PRIVACY, SECURITY, INTEROPERABILITY: WHY ONE SUPPORTS THE OTHER

Data interoperability is a helpful component to building and maintaining quality software. Interoperability isn't a panacea, but making intentional and informed choices about implementing an interoperability standard contribute to better development practice, better privacy practice, and better security practice. **Here are 5 ways interoperability, privacy, and security enhance each other.**

Clarity: Implementing an interoperability standard adds clarity to data collection and management

Most interoperability standards define information that is required to align with the standard, and/or that is required in order to have the standard achieve its purpose. The structure that standards provide can be considered “guard rails” that protect against collecting more data than is needed to provide a service. Additionally, because an interoperability standard defines the data elements you are using and storing, it is easier to determine the best strategies for protecting the information trusted to you.

Ownership: Interoperability is essential to data portability and ownership

Supporting interoperability means that a vendor has made steps to support people using a system to get their information out of that system. This is a critical first step to supporting data portability. Most consumer systems make this incredibly difficult to do, if they support it at all. From a business perspective, the rationale behind this is clear: if a company makes it easy for a person to leave a platform, some companies are worried that people will do just that.

Companies that support interoperability show a level of respect for the people using their service. By supporting interoperability, they have taken a critical first step toward ensuring that people both own and have unbroken access to the information they create in a system.

Security: Supporting an interoperability standard creates secure and usable software

Implementing an interoperability standard can help companies build better products because the data standard helps inform the underlying data architecture of the product. Using a data standard allows a company to get the benefit of a solid data architecture as the foundation of their work. Data architecture is invisible to most people using software unless you know where to look, but the benefits of a sound data architecture - like many invisible things we don't think about - are easy to take for granted.

How many times have you used a software product where it takes you 15 mouse clicks to accomplish a simple task? In some cases, this is just bad design, but frequently, it's an indicator of a sloppy data architecture. In many cases, bad design decisions get made because the underlying data architecture makes better decisions impossible.

The work that goes into defining an interoperability standards reflects countless hours of experience spent solving real problems in real-world use cases. If we think of an interoperability standard as free consulting on a data architecture, we get a clearer sense of the processes behind defining interoperability standards.

Transparency: Supporting interoperability increases transparency around data practices, a requirement for informed consent.

An additional benefit of both supporting interoperability and using an interoperability standard is that it simplifies the process of documenting what information is collected, how this information is used, and how access to this information is controlled. When a company or an organization commits to using an interoperability standard, it is easier for them to be more transparent. Increased transparency leads to an environment where informed consent can become the norm -- rather than the exception -- in using software.

Compliance: Interoperability standards simplify the process of privacy law compliance

In Colorado, the Student Data Transparency and Security Act went into effect in 2017. Two of the requirements of this law include vendors providing education agencies with clear information about the student data they collect, and vendors agreeing to destroy data shared with them if the school or district requests this. Because interoperability standards make it easy to document data that is collected and stored, the process of producing that information for education agencies is subsequently easier. Along similar lines, if and when a school asks for data to be destroyed, the improved data architecture that comes with implementing a data interoperability standard will simplify the process of destroying data.

On May 25, 2018, the General Data Protection Regulation (or GDPR) went into effect in the European Union. This law is not in effect in the United States but provides a clear signal for the evolving regulatory structure and consumer demands relative to data portability and security. One of the rights for people under GDPR is the right to data portability. The regulations specify that people must be provided their information "in a structured, commonly used and machine-readable format." Because interoperability standards define commonly used and machine-readable formats, using an interoperability standard streamlines compliance with this section of GDPR.

PROJECT UNICORN

Project Unicorn is an effort to improve data interoperability within K-12 education. We aim to create a community of innovators who make the broader case for secure interoperability by determining shared priorities, working in partnership with school systems and vendors to understand its importance and benefits, creating a demand side push for interoperability through partnerships, and educating buyers to consider the total cost of ownership through informed comparison of vendors.

Project Unicorn does not endorse a specific product or data standard but instead is an educational initiative dedicated to the secure, controlled interchange of data.

*INTEROPERABILITY: THE SEAMLESS, SECURE, AND CONTROLLED EXCHANGE OF DATA BETWEEN APPLICATIONS