

# European Study Probes RFID's Impact on Privacy

Issued by the European Parliament's Scientific Technology Options Assessment committee, the report finds that the use of RFID to date has not had significant negative impacts on the privacy of individuals, though it does call for transparency.

By Mary Catherine O'Connor

July 11, 2007—The European Parliament's Scientific Technology Options Assessment (STOA) committee, comprised of 15 Parliament members, provides the governmental body with information about new applications and innovations in technology. The committee recently released an 86-page report entitled "RFID and Identity Management in Everyday Life," exploring the perceptions, benefits and concerns surrounding the use of RFID technology among consumer end users in Europe, as well as among vendors and implementers of the technology.

The report was researched and written by members of an independent Dutch organization called the Rathenau Institute. Founded and funded by the Dutch Ministry of Education, Culture and Science, and administered by the Royal Netherlands Academy of Arts and Sciences, this organization carries out research into the development of science and technology.

The Rathenau Institute conducted the study as part of the European Technology Assessment Group (ETAG), which provides the European Parliament—by reporting to the STOA committee—with research regarding the social, environmental and economic aspects of new technological and scientific developments. The body of research used for the report consists of 24 case studies conducted by the institute on a variety of RFID deployments. In addition, it features interviews with RFID technology experts and end users, as well as reviews of existing reports and other documentation.

The study's mission is to provide the European Parliament with insight into how RFID has been used to date, as well as create scenarios for how its uses and capabilities will expand in the coming years, and discuss possible implications on personal privacy and other issues linked to the technology's growth.

Based on the case-study results and interviews, the report concludes that the use of RFID thus far has not had significantly negative impacts on the privacy of people carrying tags on their person in Europe—whether voluntarily, unknowingly or through an employer or government mandate. However, it does make the case that technology could be misused in ways that have negative implications on privacy.

One example the document cites involves an office building in The Hague, where employees are issued RFID cards used to grant access to the main entrances and other sections of the building (not all workers have equal access). The report notes that the access-control system saves a log of the card ID numbers read by the HID 125 kHz readers mounted at secure doorways, and could use this information to track the times at which employees arrive at work. It also indicates that while office administrators do not access this data to track employees' arrival times, employees are not informed that this data is being collected (most think the cards only allow access, anonymously). This creates a scenario in which workers' movements could be tracked without their knowledge.

The report also describes how two employers are using RFID to provide access control, while also tracking employees' work hours and maintaining building security. The personnel are aware of the technology and how the companies are using it, the report adds, and none expressed strong concerns that the technology might infringe on their personal privacy. In fact, a labor union at one of the companies believes the system offers a way to track overtime and ensure workers are accurately compensated for time worked, since the system reads tags as they enter and exit the job sites.

At least one case study describes an RFID deployment in which the authors claim it is hard to determine if personal privacy is being infringed. At a zoo in The Netherlands, visitors are issued green bags to cover up their purses or packages so monkeys roaming freely among the guests can't access the goods inside them (which they've shown a tendency to do). The zoo has decided to attach active RFID tags to some of the bag covers they distribute to visitors, to track traffic patterns in the zoo. Administrators indicate this data can help improve exhibit layout and usage. While the zoo tracks only the visitors' movements, rather than their names or any other identifying elements, the guests are not told they may be carrying such a tracking device. The authors suggest that if they knew, some might object.

As implied by its subtitle, "Striking the Balance Between Convenience, Choice and Control," the report suggests RFID should be used when and where it can provide a benefit to both implementers and end users—be they consumers or employees. It further recommends that with the technology being employed for applications ranging from public transit fares to passports, access devices and payment cards, RFID should be deployed in lockstep with what it calls an identity management program.

Under such a program, it says, end users could interact with an information system to learn what specific personal information or tracking data was recorded or not recorded, and what was accessible or inaccessible to either implementers or other users of the technology. Such a system, the report says, goes "beyond the juridical notion of protecting personal data, and emphasizes an active role for users determining their identity in the digital public space."

**RELATED\_ARTICLES** Although the document notes that a more comprehensive study of RFID usage is required to generate definitive conclusions, it does suggest that general ground rules for using the technology in consumer or employee applications should provide transparency about which parties are collecting personally identifiable data, and what data is being collected and stored. Parties implementing RFID technology for these applications should follow existing privacy laws in Europe, the report maintains, allowing users to determine what identifying information, if any, is tracked. It also recommends governments within the European Union develop a policy determining whether personal data collected by or stored on RFID devices can be used in criminal investigations.

The full STOA report is available for download [here](#).

Copyright ©2005 RFID Journal, Inc. All Rights Reserved