

Researchers, standards bodies and RFID technology vendors are all looking at ways to create better security for RFID tags.

Bruce Schneier, a well-known security technologist and author, has been taking aim at RFID in his blog [Schneier on Security](#). On Dec. 12, he pointed out that researchers at the [University of Washington](#) demonstrated that you could track people using a unique ID broadcast by the Nike+iPod Sport Kit, which runners can use to get information on their run (see [Tracking People by their Sneakers](#)).

RFID Journal contacted [Nike](#) a few months ago, and the company denied that the system uses RFID. It refused to elaborate, but clearly the system uses radio waves and there has to be a unique ID, to make sure one runner doesn't get information from another runner's sneakers.

In his blog, Schneier didn't describe the Nike system as RFID, but wrote: "The people who designed the Nike+iPod system put zero thought into security and privacy issues. Unless we enact some sort of broad law requiring companies to add security into these sorts of systems, companies will continue to produce devices that erode our privacy through new technologies."

Then, on Dec. 27, Schneier pointed out that RFID tags used to broadcast the temperature and pressure of tires could be used to track cars because each transponder has a unique ID (see [Tracking Automobiles Through their Tires](#)).

Schneier's point is valid. Companies often adopt new technologies without thinking through all the implications. The question is not whether Nike or [Apple](#) would use the Nike+iPod kit to spy on people, but rather who else might be able to. The kit reportedly transmits its signal 60 feet.

Some might feel that there is little or no danger of people being tracked by these devices or from transponders in cars. But Schneier's point is we don't know what will happen in the future, and it doesn't make sense to have a technology proliferate and then find there is a potential threat to personal privacy.

The problem with his proposal for a law, however, is that it is difficult to legislate against a problem that doesn't exist. Until a technology starts to be adopted, you can't tell what kind of security you need, when you need it or how much you need.

RFID is starting to proliferate and people are raising the security issue—and researchers, standards bodies and technology providers are responding. [EPCglobal](#), the nonprofit organization that is commercializing Electronic Product Code technology, has a subgroup looking at whether additional security is needed for certain applications.

The problem, of course, is that security comes with a cost. EPC tags were first designed for use on cases and pallets in the supply chain, so it didn't make much sense to put a lot of security on them. Making tags really secure would require more sophisticated chips in the tags, which would make the

tags more expensive. That cost eats into a company's profits.

Now that companies are looking at such RFID applications as drug authentication and anti-counterfeiting, EPCglobal and researchers at the [Auto-ID Labs](#) are reexamining the issue. The Auto-ID Lab at The University of Adelaide is developing novel encryption mechanisms based on the concept of lightweight cryptography to ensure only authorized interrogators read a tag. That would prevent people from skimming data off a tag without someone's knowledge.

RFID vendors are also addressing the issue. In November, *RFID Journal* reported that [Texas Instruments](#) (TI) worked with [Certicom](#), a Mississauga, Ontario, provider of wireless-information security solutions, to develop a new security platform application for companies using passive, high-frequency ISO 15693 RFID tags to track and trace products in the retail supply chain (see [Certicom and TI Announce Data Security for HF Tags](#)).

The system utilizes public-key elliptic-curve cryptography (ECC) to encrypt a drug's National Drug Code (NDC) written to a tag. Supply-chain partners can read the encrypted tags as they receive tagged goods, allowing them to authenticate that the goods are genuine product made by the manufacturer, not counterfeit. With the right software, the partners can then decrypt the encrypted part of the tag data if they need to.

There is no magic bullet to solve the security and privacy issues. There will be different solutions based on different needs for different applications. It's highly unlikely that legislators would be able to craft a law that would protect consumers and still allow consumers and businesses to benefit from RFID. Security will evolve over time, as the need arises. It's fine for Schneier to point out the need for greater security in RFID systems, but I think he's off base in calling for a legal remedy.