MERCATUS CENTER
GEORGE MASON UNIVERSITY

REGULATORY STUDIES PROGRAM

Public Interest Comment on
The Use of RFID for Human Identification[1]

May 22, 2006

The Regulatory Studies Program (RSP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of the impact of regulation on society. As part of its mission, RSP conducts careful and independent analyses employing contemporary economic scholarship to assess policy proposals from the perspective of the public interest. Thus, this comment on the Data Privacy and Integrity Advisory Committee's report on the use of RFID for human identification[2] does not represent the views of any particular affected party or special interest group, but is designed to evaluate the effect of the use of RFID on overall consumer welfare.

Radio frequency identification (RFID) systems are a subset of a larger class of technology known as automatic identification (Auto-ID) systems. Other Auto-ID systems include such common technologies as barcodes, magnetic stripe cards, and optical character recognition systems. The purpose of these technologies is to identify and track people, animals, and goods. While a barcode requires line-of-sight scanning, and smart cards require physical contact with a reader, RFID-tagged objects can be identified at a distance because the technology employs radio frequency transmission.

RFID technology has been used effectively to manage inventories of goods and to track objects in supply chains and other logistical undertakings. However, the tracking of humans using RFID, especially by government, presents serious privacy questions. The Committee's report admirably raises these questions and presents solid advice about how to consider RFID for human tracking. The committee's recommendations are applicable not only to the Department of Homeland Security, but also to the entire federal government.

The analysis and conclusions of the Committee's report are sound and correct. As the Committee has noted, the privacy concerns created by using RFID to identify humans generally outweigh any benefit that could be gained. While the threats to privacy

[1] Prepared by Jerry Brito, J.D., Legal Fellow, Mercatus Center at George Mason University. This comment is one in a series of Public Interest Comments from Mercatus Center's Regulatory Studies Program and does not represent an official position of George Mason University.

[2] Data Privacy and Integrity Advisory Committee, Privacy Office, Department of Homeland Security, THE USE OF RFID FOR HUMAN IDENTIFICATION, Draft Report Version 1.0, *available at* http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_advcom_rpt_rfid_draft.pdf.

presented by RFID tracking of consumer goods have been exaggerated, government use of RFID to identify humans does entail serious privacy consequences.[3] Moreover, the costs of employing RFID in a government identification system are also significant.

The surreptitious monitoring of persons cannot easily be accomplished by tracking RFID tags embedded in consumer goods. Among other things, such monitoring must assume that identification of an object is identification of a person, which can never be assured. We generally carry many consumer goods with us, and in an ever-changing combination, so that no one RFID tag can ever be guaranteed always to be on our person. The exception to this rule, however, is when government mandates that we identify ourselves using RFID.

If RFID becomes widespread in government identification documents that citizens must carry with them out of convenience or to comply with the law,[4] then the surreptitious RF surveillance of humans does become a real concern. As the committee noted, even if personally identifiable information encoded in an RFID chip is encrypted, "[t]hough indecipherable itself, the encrypted information can act as an identifier if it remains the same each time the card is skimmed."

Additionally, the cost of including RFID technology in government identification documents would be more expensive relative to other comparable Auto-ID technologies, such as magnetic stripes or barcodes. This is doubly the case if the RFID chips used are properly designed to provide the security assurances the Committee's report rightly recommends. For example, as the Committee notes, RFID-equipped passports issued by the State Department include a special metal cover to prevent access to the chip. This and other safety measures, such as dynamic encryption, will make RFID solutions more expensive.

The benefits of RFID to human identification processes are a perceived increase in the speed of reading documents. However, as the committee has explained, while the speed of document reading may be increased, the speed of identifying a human will not; it still must be ascertained that the bearer of the document is in fact the person identified by it. Therefore, any planned adoption of RFID should measure the marginal increases in speed against the relative higher cost of employing RFID technology.

We commend the Committee for its analysis and conclusions. Hopefully any planning by government to use RFID to identify humans will take into account both its consequences to privacy and anonymity and its greater relative cost.

---

[3] Jerry Brito, *Relax, Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature*, 2004 UCLA J. L. & Tech. 5 (2004).

[4] *See Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, 542 U.S. 177 (2004) (holding that citizens cannot refuse to identify themselves when government agents demand it).