

RFID Vendors Need a Privacy Strategy

To succeed, companies providing RFID solutions must work closely with their customers to develop a strategy for ensuring privacy and security compliance.

June 19, 2006—News reports continue to raise fears that RFID will be used to monitor consumers' personal lives. These reports demonstrate firsthand that RFID solutions providers that do not account for privacy and security concerns in their product development, marketing and sales cycles will be at a substantial disadvantage to those providers that do. A report published in the June 2006 issue of *Consumer Reports* (see [Consumer Reports Looks at RFID](#)) strongly implies the industry has decided to keep its head in the sand and hope privacy and security concerns will subside. Even though the implication is false, the likelihood of privacy and security concerns dissipating is slim.

Given how the press has followed the [National Security Agency's](#) alleged monitoring of phone calls made in the United States, it is much more likely that privacy and security concerns raised by RFID will continue to swell. In fact, a recent poll found 70 percent of Americans to be "worried about the invasion of privacy through new technology." This percentage was the highest among all countries surveyed, according to a poll taken by [Roy Morgan International](#) (see [Five Countries Review Privacy, Technology](#)).

RFID solutions providers that work closely with their customers to develop a strategy for ensuring privacy and security compliance will be rewarded. Those that can demonstrate a deep understanding and appreciation of the concerns raised by applications including personally identifiable information (PII) will be more likely to gain customers' trust and close more substantial deals than those that only offer lip service to those concerns. How can RFID technology vendors use the issues of privacy and security affirmatively to give themselves a competitive advantage?

Develop a Compliance Strategy

RFID solutions providers should develop an appropriate program for managing their customer relationships from a privacy and security standpoint. It should be no surprise that the marketing credo of "know the customer" applies with equal force to RFID privacy and security issues. Solutions providers need to understand how and why their customers use PII, what they do with it and with whom they share it.

RFID solutions providers will find that many of their end-user customers outsource data management tasks, including those that involve PII. While the majority of domestic and international privacy laws permit outsourcing, the outsourcing of business operations involving PII introduces added risk (legal, political and reputational). These risks are made real by widespread publicity about security breaches and enforcement actions from regulators aimed at companies suffering such breaches. The emerging standard for addressing these issues from a legal perspective is to require additional oversight of end-user customers—at the front-end, due-diligence stage and at the back-end, through both comprehensive audits and spot-check assessments. Most end-user customers recognize this to be a serious and daunting challenge, one that must be taken seriously to avoid harming their business reputation.

Learn From Mistakes

Businesses also need to follow up on mistakes. From both an enforcement standpoint and a risk-management

perspective, end-user customers need to be apprised of areas where mistakes or complaints have been made—and they must make sure a plan is in place to modify behavior to address problems promptly. RFID solutions providers can also demonstrate that they learn from others' mistakes by monitoring the external privacy and security marketplace. Did a potential customer suffer a security breach? Were Social Security numbers disclosed in a situation where their use was not necessary? What precautions can be taken in order to limit the occurrence of similar problems?

It should be no surprise that the surest path to strict enforcement action and severe penalties is to know of a problem but take no responsive action (or to be the second company facing a particular problem that has an easy fix).

RFID solutions providers must be aware of these problems and demonstrate agility in addressing them. These providers also would be well served to suggest a security-breach notification plan that its end-user customers should adopt. Two important elements of such a plan (which should be in place before a breach occurs) are a mitigation procedure, and a speedy and reliable means to determine whether notification should be carried out—and, if so, how.

Monitor Privacy Laws

RFID solutions providers need to keep apprised of the scope of the privacy and security laws that can affect their business. The current patchwork of statutes and regulations prescribe varying rules on the privacy of credit reports, medical data, phone records and video store rentals, to name a few. Government agencies and other end-user customers are now including privacy and security requirements in their business contracts. Moreover, the breadth and depth of topics covered—from financial records to health care to employee privacy—is expanding. Thus, RFID solutions providers looking to do business with customers subject to specific laws (such as those in the financial and medical fields) will need to adjust their privacy and security practices accordingly. Customer-specific plans may be necessary.

Privacy legislation is still a hot topic for both state and federal legislators. In certain instances, RFID solutions providers may want to influence pending legislation that could impact their business.

Given the current legal landscape, RFID providers should maintain their privacy and security compliance strategy as a "living document" that is updated in accordance with new laws and lessons learned. Such a strategy will be critical to landing that all-important first customer sale. In addition, savvy RFID providers will use timely updates to their compliance strategy as a means of maintaining ongoing contact with customers, realizing that such contacts often lead to follow-up sales. An effective compliance strategy is one that balances legal requirements with successful business approaches.

Kirk J. Nahra and John W. Kuzin are attorneys at Wiley Rein & Fielding, in Washington, D.C. Nahra is a partner and chair of the firm's privacy practice; Kuzin is a communications and privacy attorney who specializes in RFID technology.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved