

DHS Subcommittee Advises Against RFID

A draft report from a DHS advisory group argues that the benefits from using RFID-enabled documents to verify an individual's identity are overshadowed by the risks to personal privacy.

By Mary Catherine O'Connor

May 22, 2006—RFID might be a great technology for identifying and tracking goods, but according to a draft report from a subcommittee of the Privacy Office of the U.S. Department of Homeland Security (DHS), it's not a panacea for long lines and forged IDs at border crossings and airports. Furthermore, the report claims, its use could weaken the privacy of individuals whose government-issued identity documents might carry RFID tags. The report urges the DHS to consider "other technologies that may serve the same [identification] goals with less risk to privacy."

The DHS Emerging Applications and Technology Subcommittee of the Data Privacy and Integrity Advisory Committee wrote the 15-page report to guide the department's secretary, Michael Chertoff, acting chief privacy officer Maureen Cooney and DHS program managers in deciding whether to deploy RFID technology within DHS programs to identify or track individuals. The report has not yet been submitted to Cooney, who has the lead role at DHS in analyzing and deciding the legal implications of various programs and their impact on privacy.

The Privacy Office is tasked with ensuring that no DHS programs or policies negatively impact the privacy of U.S. citizens and visitors, based on the Privacy Act of 1974, the Freedom of Information Act and other laws, including Section 222 of the Homeland Security Act. Within the Privacy Office sits the Data Privacy Integrity Advisory Committee, which advises Chertoff and Cooney on a number of matters, including technological issues relevant to the DHS that affect individual privacy.

The Emerging Applications and Technology Subcommittee is made up of D. Reed Freeman, Jr., chief privacy officer at online advertising services company Claria; James Harper, editor of Privacilla.org and director of information policy studies at Washington, D.C.-based think tank, the Cato Institute; Lance Hoffman, professor at George Washington University; Tara Lemmey, CEO at Lens Ventures and former president of the Electronic Frontier Foundation (EFF), a privacy advocacy group; Joseph Leo, vice president at research and engineering firm Science Applications International Corp. (SAIC); John O. Marsh, professor at George Mason University School of Law; and Charles Palmer, group manager of IBM's security, networking and privacy departments. The report, titled "The Use of RFID for Human Identification," will be presented to the full committee at a June 7, 2006, public Advisory Committee meeting in San Francisco.

Some government observers, however, say the report's potential effect may be limited. "The impact of the report is more public relations value against the use of RFID in applications related to tracking individuals, like e-passports or I-94 forms," says Douglas Farry, a managing director of McKenna, Long & Aldridge, a nationwide law firm focused on the intersection of public policy and technology. "There is no statutory or mandatory authority associated with these reports—it's just ammunition for those who might want Congress or the DHS itself to limit or prevent RFID from being used for [tracking individuals]."

"Whether it is RFID or any other kind of automatic identification system, the same privacy and security issues are at stake," he says, noting that they should all be addressed equally. The report's value, he adds, is that it "speaks to the need to have this kind of evaluation *before* large public announcements are made by government agencies that they are rolling out certain programs."

The report notes, however, that it is the use of radio frequencies to transmit data that makes RFID different than other technologies, such as bar codes or contact-based chips. This use of RF, the report maintains, is why the utility and appropriateness of RFID in identity documents should be examined and questioned.

Emerging Applications Subcommittee member James Harper says, "The draft report is already having an impact in that it's forcing a conversation between two parties that have not talked to each other enough: the RFID industry and privacy community." He adds that the "bad press" RFID is receiving—largely due to perceptions that it will become a tool for Big Brother to track citizen's every move—is diminishing the technology's important value in the supply chain and for other applications outside of identity documents. What's more, he maintains, if users of E-ZPass and other RFID-enabled electronic toll-collection systems had to stop and check each transponder to make sure it belonged to the driver using it, that would negate the technology's main benefit. Because identity documents must be checked by an agent and tied to its carrier, the speed in data transfer that RFID enables is thus diminished.

The DHS has already completed tests of RFID-enabled passports and plans to begin issuing them to citizens later this year (see DHS Completes E-Passport Test at SFO). The US-VISIT program is also using RFID in forms it issues to visitors with nonimmigrant visas (see DHS Testing Tags for US-VISIT Program).

The DHS report surveys the various methods by which a human subject's identity can be presented and authenticated by a DHS agency at airports, government buildings, border checkpoints and other locations, and claims that RFID can not improve the speed at which a human subject can be identified. The technology can lead to fast data transfer between the piece of identification and a reader, but without being linked to a biometric proving the identity of the ID-holder, it says, a person can not be reliably identified.

Still, linking the RFID tag to a biometric (such as a photograph or fingerprint of the person being identified) decreases the benefit of speedy data transfer. "In terms of speed, the use of RFID probably represents only a marginal improvement in speed over alternatives such as contact chips, 2-D bar codes and optical character recognition," the report says.

According to the report, the "benefit provided by the use of RFID in identification documents is not a product of its use of radio, but rather the fact that the data is in a digital format. Any data in digital format can be encrypted. Thus, RFID as such offers no anti-forgery or anti-tampering benefit over alternatives such as contact chips, bar codes or pixelization."

Moreover, the report goes on to claim, the use of RF signals to transmit data presents some risks not found in contact-based chips and other technologies. These risks include the interception of data linked to one's identity through skimming (creating an unauthorized connection with an RFID tag to pull data from it) or eavesdropping (intercepting data being exchanged between an RFID tag and an authorized reader). The report, however, does not mention any recorded instances of such privacy invasion occurring.

Finally, the draft report concludes that the use of RFID in identity devices will make people carrying the devices "subject to greater surveillance" than those not carrying RFID-enabled IDs. Individuals, it states, will not know when, outside of presenting an ID to an agent for visual inspection, the devices they hold might be read surreptitiously within a public area.

Based on these security risks, as well as the benefits of using RFID compared with other means of transferring

data from a ID to a back-end data system, the report concludes that the DHS "should consider carefully whether to use RFID to identify and track individuals, given the variety of technologies that may serve the same goals with less risk to privacy and related interests."

Copyright ©2005 RFID Journal, Inc. All Rights Reserved