

Much Smoke, No Fire: The RFID Debate

James A. Lewis

November 2006

If the Americans of the 19th century behaved as many Americans do today, we would still be a nation of farmers, living somewhat like the Amish with their reliance on horses and hand power. This is because an exaggerated aversion to risk shapes discussion (from missile defense to free trade) in ways that the more confident America of the past could not have imagined. New technologies in particular excite this aversion, and Radio Frequency Identification (RFID) leads the pack when it comes to exaggerated concern.

There is no plausible scenario where RFID poses a threat to privacy. The most extreme fears expressed about RFID seem to be based on films like *Minority Report*, in which an omnipresent state tracks its citizens' every move. Governments and giant corporations, we are asked to believe, will implant RFID chips into underwear and soup cans, allowing them to invade privacy at will and amass vast amounts of data on individual behavior.

The problem with this scenario and others like it is that they do not make any sense technologically or commercially. A brief review of the technology shows why risk is miniscule. RFID technology involves a tiny radio device that can be attached to an item, person, or animal. The device emits a radio signal that contains a small amount of data – a serial number or other unique identifier and perhaps a few other details. The small tags envisioned for commercial use in particular have very limited capabilities.

RFID comes in two varieties: passive, unpowered tags, where the tag only emits its data-carrying signal when it is queried by another radio; and active tags, where the tag carries its own power supply. Active tags are more expensive, but their signal can be read at a greater distance than passive tag signals. Passive tags are cheaper, smaller, and more attractive for most commercial uses, but they can only be read from a short distance. Soup cans and underwear may some day carry passive tags, but a giant corporation would need to get within a few feet of you to read the tag.

Besides the unique identifier number, tags can also contain a small amount of information such as date, color, or size. Most tags are not reprogrammable, meaning that there is a fixed amount of information written on the tag that cannot be changed. More expensive tags can allow for information stored on the chip to be re-written, but the cost is prohibitive for most consumer-level uses. This means a tag on an item does not say “This item belongs to [purchaser’s name],” it says “This is tag 63736 00885.” An individual could be identified only if there is some way to link him or her to that specific tag. This link between consumer and tag occurs at the cash register, when the store scans both the tag and a credit card. The retailer will have this transaction data that associates an RFID-carrying item with the person who purchased it, and unless they share it, there is no way for others to know which person is carrying which tag.

This means that RFID tags, whether active or passive, by themselves pose no real threat to privacy. Only when an RFID tag is combined with the right data base can there any risk, and even then, that risk is miniscule. Linking the tag with data requires a “reader.” The tag reader is another small radio device. Readers for passive tags emit a radio signal and the passive tag responds with its pre-programmed message. If the reader is connected to a

computer network, it can then allow this signal from the tag to be linked to identifying data. Without that link, the information provided by most tags will be “This is tag 63736 00885.” Since the merchandiser already has the information on what you have purchased, the only benefit from tracking RFID tags comes from gaining additional knowledge about the location of the item after it leaves the store.

But to gain this locational knowledge, given the short range of a tag’s transmission, there would have to be thousands of readers scattered about a city. Some scenarios envision the surreptitious planting of readers around a city to allow RFID tags (and the persons wearing them) to be tracked. Other scenarios imagine criminals and terrorists acquiring readers, having also obtained the software and databases needed to make sense of a tag’s signal, and using them to identify potential victims. Concerns that the new e-Passport would contain an RFID-like tag and emit signals that terrorists could use to identify Americans exemplify this exaggerated fear of rogue readers. Note to U.S. citizens: terrorists need not bother to obtain RFID readers to identify you as American as you stroll through foreign airports. Your clothing and behavior will be enough.

RF technology can also be used for contactless cards – a plastic card with an embedded chip (companies that sell these cards do not like to be associated with RFID, because of its negative connotations). Contactless cards are a type of passive RF device where the card responds to a reader to transmit data – the most common applications are credit cards or transit fare cards. Instead of being swiped, the card is waved in the reader’s vicinity; the card must be no more than a few inches away to work. At first, there were fears that a contactless card’s signal, if transmitted “in the clear,” could be captured and recorded by a criminal and then replayed to make fraudulent charges. However, contactless cards are usually more secure than an RFID tag, as they are more capable of being secured. Newer contactless cards use a variety of security techniques to defeat capture and re-use, including mutual authentication by the card and reader; unique, diversified session keys that change with each charge (foiling the simple record-and-replay scenario); and the use of encrypted signals.

Contactless card build on the experience of E-ZPass and similar systems, when an RF device mounted on a car can pay tolls automatically by driving past a reader without the car having to stop. E-Zpass and its kindred toll-payment systems present an anomaly for privacy advocates. Millions of Americans use these systems. The systems track their movements, and data from the toll-paying systems have been used as evidence in court cases. Yet there is no surge of outrage nor are people abandoning contactless toll payments. Americans seem willing to trade a little privacy for the ability to go through turnstiles and tollbooths a bit faster. In retail settings, consumers seem willing to accept RFID tags when they are provided with adequate information on how the tags worked, what data was being created and collected, and how that data would be used.

