RFID Policy: What Does Congress Need to Know?

Answer: RFID Raises Major Privacy, Security and Accountability Issues

Electronic Frontier Foundation (EFF) http://www.eff.org
Lee Tien, Senior Staff Attorney, 415-436-9333 x 102 tien@eff.org

Imagine a world where your every possession could be precisely and invisibly tracked. In this world, your purchases, movements, and activities could be monitored in real time or recorded for posterity by marketers or the government, all without your knowledge or consent. This is the world that RFID technology could bring if RFID tags and sensors become common.

Radio-frequency identification (RFID) "tags" are small wireless devices that emit unique identifiers when interrogated by RFID readers or sensors. Today, both government and the private sector are using and promoting the use of RFID tags for many applications, from consumer items to government ID cards. EFF believes, however, that society is moving too quickly to adopt RFID technology. Used improperly, RFID can jeopardize privacy, reduce or eliminate anonymity, and threaten civil liberties.

Three technical aspects of today's RFID tags create privacy problems. First, they're *promiscuous*: they'll talk to any compatible reader. Second, they're *remotely readable*: they can be read at a distance through materials like cardboard, cloth, and plastic. Third, they're *stealthy*: not only are the tags inconspicuous, you don't know when they're transmitting information – or to whom. In short, the personal information and unique ID numbers on RFID tags can be "sniffed" by unauthorized parties. Unfortunately, the typical commercial RFID tag can't implement basic cryptographic protections. That's why Sen. Patrick Leahy warned that RFID may herald an age of "micro monitoring."[1]

RFID includes sophisticated devices with cryptographic functionality that *can* support privacy and security precautions. But whether such protections are used is another matter. Case in point: the U.S. government's proposed "contactless" e-passport has built-in encryption, but the State Department thus far has chosen *not* to use encryption to prevent exposure of citizens' personal information. Also, it cannot be assumed that cryptographic precautions (if used) are properly implemented, as shown by Johns Hopkins University's recent discovery of a security weakness in the RFID device used in the Exxon/Mobil SpeedPass payment card and many automobile anti-theft systems.[2] Part of the security problem is that RFID tags often are used in *mass* applications; thus, the devices will be easily available for reverse-engineering, while lack of security could result in widespread harm.

As the preceding comment suggests, RFID also poses public accountability problems. Yet government entities large and small are now making decisions to "tag" people with little or no public input. Only last month did the State Department issue a Federal Register notice about its "RFID passport" plans, despite months of public criticism from civil-liberties groups. And one school district in California had planned to use RFID in student ID badges with little parental input before local parents supported by the ACLU and EFF publicized and ultimately halted the program.

Without good security, every RFID tag creates "privacy pollution" by exposing personal information or a unique ID number to snoops. Congress must act to rein in unnecessary or careless government RFID implementations, and promote public debate over alternatives to RFID.

---

[1] Remarks of Senator Patrick Leahy, "The Dawn of Micro Monitoring: Its Promise and Its Challenges to Privacy and Security," Conference on Video Surveillance: Legal and Technological Challenges, Georgetown University Law Center, Mar. 23, 2004, <http://leahy.senate.gov/press/200403/032304.html>.

[2] http://rfidanalysis.org