, and which are not.

Because the state Jordan lives in manages the digital transcript system, they act as a governance authority, creating rules regarding what credentials are supported and which institutions are trusted. Verifiable credentials support a variety of proof mechanisms to ensure the credentials are reliable, that the issuer attests that they are correct, and suspends or revokes issued credentials if necessary.

DIDs serve as unique identifiers for individual credentials that are registered with a public network. Notably, DIDs are built on open standards, so individuals can register any DID to any public network without being locked into a particular vendor or system. Decentralized identifiers provide a means for both institutions and learners to establish identity without relying on a centralized party. The same DID Jordan uses to access the state system could be utilized as a consistent, platform independent identifier across systems to access high school records, professional development courses, and even vocational school.

Private keys constitute the digital signature of the trusted issuer. Private keys are typically issued by trusted third party certification authorities. In the case of Jordan, one of the trusted issuers might be the trade school she attended years ago. When the private key of the trade school is associated with the digital credential that she sends to the community college, it serves as proof that the credential is genuine and was issued by the school. Private keys can be loosely compared to the physical key to a house.

Public keys are paired with private keys and written to the public network in association with DIDs to give verifiers a way to associate issuers' DIDs with digital signatures. If a private key can be compared to the physical key to a house, the corresponding public key is the house's address. Both the private and public keys are needed to access credentials.

Several technologies are responsible for enabling SSI, including verifiable credentials, decentralized identifiers (DIDs), private keys, and public keys. In turn, these are used by institutions and individuals, including issuers (such as schools), individuals (such as students), verifiers (such as employers), and governance authorities (such as state education agencies).

FERPA, SSI, and FIPPS

Federally owned or operated systems that house or process an individual's data are generally required to incorporate processes to protect the privacy and security of the individual. These Fair Information Practice Principles (FIPPs) form the core of the Privacy Act of 1974, and are widely incorporated into other federal information privacy laws.[1] Both the Federal Educational Rights and Privacy Act (FERPA) and SSI share a common emphasis on FIPPS principles, empowering people to be informed of the information collected about them, providing access and consent to its use for specified purposes, and ensuring that these data are correct and protected from unauthorized disclosure.

This lineage forms an important foundation of privacy and security for data in general, and the continuity between FIPPs and SSI principles means that data remains protected even when federal laws, such as FERPA, may no longer apply. FERPA incorporates several fair information practice principles as requirements:

- **Use limitation** - Any consent form under FERPA must specify the purposes for which the data is being disclosed. This is effectively 'use limitation,' since any use of the data for purposes other than what the individual has consented to would potentially constitute a violation of the law. Notably, FERPA does permit PII from education records to be disclosed without consent under one of the exceptions. Exceptions to the FERPA general consent rule have specific prohibitions or criteria that must be met before information can be disclosed, such as legitimate educational interest in the case of the School Official exception, or conditional on parent or eligible student "opting out" of disclosure in the case of the Directory Information exception.

- **Data quality/integrity** - Individuals have a right to request amendment of their education records in order to correct false or misleading information.

- **Security safeguards** - FERPA requires that PII from student records not be disclosed without consent and that schools adopt 'reasonable methods' to protect the information from unauthorized disclosure. There are a few limited exceptions, such as when teachers must exchange student information as part of their educational duties. The general consent rule does not apply, as this activity is

[1] https://www.nationalpublicsafetypartnership.org/Documents/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf

specifically exempted under the “School Officials” exemption. A school official generally has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. Other exemptions include provisions to enable schools to conduct studies, perform audits and evaluations of educational programs, or respond to health or safety emergencies. All of these exceptions come with limitations that aim to protect the privacy of student data, such as limitations on redisclosure and data use.

- **Transparency and openness** - Under FERPA, schools and districts are required to annually publish a notice of parent and eligible student rights as it pertains to the law. If the school or district also opts to create ‘directory information’ policy, the school must provide notice to parents and eligible students of what information is contained within that policy and provide for them an opportunity to opt out of the disclosure. Additionally, the Department recommends that schools, districts and IHEs be transparent about their data collection and use in order to build trust with the parent community or with other stakeholders.

- **Accountability** - While not required under FERPA, accountability is a component of several fair information practice principles. The Department recommends as a best practice that agencies and institutions train their staff on FERPA and other applicable privacy laws.