The crucial element here is transparency and knowledge about RFID use. Consumers in the U.S. and elsewhere react with displeasure when they discover that RFID is being used without their knowledge. Their displeasure is amplified if they find that RFID use is combined with surreptitious market research activities (such as using in-store cameras to remotely monitor consumers as they select an RFID-tagged item – an ill-conceived and short-lived experiment by one large company). These consumer reactions suggest that if there is a problem with RFID, it involves the surreptitious collection of data for unknown purposes.

The RFID debate thus rests on two misconceptions. The first misconception is that RFID is a source of unique new information and therefore a new source of risk to privacy. The second is that adopting rules that restrict RFID use will somehow protect privacy. The real issue is how companies and governments collect and use information on consumers and citizens, but this concern has little to do with radio technologies.

Does RFID provide unique data not readily available from other sources? Not really. Stores already know what you buy (unless you use only cash). The new knowledge that RFID could generate is about location – where a tagged item is going. Marketeers like this kind of data because it allows them to refine their advertising, but collecting this locational data from public spaces would be expensive and difficult. In theory, a company could place readers around a city that would allow it to continue to receive signals from an RFID tag embedded in clothing or other items. For this to work, a company would have to emplace many readers in public spaces, on buildings or light poles; the tag would have to pass in close proximity to the reader; and the data collected by the reader would have to be transferred to the company's network. A battery-powered reader could be placed on a door frame or telephone pole, for example, to read RFID tags when you walked by. A company could have mobile readers hidden in trucks or cars and, if the truck or car could get close enough to the tag (assuming that consumers did not notice a vehicle creeping closely behind them), it could read the RFID tag, collect the data, and relay it to some central point to allow identification of the individual.

This scenario is fascinating, but improbable. By itself, the RFID tag identifies an item, not the individual wearing or using it. A company could obtain the RFID signal from an item you are wearing and then match it to purchase records - if it had access to those records. It could assume that in many cases, but not all, that the person wearing or using an item was the same person who purchased it. This sort of collection is possible, but is costly and imprecise. The readers would be in public spaces, subject to theft, vandalism (bands of privacy advocates would surely undertake this as a sacred mission), and possibly to charges of trespassing. There are alternative technologies (wireless communications and, someday, facial recognition) that are more reliable for obtaining locational data. The costs and technical difficulty of using RFID tags on consumer items to track individuals are prohibitively high.

RFID chips can, of course, be implanted in people or animals. In a famous case, a bar gave customers the option of having a chip that was a bit larger than a grain of rice implanted in their arms, so that they could purchase drinks without having to carry cards or cash. In another case, a Florida family had chips containing their medical histories implanted in their bodies. However, in neither case did these implants allow the individuals to be tracked. Many pets now have a chip implanted in them with an identifying number, but this chip will not help you find a missing pet when it is lost. If an RFID chip is implanted beneath the skin (subdermally) of a person's arm, that person would need to get within a foot or less of a reader for the chip to be detected. Some news stories expressed concern that subdermal chips could even contain GPS devices to allow for tracking. This would be true only if two AA batteries needed to power such a device were injected at the same time as the chip. In any case, existing laws criminalize the injection of items into people without their consent.

This means that the various RFID rules and guidelines rolled out by the private sector or considered by government agencies or state legislatures are largely irrelevant. They do not address the real problem. Since data created by RFID is available from other sources (usually with more detail and at lower cost), restrictions on RFID do nothing to protect privacy. A

focus on RFID confuses symptom with cause. The real issue is the patchy safeguards the U.S. now has for the collection, aggregation, and use of personal data.

U.S. privacy protections for personal data can charitably be described as erratic. Existing privacy laws and policies create significant ambiguities for data collection and use. Technological changes in methods of data collection and analysis are not adequately reflected in current policies. Many people distrust the ability of both governments and businesses to safeguard personal information and not misuse it (and every data breach only reinforces this). The ambivalence in the private sector towards privacy complicates this – companies want to reassure customers that their privacy is safeguarded, but they also want to collect and use data from transactions with those customers. Whether the distrust is justified or not, the issue driving public concern over RFID is a lack of confidence in the patchwork approach taken to privacy by the United States at a time when personal information is becoming easier to obtain and use.

This erratic protection is the problem, not RFID. If the right privacy protections were in place (such as rules for what data is public and what data is private, which party owns data created by a transaction, and what their rights are for the further use of this data), this aggregation of personal information would only be beneficial. We do not have these rules in any meaningful sense, and thus technologies like RFID appear frightening. The misconceptions about RFID suggest that the debate is really a way for Americans to deal with their anxiety over the larger erosion of privacy and our apparent inability to do much about it. Psychologists call this sort of thing “displacement,” a mechanism for dealing with anxiety. Displacement is not a good guide for policy

When the first automobiles began to appear on the road, some states required a man with a warning flag to walk before them, to avoid frightening horses and children. If we had kept warning flags for cars, the country would be poorer for it. The same is true for RFID. We have entered a period where information is widely available and easily stored, processed, and communicated. Our laws have not kept pace with these changes. RFID legislation addresses a symptom. The issues we need to consider are how giant databases are created and used and how the mobile, networked IT environment that is developing around us challenges our old concepts of what is public and what is private. Restrictions on RFID would not be without effect, however. The technology offers increased efficiency and safety. Its use could make the American economy more competitive. If we mismanage the debate over RFID and allow misplaced fears to guide policy or slow deployment, these benefits will be lost. This is the only real risk we face with RFID.