

People-Tracking Experiment Offers Insights Into RFID Privacy Concerns

At a counterculture technology conference in Berlin, 900 attendees submitted to RFID tracking. The major lesson: People need to feel in control.

By Mary Catherine O'Connor

Jan. 11, 2007—Adding RFID tags to conference badges is nothing new. At the annual [RFID Journal LIVE!](#) events, for instance, passive inlays are attached to conference badges and used to track room attendance for breakout sessions. Exhibitors can then read the tags to gather new customer contact information.

Few, however, would have expected attendees of last month's Chaos Communication Conference (CCC)—an annual forum for hackers, open-source programmers, social scientists and others interested in life in the digital world—to have carried active 2.45 MHz RFID tags to identify themselves during the three-day event in Berlin. Many CCC attendees would normally be more inclined to try cloning an RFID tag or duping an RFID reader than to voluntarily don a tag, since one of the prevailing sentiments among attendees is that RFID is likely to be used as a tool for surveillance, degrading personal privacy.

But does it? wondered Milosch Meriac. The computer engineer designed Sputnik, an RFID experiment carried out at the event so attendees could experience RFID tracking first hand. Meriac is the owner of the Berlin-based hardware and software design firm [Bitmanufaktur](#). The Sputnik project offered an opportunity for him to survey attendees who opted to participate in a system able to locate the tags they wore at any time.

"The idea behind the test was to get an idea of what the future might bring," says Meriac, anticipating the day when it's commonplace for people to carry RFID tags, and for some public or private entities to use the technology to track them. Meriac developed the tags and readers—a system dubbed Open Beacon—used for the Sputnik project, and has made the platform's computer code and reference design available as open-source software at [OpenBeacon.org](#). Upon registration, attendees were offered the tags, which they had to purchase for €10 to cover manufacturing costs. Meriac says he brought 1,000 tags to the event and sold all but the 100 he kept for demonstration purposes. Among the 3,000 or so attendees, he says, demand was high for the tags.

After purchasing their tags, attendees could decide the types of personal information that would be associated with their tags' unique ID numbers. Participants could link their own names, as well digital photos of themselves, to their specific tags. If they wanted to, they could also provide contact info. Those who did not want any personal info linked to the device could use a nickname not tied to any personal information in the database. Meriac says most participants took this route.

The tags have a read distance of up to 10 meters (about 33 feet). To deploy the Sputnik network, 25 of Meriac's Open Beacon readers were deployed throughout the conference rooms, corridors and lobbies in the [Berliner Congress Center](#) (BCC), where the conference was held. Meriac worked with German interactive software developer [ART+COM](#) to create the Chaos Positioning System, which displayed a three-dimensional

representation of all the surveyed areas, showing the location of every tag being read at any given moment.

Each tag's location was determined by measuring the strength of its signal from the reader or readers receiving it. The tags were represented by generic human figures. Live feeds of the location software could be seen during the conference online, over an XML stream. Specific tags could be located by searching for the attendee's name or nickname. If additional information was provided, such as photo or contact info, a viewer could see it as well by clicking on the figure.

"Several people [told me they] felt funny [wearing the tag]," says Meriac. "They constantly felt like they were being watched," and this made them consider their decisions about which sessions to attend. But not all attendees had such a Big Brother experience. Regine Debatty, an attendee and blogger for the site [We Make Money Not Art](#), says she purchased a tag and wore it, but that she completely forgot she had it on. As a result, she says, she forgot to bring it to the conference the next day.

If, at any point, participants wanted not to allow their locations to be tracked, they could simply remove the tags' batteries.

RELATED_ARTICLES Meriac says the Sputnik experiment generated a lot of discussion at the conference about the potential benefits and drawbacks of using RFID to track people. The only way to deploy the technology in a positive manner, he concludes, is to give people control and allow them to choose how the technology will be used. "You need to be able to make yourself untraceable at any time. If you can, it can be a very useful technology."

The design for the Open Beacon tags and readers are available freely to any company interested in manufacturing and deploying them, and Bitmanufaktur is also offering consulting services to help firms deploy or customize the hardware. Meriac says he is early discussions with two companies interested in using Open Beacon to automate their production processes, but that so far, no firms interested in tracking people have approached him.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved