

RFID-Enabled IDs: Educate, Don't Legislate

Whenever we're faced with an emerging, unproven technology such as RFID-enabled identification documents, there is a premature urge to create laws restricting or stopping it.

Aug. 28, 2006—This year, we have seen considerable controversy over government identity programs such as the U.K.'s Home Office Identity Cards Scheme and the U.S.'s Western Hemisphere Travel Initiative (WHTI) and Real ID Act, as well as bills that legislate against the use of RFID such as those proposed recently in California regarding driver's licenses and student IDs.

These efforts have garnered the spotlight from all angles, including both religious and privacy activists. RFID technology and the Real ID Act for example, have been likened to the "Mark of the Beast" foretold in the Bible. Privacy advocates have voiced opposition on a number of levels, including Big Brother concerns, skimming and tracking fears and, in particular, apprehensions about the viability of the technologies that are at the heart of these programs—everything from RFID to smart cards and biometrics.

While these technologies have been around for a long time, their use in the field of human identification is relatively new—at least, on the broad scale now underway. Starting in 2008, the U.K. Identity Cards Scheme will force everyone over the age of 16 applying for a passport to have their personal biometric details—including fingerprints, eye or facial scans—added to a national identity register. For this reason, we can consider them emerging technologies since their field of use, or scale of use, is still maturing.

Throughout history, emerging technologies have faced the same level of scrutiny, and often mistrust, until they became familiar, better understood and eventually accepted by the masses. This is the basic technology-adoption lifecycle. An example from the industrial age is the locomotive engine. At that time, it was thought that traveling in excess of 30 miles per hour on one of these new locomotives would subject the human body to so much pressure that an individual would not be able to breathe. A more extreme example of technology mistrust involves the Luddites of the early 1800s, who smashed textile machines in various U.K. counties fearing the machines would make their skills obsolete.

The World Wide Web and wireless technologies are more recent examples of emerging technologies that initially met considerable hurdles but went on to benefit society. Identity technologies face many of the same privacy and security concerns that the World Wide Web and wireless technologies faced early on—and still face today. It goes without saying that such concerns are valid and must always be addressed. Fortunately, the market solves many of these problems by way of companies developing solutions specifically to help close the gaps and loopholes.

In general, whenever we face an emerging technology that is relatively unknown and unproven, there is a tendency to legislate against it, or to attempt to mandate certain better-known approaches. While a healthy debate about privacy concerns is critical to the success of these large-scale programs—and any program that deals with consumer-sensitive information—it is important not to over-legislate against the use of technology before its strengths and weaknesses for a particular field of use are well understood.

The Home Office Identity Cards Scheme, the Western Hemisphere Travel Initiative and the California bills

are interesting, and ongoing, case studies of where the center of the debate—or even legislation, in the case of the California bills—can sometimes work counter to the best interests of consumers and government alike.

Legislation against a particular technology from use in certain application scenarios can limit technology innovation within the government, and benefits to citizens.

The two bills approved by the California Assembly Judiciary Committee, SB 433 and SB 1078, would put a three-year moratorium on the use of RFID technology for driver's licenses and student ID cards, respectively (see New RFID Bills Moving Through Calif. Assembly). These kinds of moratoriums, if adopted, would prevent the use of the technology before its relative pros and cons for use in these applications have been fully explored. If instituted on the national level, such moratoriums also would provide other countries with the time to innovate and explore these applications and potentially move ahead in their level of competitive advantage. Rather than ban the technology, which does little more than put the problem on ice for a given time period, we need to work with all parties concerned toward understanding the issues involved and solving them. (To its credit, the California Assembly removed such a moratorium from another bill, SB 768: See Calif. RFID Bill Drops Moratorium, Could Pass Senate.)

Prescriptive technology mandates can limit innovation and the competitive process.

On the flip side to the California bills, if legislation becomes too prescriptive in terms of the technology it recommends for a particular application (as opposed to barring a particular technology completely), it can also limit innovation and stifle competition.

The Western Hemisphere Travel Initiative was established by the Intelligence Reform and Terrorism Prevention Act of 2004 to require better documentation for individuals traveling across U.S. borders. Individuals will be required to present a passport or a frequent-traveler card known as PASS (People Access Security Service). Over time, there has been an ongoing debate between the Department of Homeland Security (DHS) and the State Department regarding what type of technology to use—some favor ISO RFID standards such as 14443 (the proximity card standard), while others prefer EPCglobal UHF RFID standards. Each has its pros and cons.

