RFID: Airport Greeters and Amber Alerts

RFID is seeping into the information landscape—an "Internet of Things" is slowly forming. Notwithstanding the weight of the Wal-Mart and DOD mandates, it will be no tidal wave; those 800 pound gorillas and their competition can force aggregate RFID tagging, but can't as easily mandate item-level tagging (for items below the scale of a microwave oven or an M-16), and probably won't care to.

But it will be increasingly likely that when one looks for RFID, one will be able to find it. A range of portable, personal objects are RFID-based, including contactless payment devices, building access badges, and inventory management and anti-theft tags in everything from PCs to library books. And while many of the applications it's being deployed for are "closed loop," passive RFID in particular is horribly promiscuous: readers can interrogate any tag in their particular RF band, and every tag in range does its best to respond.

And that makes 3rd-party collection of RFID data interesting. All of those ostensibly private applications will be visible, to some degree, to 3rd-party observation. Any given RFID reader will see both the RFID tags it was deployed to detect, and others it wasn't originally intended to find.

An "airport greeter" analogy might best describe this situation: the individual standing by the concourse exit, holding the hand-lettered sign, is watching and waiting for some other specific individual—and while they wait, can monitor everyone else who walks past. Humans aren't particularly effective monitors, with a limited short-term memory; machines are vastly better.

The so-called "Amber alert"—notifying highway drivers to missing children via roadway signs—is another approach to applying surveillance. It floods a community of sensors with a watch list, providing a small amount of information on what to look for. (Those of us over a certain age remember the Amber Alert's earlier incarnation, as the "milk carton alert," with missing children's photographs printed on the side of the half gallon we stared at over breakfast. A roadside electronic sign can be updated in seconds, however, and the stock of milk cartons deployed to grocery stores, 'fridges, and, ultimately, the breakfast table, cannot.)

The two approaches differ somewhat in their demands: the greeter model can employ a "dumb" sensor, but is hard on the network, while the Amber alert requires that sensors be able to specifically identify a target, i.e., have enough "smarts" locally—if only a set of specific tag IDs—to know what's important when they see it.

One wrinkle in the use of RFID for surveillance is the significance of legacy standards. While the EPC standards are only recently formed, they necessarily embed the

previous generation of product codes—manufacturers will base their EPC assignments on the existing UPC bar codes, making the evolution toward RFID more seamless and simple. So noting the appearance of an EPC tag can actually tell you a fair amount, e.g., the manufacturer, and the type of product. Types of products, in turn, suggest the nature of the person wearing or bearing the items: most kids won't have contactless payment devices; most people associated with petite women's dresses will be (no surprise) petite women. (Not all RFID one encounters will be EPC formats, of course, and their future pervasiveness will depend on the degree to which item-level RFID tagging makes sense in commerce.)

Readers, being machines, can also happily multitask, and across an enormous range of applications, without the cognitive dissonance that might make a human seize up. The same reader that's monitoring store stock against employee theft can also note how many and what forms of contactless payment devices pass by, perhaps to advise management as to whether or not to deploy new registers, or, making inferences from EPC tags seen, attempt to characterize the customers for the marketing department. (Arguably, this isn't any less strange than inviting you to read up on the FBI's ten most wanted, while you wait to pay for postage stamps!)

The willingness of various RFID-using parties to collaborate and share will determine how quickly and extensively such surveillance-related applications will be possible. It isn't hard to imagine all readers across a given enterprise being used as a grand, collaborative surveillance network. It's a little less likely that this would occur between multiple parties at a shared facility, e.g., in an airport or a mall. And the more collaboration is required, the more the parties may choose to suppress some information.

At the far extreme, one might imagine the extensive internetting of many organizations' sensors, e.g., across the whole of a given economic sector. Banks, say, might collaborate in a shared situational awareness network.[1] This is far more likely to be how national-level surveillance networks are created: bottom-up integration, and not any kind of top-down architecting.

Once tags and readers are sufficiently pervasive, applications will suggest themselves. For example, one could create something along the lines of an RFID-based "Lojack" system: if a given tagged item is lost or stolen, push its ID to the network of readers, as an all-points bulletin… "Look out for X, please!" (an RFID version of the Amber alert).

One man's boon is another's bane, of course; one could as easily ask the network to be alert to tags known to be associated with a given individual, with neither his knowledge nor permission. Sensitivity to privacy may govern the acceptability of any given application.

[1] "Privacy Invasion as ROI," AIM Global guest editorial, http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=427&zoneid=24

Such potential futures ought to guide our planning for RFID technologies and policies. At a minimum, they advise caution to those envisioning broad post-purchase use of RFID tags. Strategies for decoupling tag values from individual identities may be a solution to privacy problems, but may be hard to implement (e.g., reprogramming a tag, which takes time and effort), and would break many of the applications being discussed. And because deployment will be dominated by the primary interest of improving the manufacturer-to-retailer supply chain, before objects even encounter end consumers, we shouldn't expect consumer interests to receive as much attention as the cost of tags, or the effectiveness of readers scanning pallets.

Stapleton-Gray & Associates is a Berkeley, California-based technology and policy consultancy, focused on issues of security and privacy, including those surrounding RFID and mobile devices. http://www.stapleton-gray.com

Copyright © 2005, Stapleton-Gray & Associates, Inc.