However, it is important to note that in this particular use case, FERPA would have only limited applicability. In short, Jordan would consent to the disclosure of her records. Under FERPA, any disclosure of PII from education records requires the consent of the parent or the student, in the case they are over the age of 18 or attend a postsecondary institution—with some exceptions.

Jordan’s transcript is considered an ‘education record’ under FERPA because it is directly related to her and maintained by the school or university (or a party acting on their behalf). She would need to provide consent in order for the school to essentially ‘release’ this transcript into the digital transcript system. Once the transcript is provided to the system, there would be no further application of FERPA. The digital transcript in this case could be considered a ‘copy’ of the education record and would be considered to be wholly owned by Jordan and therefore may be redisclosed, shared or deleted so long as the system permits such actions. Thus, while the protections of FERPA may cease, a system that embraces principles of Self-Sovereign Identity can continue to provide privacy and security to that information because it is intrinsically tied to her identity. And because these SSI principals align FIPPs that are present in FERPA (or recommended by the Department), the privacy and security protections of the information are maintained, even after the application of federal law has ceased.

The following principles of SSI align with the either requirements or best practices for data privacy and security under FERPA and other privacy laws/principles:

- **Control** – While FERPA-protected student records are owned by the school and not the parent or student, FERPA requires that parents and eligible students have a certain amount of control over the use of those records that schools maintain on their children, or themselves. A system that embraces this SSI principle extends that control beyond what FERPA provides because it would allow the parent or student greater visibility into the use of that data and control of its distribution to outside entities with a more granular approach. Where FERPA consent forms are generally written as broadly as possible, a system which embraces SSI principles might provide a host of controls to enable the user to control exactly what data is shared and under what conditions, and to view the provenance of information in their records.

- **Access** – FERPA requires that schools provide access to education records they maintain on students. A digital transcript system that allows access to the records that a student owns extends this right because it reduces the barriers involved in obtaining copies and forwarding official transcripts through regular channels, and allows this to be done both quickly and at the student's convenience. This benefits schools as well because technology integral to SSI, such as verifiable credentials and digital signatures, enable this exchange to happen seamlessly without the need to manually verify these assertions.

- **Consent** – The student must consent initially for the disclosure of records into the digital transcript system. Providing means for additional consent reinforces the control and transparency of how the system uses and shares the data contained within. Note that there are exceptions that allow disclosures of information without consent in specific instances like when school officials need to share data within a school. Please see the FERPA Exceptions Summary from the Privacy Technical Assistance Center for more information.

- **Minimization** – Data Minimization is the concept of collecting and retaining only the data elements required for a particular need. It is considered a best practice under FERPA to apply data minimization principles to the collection and retention of student records to ensure that data is sufficient and relevant to the need. SSI principles reinforce that by applying approaches, including zero-knowledge proofs; for example, a system may provide proof that an individual is above a certain age without revealing an individual's date of birth. This can minimize the specific identity details about a person which are disclosed.

- **Transparency** – This is another recommended practice under FERPA. When system owners are transparent about data use and processing, parents and eligible students remain aware of the decisions and use of information that schools maintain on students. Being transparent means being open about what data is being collected, who data is being shared with, and the reasons for sharing the data. A system that embraces this principle of SSI builds trust with users regarding the use and disclosure of data.

Moving forward with SSI in education from a privacy perspective

As they both intend to increase the security and privacy of student data while allowing for better control, FERPA and SSI can work together to modernize education data and credentialing. The education data community now must move forward and establish the collaboration necessary between education stakeholders, such as schools, ed tech vendors, and the public, to develop open and transparent standards and systems to leverage these technologies to their fullest potential and transparency.

Incorporating SSI principles into the development and design of education technology provides the opportunity to proactively address data privacy and security at the earliest stages. If privacy is left as an afterthought, it becomes far more difficult to resolve issues as they arise. It is important for the community to include privacy and cybersecurity experts who can provide a strong stance on not only compliance, but also ethical and technical implications of choices made while building the governance framework.

Bringing together the education data community and beginning to consider these approaches is the first step and perhaps the hardest. Collaboration is difficult under the best circumstances, and aligning the interests of parents and students, education officials, technology vendors, and policymakers are just a few of the groups to include.   Determining who is a best fit in this process is specific to your circumstances. It is better to engage stakeholders early and be thoughtful and strategic in your approach. Though this type of engagement may prove challenging, it is an essential step in protecting the privacy of students throughout their lifelong learning journey.

References

Allen, C. (2016, April 25). *The Path to Self-Sovereign Identity.* Retrieved from Life with Alacrity: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html