

I.D. Cards: Security vs. Privacy

Security and privacy interests are clashing again. The United States is becoming unique in the world in that we do not have national identification cards or papers. In the interests of security, the concept of national identification cards has been floated and discussed, but never enacted. The introduction of “smart” identification cards, those with imbedded computer chips, is raising privacy concerns in many quarters and vulnerability concerns in others.

Congress propelled the discussion in 2005 when it passed the Real ID Act of 2005,¹ which sought to standardize state-issued drivers’ licenses with Real ID compliant identification documents in lieu of a national identification card system. The implementation regulations were issued earlier this year² and have been met with protests from many quarters. Implementation of the law has been delayed for two additional years pending further consideration.

Companies, governments, and other organizations have begun issuing a variety of identification cards, key cards, documents, and other devices embedded with microchips. This allows scanning devices to recognize that the individual possessing the card is authorized to enter the establishment. Other cards are embedded with radio frequency identification (RFID) chips, which can be scanned to identify a person entering or leaving a specified area. RFID chips are very common in tracking inventory and goods in transit but have also begun to be used in everything from passports to school identification cards.

A variety of questions arise from the use of these devices. Are the privacy rights of individuals being compromised? Are the devices really secure? Do they offer us real protection?

Privacy and Consent

If my firm decides that each employee should have a pass card with an

embedded RFID chip that would allow a security system to recognize me as the owner of the card and allow me access into the offices, inherent in that decision is that each employee can effectively be tracked by those same systems. In the business context, that seems to be an easier balance. If I do not wish to be tracked by the firm that is giving me a paycheck, I can make a decision to go elsewhere. The issues become more complex if the application is used for students at the local high school. An RFID scan might identify individuals without the proper pass and alert school security that a potential intruder is on campus. However, attendance at school is mandatory for most students. Does the ability to be tracked through the use of an RFID card trample on the rights of privacy?

Recognize that each of these technologies is not completely secure; an insecure technology can put the privacy rights of people at risk. For example, if a determined hacker was able to access personal information from RFID cards as employees, students, or governmental workers stroll by, data residing in the smart cards could be “mined” and used by identity theft rings. Specific individuals could be tracked without their knowledge.

How Good is the Technology?

Sometimes lost in the debate is the need to strike a balance between effectiveness, security, and privacy. An easy, less intrusive system is likely to be less secure. A more secure system, such as biometric scanning, is secure but certainly more intrusive. In each application, businesses, governments, and schools need to determine the purpose for the application of the technology, the level of security desired or needed, and the personal interests of the individuals involved.

What is clear from the research is that any technology can be hacked,

replicated, and used by a determined thief. The new car that allows you to start the vehicle with a push of a button because the car recognizes that the keys are in your pocket offers tremendous convenience. However, the security of the device can be compromised by a determined criminal. If the criminal can replicate the signal, he can drive off with your new car.

Where Do We Go From Here?

Expect a lot of debate and discussion about the use of tracking, identification, and other smart card technologies. Applications for such technologies will be growing. You may have even seen the availability of products to insert identification microchips in your child or pets. In a soon to be published paper, a myriad of concerns are raised by Nicole A. Oser, the technology and civil liberties director at the ACLU of Northern California.³

The balancing of security, privacy, and personal rights will continue. California is again leading the way on privacy rights with the introduction of new legislation regulating RFID tags,⁴ and other states will likely join the debate.

NOTES

1. Public Law No. 109-13

2. 6 CFR Part 37

3. Oser, Nicole A., *Rights Chipped Away: RFID and Identification Documents*, to be published in the *Stanford Technology Law Review*. Link to draft article available at http://aclunc.org/issues/technology/dont_chip_our_rights_away!.shtml

4. California Identity Information Protection Act of 2007, SB30.



Michael S. Khoury, of Jaffe Raitt Heuer & Weiss, PC, Ann Arbor and Southfield, practices in the areas of information technology, electronic commerce, intellectual property, and commercial and corporate law. He is the Chairperson of the State Bar of Michigan Business Law Section and past chairperson of the Computer Law Section. He is also a member of the American Bar Association Sections of Business Law, Science and Technology, and Intellectual Property.