Technology Observations for Student Privacy

(1) The weakest link in any security system is the human beings who use it.

(2) Even in the digital age, the "cloud," and the world wide web, possession is still nine-tenths of the law. Direct physical control of digital information is practically indistinguishable from complete ownership. Absent exclusive, direct, physical control, claims of ownership or even responsible custody are largely wishful thinking.

(3) Personal information cannot be "anonymized" by the use of numerical identifiers (as claimed for statewide databases). Widely-reported scholarly research has found that individual Americans can be identified with 87 percent accuracy using just a birthdate, gender, and zip code. For rural Vermont, that percentage is probably higher.

(4) In the world of digital technology as elsewhere, the very best way to keep a secret is not to share it. Generic claims that data is "encrypted" do not mean that students' personal information is protected *in any way* from access by outside hosting providers.

(5) Local computing infrastructure is not rocket science; environmental requirements are nearly zero; administration is frequently automatic or software-assisted.

(6) Assembling many student records together for "efficiency" significantly reduces the security of any individual record.

(7) The strongest security is achieved by transparent system design --- not "security by obscurity." Security professionals advise that the security properties of a system should be independently provable from its internal structure and the assumption that its passwords or secret keys have not been compromised. Thus, security algorithms, source code, and all implementation detail should be open to public inspection and critique.

(8) Software (especially free and open-source software) is at least as easy to share as personal information. Should we export personal data to software vendors when we can more easily import software to process that data locally?

(9) Perimeter defense and intrusion detection are easier and more effective for smaller communities of authorized users.

The personal information about our children that outsiders wish to collect from us and then return to us as a "service" is already available at the fingertips of our school principals and superintendents. "Education reform" is little more than a major assault upon our children's privacy, including exporting personal information to outsiders, coerced student use of Internet websites, useless statewide databases, remote computer testing, retention of student data by outside consortia. Is a national consensus on completely obvious grade-level learning standards worth ongoing massive violation of our children's privacy?

Vermont should be a leader in educational privacy as well as in education.

www.respect4students.org