Written by **James Heiser** on October 13, 2010

Schools Track Students with RFID Chips

It appears that in several Houston-area schools, the motto for student security is: "If it is works for tracking cattle, it will work for tracking children." The school district has installed radio frequency identification (RFID) chips in identification cards issued to students, and this move is alarming parents — and others — who are worried that a step taken to protect students may actually place them in greater danger.

According to a *Houston Chronicle* article, the decision to track school children with RFID is starting to generate the same concerns which similar efforts sparked in California. According to Jennifer Radcliffe, a reporter for the *Chronicle*:

> Radio frequency identification — the same technology used to monitor cattle — is tracking students in the Spring and Santa Fe school districts.
>
> Identification badges for some students in both school districts now include tracking devices that allow campus administrators to keep tabs on students' whereabouts on campus. School leaders say the devices improve security and increase attendance rates.
>
> "It's a wonderful asset," said Veronica Vijil, principal of Bailey Middle School in Spring, one of the campuses that introduced the high-tech badges this fall.

How expensive technology trumps an old-fashioned "roll call" when it comes to increasing attendance is uncertain. Surely it is at least as easy to fool a scanner by having a friend carry your identity card to school as it is to have them stand in for you in a classroom roll call. The inability of teachers to keep track of their students while on campus sounds more like a human failure than a lack of technology. The underlying problem of keeping track of students while on campus has not gotten worse over the past few generation in the sense that students have developed some new technology of classroom avoidance which requires a technological escalation on the part of teachers to "keep up."

While school administrators want to track students as if they were cattle, at least some of the parents are demonstrating that they are not merely sheep. As Radcliffe reports, the grownups understand that Big Brother is not looking out for the welfare of their children:

> But some parents and privacy advocates question whether the technology could have unintended consequences. The tags remind them of George Orwell's Big Brother, and they worry that hackers could figure a way to track students after they leave school.
>
> Identity theft and stalking could become serious concerns, some said.
>
> "There's [sic] real questions about the security risks involved with these gadgets," said Dotty Griffith, public education director for the ACLU of Texas. "Readers can skim information. To the

> best of my knowledge, these things are not foolproof. We constantly see cases where people are skimming, hacking and stealing identities from sophisticated systems."

The security problems associated with the student IDs are similar to those which have plagued RFID-chipped passports. It has been known for years that RFID chips implanted in passports are a less-than-wise idea; the danger of criminals or terrorists "skimming" the data on the RFID led to passport shielding, which allegedly allows the data to be read only when the passport is open. CNET reported on the RFID passport security experiments conducted by Lukas Grunwald, a researcher with DN-Systems in Hidesheim, Germany, four years ago:

> Grunwald did say that he has not unearthed any flaws in the crypto that protect the integrity of the information stored in the chips in passports. In other words, while the data can be cloned merely by scanning the RFID tag, the information cannot be changed. Grunwald was able to read the data on the chip by duplicating a customs inspection station.
>
> It took Grunwald "two weeks and $5,000 in legal fees" to complete his project, which uses RFID-reading hardware and some homegrown software, he said. At Defcon on Friday, Grunwald also tested his setup with some corporate access cards, which he was also able to copy. This means an attacker could copy access cards and use the copies to open doors to secured buildings.
>
> "You can add RFID in a secure way, but especially in electronic passports the standards are created by compromise, and by compromise you can not do it securely," Grunwald said. "You need a lot of research to do it right, and that research is not done right now."

Several months ago the Electronic Frontiers Foundation, a technology and privacy watchdog group, highlighted some of the dangers of introducing RFID chips into the educational process:

> But of course, an RFID chip allows for far more than that minimal record-keeping. Instead, it provides the potential for nearly constant monitoring of a child's physical location. If readings are taken often enough, you could create an extraordinarily detailed portrait of a child's school day — one that's easy to imagine being misused, particularly as the chips substitute for direct adult monitoring and judgment. If RFID records show a child moving around a lot, could she be tagged as hyper-active? If he doesn't move around a lot, could he get a reputation for laziness? How long will this data and the conclusions rightly or wrongly drawn from it be stored in these children's school records? Can parents opt-out of this invasive tracking? How many other federal grants are underwriting programs like these?
>
> These are questions that desperately need answers. California is in the middle of a terrible budget crunch, but the solution is not federally funded surveillance of children who are too young to understand the implications.

The EFF assessment highlights a central issue in the debate over "chipping" America's school children: RFID monitoring is a very poor substitute for "direct adult monitoring and judgment." RFID might be fine for monitoring inventory in a warehouse or cattle on the range, but it is inexcusable to treat students like a side of beef. Teachers need to put down the RFID skimmer, and spend their time *teaching* their students, not *monitoring* them. The dangerous experiment in Big Brother monitoring systems in some California and Texas schools is a very poor civics lesson for the children submitted to such an ill-considered misuse of technology.