An amendment to the DHS Appropriations Bill requires that "the card architecture meets the ISO 14443 security standards, or justifies a deviation from such standard." While this standard may or may not be the most appropriate solution, it effectively precludes other technologies such as UHF RFID and anything else from consideration. According to the Information Technology Association of America (ITAA), which has been actively engaged on Capitol Hill in representing the broad interests of the U.S. IT community, this amendment unfairly limits competition and excludes a certain segment of the technology sector.

Additionally, 14443 is an interoperability standard, as opposed to a security standard. While the intent may have been to mandate strong security in the procured solution, the wording has the potential to exclude RF technologies other than those operating at 13.56 MHz. A more rational approach might be to prescribe system-wide business requirements and permit the market to compete more openly with a variety of envisioned solutions—both new and old.

Policies and procedures, in addition to the technology, drive the resulting level of privacy and security achieved.

In debates over privacy and security, it is typically the front-end technology that is the object of scrutiny. A recent U.K. House of Commons report from the Science and Technology Committee focused on how scientific advice, risk and evidence were managed in relation to continually developing technologies. The focus of the report was the U.K. Home Office's Identity Card Scheme. A finding of the report was that while

much attention had been paid to the biometric technologies to be incorporated into the planned system, there was a lack of transparency around the information and communication technology (ICT) back end.

To maximize the success of these types of large-scale programs, it is important to focus on the entire system, end-to-end, and also on the policies and procedures surrounding its operation and use. This holistic focus can actually improve the privacy and security of the system by helping to ensure that major procedural or technical vulnerabilities are not overlooked.

Consumer and policy-maker education is vital.

Given that legislation and debates often gravitate to controversial areas in the identity discussion and omit critical areas that must not be left out, ongoing consumer and policy-maker education is vital for the best interests of all parties. Finding the good and bad aspects of these systems is equally important, but it is also important to get the facts, scrutinize all claims and assertions, and realize that conflicting information may be accidentally or deliberately omitted.

For example, a recent e-passport demonstration showed how an RFID passport could be skimmed and cloned. While it is important to get the issue on the table, it is also important to realize the true implications this type of scenario has for consumers. According to the [Smartcard Alliance](#), this cloning was equivalent to simply taking someone else's passport and attempting to pass it off as one's own (see [Industry Group Says E-Passport Clone Poses Little Risk](#)). In fact, the e-passport is likely more secure since a digital biometric photo cannot be altered in this cloning scenario, whereas a non-RFID passport could have its printed photo readily substituted.

Another recent report, "The Use of RFID for Human Identification," seemed to suggest RFID offers little benefit other than for miners or firefighters "when compared to the consequences it brings for privacy and data integrity" (see [DHS Subcommittee Advises Against RFID](#)). This draft report, written by an advisory group to the U.S. Department of Homeland Security, clearly overlooks applications such as those in health care for patient tracking and medication administration. Patient tracking can be used in an emergency department for customer convenience in much the same way that we use pagers in restaurant queues today. It can help ensure patients are seen by medical staff in a timely manner and receive the level of care they require. Use of RFID for medication administration can help ensure the right patient gets the right medication at the right time, while helping reduce the medical error rate and substantially save lives.

Another example is the use of RFID in theme parks to help track missing children so their parents can quickly locate them. This serves as a valuable safety device to help reduce the stress from accidental separation and can even prevent potential abductions.

Privacy and security are not mutually exclusive.

Policy makers and end users of identity programs often presume that they need to make a choice between privacy and security. That is, they believe they either must take the privacy side and legislate against or refuse to use these systems, or opt for the interests of national security and their own personal security, and give up some of their privacy. In truth, however, this decision does not need to be a binary one: It is possible to create identity programs that offer both security and privacy.

Emerging technologies such as RFID and biometrics can actually help to improve privacy and security by providing stronger forms of authentication and, hence, assertion of an individual's identity. Such technology solutions can help to combat the problem of identity theft by removing the need to rely solely upon weaker forms of authentication such as user names, passwords and PINs. Given the current statistics on levels of identity theft and data loss of consumers' personally identifiable information, it is important not to legislate too fast or fixate on only a small portion of the problem space.

The debate must occur, but it must be well formed and well considered, and the potential benefits given equal consideration.

Nicholas D. Evans is a vice president in the Strategic Program Office at Unisys. He is the author of Business Innovation and Disruptive Technology (Financial Times, Prentice Hall) and chairs the RFID Standards Task Group for the Information Technology Association of America.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved