GlobalResearch
Center for Research on Globalization

Big Brother: Radio frequency identification (RFID). Putting "Radio Tags" on Americans

By Global Research
Global Research, April 07, 2008
Seattle Times 7 April 2008

Region: USA
Theme: Police State & Civil Rights

UW team researches a future filled with RFID chips

By Kristi Heim

Seattle Times business reporter

Some University of Washington students, faculty and staff are being tracked as they move about the computer-science building, with details of where they've been, and with whom, stored in a database.

Professor Gaetano Borriello checks a computer to find graduate student Evan Welbourne's last location: on the fourth floor, outside room 452 at 10:38 a.m. Wednesday. He opens another screen to reveal the building's floor plan, and a blinking green dot representing Welbourne shows him walking down the hall.

If it seems a bit like Big Brother, that's the intention. The project is meant to explore both positive and negative aspects of a world saturated with technology that can monitor people and objects remotely.

"What we want to understand," Borriello said, "is what makes it useful, what makes it threatening and how to balance the two."

The technology, radio frequency identification, or RFID, is rapidly moving into the real world through a wide variety of applications: Washington state driver's licenses, U.S. passports, clothing, payment cards, car keys and more.

The objects all have a tiny tag with a unique number that can be read from a distance. Many experts predict that the radio tags, as an enhanced replacement for bar codes, will soon become ubiquitous.

Leaders of the UW's RFID Ecosystem project wanted to understand the implications of that shift before it happens. They're conducting one of the largest experiments using wireless tags in a social setting.

"Our objective is to create a future world where RFID is everywhere and figure out problems we'll run into before we get there," said Borriello, a computer science and engineering professor.

RFID has been used primarily to track goods in supply chains, and the RFID Ecosystem

works as a kind of human warehouse.

For more than a year, a dozen researchers have carried around RFID tags equipped with tiny computer chips that store an identification number unique to each tag. Researchers installed about 200 antennas throughout the computer-science building that pick up any tag near them every second.

The researchers hope to expand the project, funded by the National Science Foundation, to include participation by about 50 volunteers — people who regularly use the building. Volunteers will have the option of removing their data at any point.

The system can show when people leave the office, when they return, how often they take breaks, where they go and who's meeting with whom, Borriello said.

The technology seems less intrusive than a camera, but it's much more precise.

It's a lot easier to fool a camera with a blurred image or disguise. But the latest RFID tags contain a 96-bit code meant to uniquely identify an object or person.

Yet if people don't see the tags, it's easy to forget they are giving out information whenever they come within range of a reader.

"One of the most surprising things is how invisible these tags can be," said Welbourne, who stashed the paper-thin tags in his jacket and bag nine months ago and doesn't always remember he's carrying them. "It's a risk for people. I built part of the system, and I'm caught off-guard."

Lessons learned

UW researchers are gaining some valuable lessons on how to make the technology useful while protecting privacy. Radio tags add a new dimension to social networking. The key is allowing subjects to control who sees what information about them.

They created an application called RFIDDER that lets people use data from radio tags to inform their social network where they are and what they're doing. The feature can be used on the Web and on a mobile phone, with a connection to the social-networking service Twitter.

Borriello can let Welbourne**,** the project's lead graduate student, see where he is all day, or he can modify settings so Welbourne can only see where he is within 15 minutes of their scheduled meeting. The system is transparent, so each can tell if the other has checked his whereabouts.

The lab's Personal Digital Diary application detects and logs a person's activities each day and uploads them to a Google calendar. Users can search the calendar to jog their memories about when they last saw someone or how, where and with whom they spent their time.

Potential pitfalls

Yet the UW researchers also recognize many potential privacy pitfalls.

Some systems, including new U.S. passports and driver's licenses, have been designed to divulge more information than necessary, opening the door to security and privacy problems, Borriello said.

Experts from the UW RFID team went to Olympia to testify on privacy issues related to the state's Enhanced Driver's License.

"There's no reason to have remotely readable technology in a driver's license," Borriello said. He recommends a system that requires contact with the surface of a reader, so the license-holder knows when information on his license is being read.

However, the U.S. Department of Homeland Security required states to use an RFID chip that is readable from a distance to be compatible with its REAL ID initiative.

Washington state went along so it could offer an optional Enhanced Driver's License as an alternative to a passport for residents crossing the Canadian border.

Gov. Christine Gregoire signed a bill last week that attempts to mitigate security and privacy concerns by making it a felony for unauthorized users to read or possess information on another person's identification document without that person's knowledge or consent.

Piecing a profile

Without the right safeguards, data from radio tags can be pieced together to offer a detailed profile of a person's habits without his or her knowledge.

"People don't understand the implications of information they're giving out," Borriello said. "They can be linked together to paint a picture, one you didn't think you were painting."

If someone carrying the new RFID-chipped driver's license visits a store that has an RFID reader and then uses a credit card, the store can start to form an association between the ID number and the credit-card number.

That information can be used to send targeted advertising messages to the customer, a scenario depicted in the film "Minority Report." A man is recognized as he walks by a store and given a personalized sales pitch.

RFID readers placed around shopping malls and airports could help government agencies collect information about visitors' travel patterns, shopping habits and relationships.

"People might think maybe it's a good thing. Maybe it will make me safer," Borriello said. But he added, "You can see this inching forward until we're tracking people wherever they go."

That might sound far-fetched, but it's going on in other parts of the world. Last year, the number of police requests for information from London's RFID-based transit card rose from four per month to 100, Borriello said. Police use the data in criminal cases.

In southern China, the government is installing RFID readers throughout the city of Shenzhen to track movements of citizens, and U.S. companies are helping deploy the technology, The New York Times has reported. Chips in national ID cards contain not just a number, but a person's work history, education, religion, ethnicity, police record and

reproductive history.

“You could argue for any of this stuff in the name of security,” Borriello said. “It’s important to understand what the technology can do and we, collectively, have to decide what we’re going to use it for.”

The lessons from the UW RFID project point to the need for consent and transparency, informing people what data are being collected and giving them a way to review, correct or delete it.

The technology alone can’t be made to do the right thing without a good system of laws and policies around it.

Protection lacking

So far, there are few such legal protections in the U.S., Welbourne and Borriello say.

While RFID is relatively new, one technology with a potential to track people is well-established: cellphones.

“Most of us trust that information is not being tracked by anyone, but in fact it is,” Borriello said.

Large U.S. telecommunications companies are in the middle of a bitter dispute over their role assisting in government wiretapping, and whether they can be sued or be given legal immunity.

Right now RFID is following a typical technology cycle, moving from obscurity into popular usage. The UW researchers are trying to stay ahead of that cycle.

“As soon as it becomes widely used, then it’s more attractive and people start attacking it,” showing its vulnerabilities, Borriello said. The trouble is “by that time, it’s hard to change.”

Kristi Heim: 206-464-2718 or kheim@seattletimes.com
