

# RFID Legal Education Should be Job One, Say Policy Experts

Organizations need to be proactive in shaping regulations, standards and public policies that will impact how RFID is deployed, say speakers at a seminar on the technology's legal ramifications.

By Mary Catherine O'Connor

Sept. 27, 2006—Speakers at Tuesday's [RFID Legal Seminar](#), a half-day kick-off to *RFID Journal's* first [Industry Summits](#) conference near Chicago, ran the gamut from think-tank libertarians, lobbyists and congressional staffers to manufacturers' public-policy officers. Still, each shared a common message: Makers and users of RFID technology will fail unless they get proactive about how regulatory and public-policy actions will shape—or limit—the use of RFID.

"If you're a project manager or engineer deploying an RFID system, you should be in contact with your public-policy staff," said Sandra Hughes, [Procter & Gamble's](#) chief privacy officer, who is responsible for ensuring that P&G and other users of EPC technology follow [EPCglobal's](#) guidelines for using EPC on consumer products. These guidelines mandate the use of an EPCglobal logo on all packaging containing RFID inlays, and that consumers be given choices in removing or disabling RFID tags from products they obtain. She also said companies using RFID technology—whether as RFID vendors or end users—need to understand the public conceptions and misconceptions about RFID and how it is used. "Even though there is not any consumer information encoded to EPC tags, the public perception is that there is," she said.

The purpose of the seminar was to provide insights into the data-security, intellectual-property, regulatory and personal-privacy implications of RFID technology's proliferation in both government and commercial applications.

Douglas Farry, a managing director of the law firm [McKenna Long & Aldridge](#) and a primary contributor to the firm's [RFID Law Blog](#), echoed this sentiment. "Technologists are often so enamored with technology that they lose sight of how it will be received by its users," he said. "Think about how policy makers will react to the RFID systems you create; don't just think about the ROI."

Jim Harper, director of information-policy studies for the [Cato Institute](#) and a member of the [Department of Homeland Security's](#) Data Privacy and Integrity Advisory Group—which earlier this year released a report saying RFID does not offer benefits to identification management that are strong enough to justify the privacy risks associated with its deployment (see [DHS Subcommittee Advises Against RFID](#))—said he believes that while RFID holds great promise to automated information gathering, some of its proposed applications are troubling. "There will be great things that will happen with RFID, but only if the government doesn't use it to track people," he said.

Not all presenters expressed the same concerns about how RFID may or may not be used, but all agreed that it's important for vendors and users of RFID to fight the widespread misinformation and ignorance that exists regarding the technology's capabilities and limitations. A group of U.S. senators recently established a forum

to help educate legislators about RFID (see [U.S. Senators Initiate RFID Caucus](#)). More than 20 states have introduced RFID-related bills (13 of which have been adopted into law). And yet, according to more than one of the speakers, virtually no one on Capitol Hill knows about RFID. Jason Roe, chief of staff for [Congressman Tom Feeney of Florida](#), who chairs Congress' intellectual-property caucus, said that after calling 10 congressmen at random, he found not one who knew what "RFID" stands for.

Educating legislators on RFID, Roe said, should be a top priority, and the concerns over how the use of RFID may impact the public privacy should be nonpartisan. "Privacy concerns unite left and right," he said, recommending that attendees begin reaching out their hometown members of Congress.

David Golden, director of commercial lines for the [Property Casualty Insurers Association of America](#) (an insurer trade association), spoke about how the emergence of RFID technology will make companies more directly liable for things such as product recalls, while enabling them to prove ownership of insured goods—such as large equipment—that could be lost in a disaster.

Golden noted that RFID could also pose problems to some companies if it is mandated in a way that does not offer them liability protections. For an example, he pointed to the [National Highway Traffic Safety Administration](#)'s requirement that carmakers add airbags to cars, and carmakers' subsequent legal woes when the bags proved harmful to children.

The importance of standards development and information sharing was also emphasized during the seminar. Tom Karygiannis, senior scientist with the [National Institute of Standards and Technology](#) (NIST), noted that the organization's Computer Security Division has just released a draft guidance document for deploying a secure RFID network (see [NIST Releases RFID Security Recommendations](#)). Karygiannis asked attendees to read the draft and make suggestions, so that NIST can provide the most timely and accurate information possible about the most current best practices, as well as tools to keep data linked to RFID systems secure.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved