RFID hits privacy snag

by Richard Bray

Every blessing of the computer age seems to carry a curse – keyboards and carpal tunnel syndrome, email and spam, networked computers and viruses. And now, materiel managers who looked forward to better inventory control, greater efficiency and easily-documented cost savings from Radio Frequency Identification (RFID) technology may have to wait longer and spend more to receive fewer benefits. A storm is brewing over the consumer privacy implications of this revolutionary new technology.

The same tiny chips with antennae that allow inexpensive, precise tracking of even tiny objects within a warehouse could, in theory, also be used to track consumers as they wander through a shopping district or spy on workers in a work environment. The same technology that could save billions of dollars by reducing theft, loss and inventory levels could also be used to create detailed dossiers on spending and travel patterns.

The same features that bring benefits in one environment are seen as intrusive in another. In the supply chain, unique numbers right down to the individual component or item mean a lasting digital record and instant inventory. In the shopping mall, the unique identity signal of a sweater could alert every store employee that a certain customer is on the way. In the workplace, RFIDs in identity badges could track employees' every move – or lack of movement.

At the retail level, the Wal-Mart chain has discontinued trials of an RFID "intelligent" inventory system that would have tracked items from the warehouse to the store, and from the shelves to the cash register. A major clothing manufacturer has sidelined its initiative to plant RFID chips permanently in every garment. Advocacy groups went public with concerns about retailers who might track consumers after the sale, scanning shopping bags and clothing to create instant profiles.

Beyond the shopping malls of the world, there is a storm of protest in Great Britain over government plans to fit every automobile with chips to provide an instant snapshot and enduring record of its movements. Not surprisingly, the Association of Chief Police Officers developed the Electronic Vehicle Identification proposal. The technology could alert police to cars that are speeding or illegally parked, or even issue tickets automatically.

While 1984 may be arriving two decades late for British motorists, privacy advocates in the United States have already received a sympathetic hearing from Californian legislators and new state laws on RFID privacy may soon be in the works.

Privacy concerns are not the only major obstacle to the vision of a single, standard RFID tracking system. High tech companies pay lip service to standards and a level playing field, but Microsoft's example of market dominance is a constant temptation to add proprietary features that slow or even eliminate the competition.

The big multinational companies that could force at least some standardization on the RFID market have not yet flexed their muscles to impose order, and international standards bodies have been slow off the mark. End users looking for inexpensive, COTS (Commercial Off the Shelf) solutions have a while to wait.

That said, there are billions of dollars of sales for vendors and recurring savings for purchasers on the RFID table. Proponents of implementation are fighting back, retaining the services of Fleishman-Hillard, one of the world's largest public relations companies to work closely with the Auto-ID Center at the Massachusetts Institute of Technology, a key player in RFID development.

In the world after September 11, 2001, it was probably inevitable that the emerging RFID industry would play the counter-terrorism card as an argument for RFID implementation.

In military deployments to Bosnia and Iraq, proponents say, radio frequency identification tracking reduced the time to distribute supplies on site from days to minutes, by instantly indicating the contents of containers. Large shipping companies are beginning to attach anti-tampering RFID tags to container locking systems, to issue alarms when they are compromised. Unfortunately, for wider usage, those systems are "one offs," for use in limited applications.

Vendors are lobbying hard to have RFID classified as anti-terrorism technology, which would not only lend instant credibility, but also protect manufacturers against lawsuits if it failed under certain conditions. One application might be in the grocery supply chain, to protect food products from contamination.

Because governments purchase such a wide range of goods and services, only wide-scale and standardized deployment of RFID technology can make a real difference. The war against terrorism may provide the decisive push.

Richard Bray is an Ottawa-based freelance writer specializing in the IT sector. He has been published in magazines and newspapers in Australia, the US and Canada. Before freelancing, he worked as a producer, reporter and senior writer for CBC in Toronto.