

Children's Privacy Requires Special Handling

Jay Cline

December 21, 2004 ([Computerworld](#))

Although you may spend most of your workday overseeing your corporate network, at home, you've got an IT job that's at least as important: protecting your children's privacy online.

A host of new technologies -- from location-based cell phones to radio-frequency school IDs -- may soon make today's teenagers the most-tracked generation the U.S. has known. In a world where violent crimes against children are a continuing threat, this is a good thing. But parents should be wary of raising children with no sense of privacy, and they need to consider some guidelines for high-tech monitoring of children.

What started all this kid tracking, anyway?

You'd have to go back to the pivotal event of 1993: the explosion of the World Wide Web. When children downloaded the first Internet browsers, they gained unprecedented direct contact with the adult world. Now, any child could go to the online library, view obscene material and interact with adult predators in online chat rooms.

Parents quickly responded. They demanded Internet-filtering software and restrictions on Internet access in schools and libraries. They also lobbied Congress to pass the Children's Online Privacy Protection Act, which limits data collection from kids.

But then came the cell phones. The Yankee Group estimates that a third of U.S. children carry the devices, a rate that's expected to soon hit the three-quarters mark you already see among Scandinavian and Japanese teens.

With the recent emergence of camera phones, our children's voices, images and locations are now practically a matter of public record. Meanwhile, parents in the U.S. and Japan have been watching a rash of school shootings and stabbings on the nightly news during the past decade. They're worried about how they could contact their own children in an emergency.

Which brings us to the present moment. Today's parents have a pent-up motive for ratcheting up the surveillance of their children -- and recent technical advances have now given them the means.

The primary means of parental surveillance in the 21st century has become the cell phone itself. Most parents have quickly turned the risks of this device into an opportunity to find out where their kids are and what they're doing. Wondering why Johnny missed the curfew? Just give him a ring.

But some are now taking it a step further. Companies from the U.S., the U.K. and France are offering kid-tracking services based on Global Positioning System (GPS) technology. The services track the real-time location of a child's cell phone and provide parents e-mail or voice-mail alerts of movement outside predetermined parameters.

With GPS-enabled "black boxes" increasingly included in new vehicles, it's only a matter of time before parents are also tracking the movement of their teenagers' cars. Indeed, retired Gen. Tommy Franks announced last week the formation of a new company to use GPS-enabled cell phones to track

teen driving speeds and alert parents of excess velocity.

The second new technology promising to enhance the surveillance of children is radio frequency identification (RFID). The first pilot schools in the U.S. have embedded RFID chips into their ID badges to help record the whereabouts of students. Some Mexican parents have reportedly even implanted RFID chips under their children's skin.

But perhaps the most important development may be the growing prevalence of video surveillance in U.S. schools. In 2002, just 15% of U.S. public schools used surveillance cameras, but by some counts, that percentage may have already doubled. Chicago's mayor announced this fall ambitious plans to link all the city's schools by camera into a 911 center.

So it's quite possible that tomorrow's child will be recorded from cradle to diploma. What's the downside to all this?

If our children are always being watched, they may well lose any natural instinct of privacy and modesty. We can already see some of the results of this: a proliferation of reality shows and personal weblogs where young people publicly expose what they previously would have kept to themselves. A generation of children who don't internalize their privacy may be more accepting of government and corporate intrusions into their personal space.

There's another downside to our children leaving electronic footprints everywhere. If these footprints aren't properly secured, outside marketers -- and predators -- will have more chances of getting between parent and child. Parents using these tracking technologies may actually be putting

their children's safety in jeopardy.

So what should a parent do? Under the Cline roof, for starters, we've implemented our own privacy and security policies for the Information Age:

1. **The Father Firewall.** No adult can elicit personal information from the children without Dad's prior approval. Any holes in the firewall that are discovered will be immediately terminated, and access privileges may be suspended.
2. **Right to Audit.** Children should have no expectation of privacy from their father, who reserves the right to audit any part of the information infrastructure without notice.
3. **Technology Certification.** Mom and Dad and the kids won't be the beta-testers for any bleeding-edge technology. We'll only certify the use of technologies whose security has been proven -- and that Dad understands.
4. **Business Justification.** The burden is on the children to justify the business case for any technology acquisition, particularly mobile devices. Popularity among peers is a soft-dollar case that won't go far.
5. **No Monitoring Without Cause.** It's up to Mom and Dad to raise the children to make wise decisions at an early age. Monitoring and tracking will be an exception, not the rule.

Do readers have any of their own home policies to add to the list? Drop me a line at privacy@computerworld.com.