



## Guest Columnist CARL BROWN

# Consumer privacy: A ship that has already sailed?

A classified document, never meant to leave the room, finds itself locked inside an unauthorized briefcase. As the briefcase is carried out of the building, it passes through a specialized reader, hidden inside a wall. The reader polls the air, searching for a pre-defined response. The document, printed on Radio-Frequency-Identification (RFID)-tagged paper, emits the response. As the briefcase moves through the doorway, a high definition video camera captures the moment. A silent alert is transmitted electronically to the nearest security personnel, complete with the video and the document identification. By the time the carrier of the briefcase opens his car door, security apprehends the suspect, with the video evidence, time-stamped and verified.

This scenario illustrates the seductive power that draws decision makers into wider and more pervasive use of RFID-enabled applications. Both government and industry leaders can envision a future in which wireless, invisible technology tracks people and things. Activist consumer groups write books, stage protests and lobby against the loss of privacy which these technologies portend. Patent applications for invasive, manipulative sounding tracking devices are filed by companies such as IBM, Procter & Gamble and NCR, even when the companies themselves admit they have no plans to use them. Marketing companies salivate over the concept of recording human behaviors in an undetectable form. Journalists imply that these tags give us the ability to silently observe and record data on people, similar to the research of the noted anthropologist, Jane Goodall, who quietly watched chimps in the wild.

"One of the most worrisome applications of RFID is the proposal to place the chips into cash," says Katherine Albrecht, founder of the consumer group CASPIAN and author of *Spychips: How Government and Major Corporations Plan to Track Your Every Move with RFID*. Albrecht is worried that widespread, invasive use of RFID would rescind the freedom which anonymity provides. A picture of readers placed in airports, supermarkets, shopping malls and offices, with tags implanted under our skin, reminds us of Ira Levin's

1970 book, *This Perfect Day*. In Levin's book, people are taught from birth to hold their wrists under wireless scanners as they walk by, so the great computer database hidden in a cave can keep a record of their movements.

And therein lies the rub, with popular worries today about the loss of consumer privacy. People are worried about loss of privacy from their credit cards, their grocery store discount cards, the barcodes on products and RFID-tagged items. Any of these products could potentially lead to a loss of privacy. Even our social security numbers, assigned in hospitals at birth, can mean we have no hope of anonymous living. We give out our social security numbers when we order telephone service in our house, apply for a mortgage, get a health insurance card, a job, or a car loan. Our drivers' licenses serve as the photo ID for anything we do.

We have little privacy as it is. Adding RFID to our lack of privacy won't make it any worse. Having researched and investigated the RFID industry over the past years, I believe that RFID is not the tipping point which changes our lives from private to exposed. That tipping

point was reached 20 years ago, when the credit card company databases instituted the concept of a "credit score."

In fact, the sheer volume of potential information about our lives, added by widespread use of RFID, promises to shield us from that exposure. More data, as any information technology professional will tell you, does not equal more information. More video, which needs to be watched by an attendant, means more actions will be missed. More recordings of telephone conversations, when searched by a software algorithm looking for keywords, results in more tape recordings that no one has the time to hear. More mappings of consumer movements, stored in bigger and faster databases, mean more nonsense spewed out the other side in patterns that lead to no actionable result. The more data we gather, the less important the gathered data becomes, until and unless we choose to target an individual.

In my experience, the aggregate databases won't be worth mining; ergo, the purpose of pervasive installations of RFID will degenerate to targeting of specific individuals or specific asset movements.

"When it comes down to tracking an action of one person, or the movement of one item, an RFID installation which triggers an alert when an item moves, and identifies exactly what happened at that time, with video evidence, can become like the DNA technology of physical identification," says a former NCIS agent who consults on physical security issues. "Before we had DNA evidence, we put people in jail who didn't belong there. DNA changed that, and made it possible for us to prove our case with certainty. RFID systems that identify movement with certainty, and give us video of the time, can prove who didn't do the crime, as well as who did."

I believe that privacy advocates miss the mark in targeting RFID. Databases filled with errors, mined for misunderstood criteria, may be the heralds of a Brave New World, but solid RFID-video evidence, like DNA technology, can only help us protect the innocent. ■

Carl Brown is the founder and president of SimplyRFID, which offers the Nox intelligent perimeter defense system. He can be reached at: [carl.brown@simplyrfid.com](mailto:carl.brown@simplyrfid.com)

## AN EXTRA SET OF EYES

The Modular Flex Series Under Vehicle Surveillance System  
Shows Every Detail of a Vehicle's Underside —  
Day or Night



- Built-in License Plate Recognition
- Easy 30-Minute Installation
- Simple Network Integration
- 100% Waterproof

- Lifetime Warranty on Camera/LED Housing
- See the complete story at  
[www.comm-port.com](http://www.comm-port.com).



COMM PORT TECHNOLOGIES INC  
981 ROUTE 33, MONROE, NJ 08831, USA  
TEL: 732-738-8780 • FAX: 732-631-0121  
E-MAIL: [INFO@COMM-PORT.COM](mailto:INFO@COMM-PORT.COM)

## CommPort