Why Internet Age Verification Makes Kids Less Safe
Or… Nothing <u>is</u> sometimes better than something

Jeff Schmidt
jschmidt@authis.com

No security measure is perfect. When considering the implementation of any security measure, we must also analyze what happens when we fail. This is especially true when dealing with the security of something as valuable as our children. The unfortunate reality is that even the most well intended actions can and often do have negative unintended consequences.

When a security measure fails, the resulting "overall level of security"[1] will be affected in one of three ways:

Net increase in security. Most security measures fail in this way. Consider a door lock or a bank vault: if a criminal forces open the lock or blows a hole in the vault, even in failure, the net security of the overall system is still increased. The act of forcing open a lock or dynamiting a vault takes time, resources, and generates noise that may alert authorities or trigger alarms. Most importantly, compromising one vault usually does not help a criminal compromise other vaults.

No change in the level of security. Optional additional screening fails in a way that has no net effect on the overall security level of a system. If a bad actor is not randomly selected for additional screening, he still is subject to normal screening. The existence of the random screening is a net plus, but not selecting a bad guy does not lower the overall security level.

Net decrease in security. This is a particularly subtle and dangerous failure mode; while few security measures fail in this way, it is important to spot and avoid these pitfalls. The root cause of this type of failure usually lies in a "daisy-chain effect" – a scenario where one failure lays the foundation for future compromises, or results in an easier path through the remaining security measures.

Internet youth age verification for the purpose of protecting children from online predators fails in this way.

Bruce Schneier, the security expert's security expert, has written extensively about this specific type of failure in reference to the Registered Traveler program.[2] While I don't wish to get into a debate about Registered Traveler, from a security perspective, Internet youth age verification has some important similarities to it. The objective of both programs is to identify and credential good actors for the purpose of segregating the population into "trusted" and "untrusted" groups. In Registered Traveler, the trusted

[1] "Overall level of security" is an abstract concept and not well defined.

[2] http://www.schneier.com/blog/archives/2007/01/clear_registere.html
http://www.schneier.com/essay-051.html

persons are subject to expedited security procedures at the airport. Similarly, the objective of youth age verification is to create "safe" areas on the Internet for children.

Unfortunately, both programs also fail in a way that yields credentialed – "trusted" – bad guys. We end up with less security than had we done nothing![3]

Regarding Registered Traveler, Mr. Schneier writes: "One counter-argument to this analysis is that most people won't be able to subvert the system… Most people will either get a card (or not) honestly, and use the system correctly. And while a few might be able to successfully attack the system, that's no reason to throw it out entirely. But the whole point of the system is to work in the face of a dedicated and well-funded adversary. Even the argument that most terrorists are stupid misses the point. It doesn't matter whether or not average people can subvert the system; we want security systems that protect us against smart people, especially smart terrorists."[4]

Replace "terrorist" with "child predator" and you see the danger. We must assume that our enemy is smart, motivated, and will become credentialed. Thus, we must assume that the "safe areas" we are trying to create using youth age verification will in fact be target-rich environments populated with underage children and credentialed predators.

In security, "something" is not always better than "nothing."

Worse, the "safe areas" will be confusing to both children and (already confused) parents. Are they really "safe" or "safer" or are they just as dangerous as the Internet at large? What guidance should adults give children when interacting in these supposed "safe" areas? The "safe areas" are in fact no more or less safe than the Internet at large. However, it is likely that this important reality would be lost resulting in a dangerous false sense of security and a net decrease in the level of security.

[3] In all fairness, Registered Traveler is as much a convenience program as it is a security program, and it does provide some benefits. However, Internet youth age verification is intended entirely as a security program.

[4] http://www.schneier.com/crypto-gram-0403.html#10