**Electronic Frontier Foundation**
Protecting Rights and Promoting Freedom on the Electronic Frontier

July 1, 2004

**Via Hand Delivery, Facsimile and Email**

Honorable Members of the Budget Committee
Supervisor Gerardo Sandoval, Chair
Supervisors Chris Daly and Jake McGoldrick, Members
Board of Supervisors
City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102-4689

**RE: Electronic Frontier Foundation opposition to RFIDs at the San Francisco Public Library**

Dear Chair Sandoval and Budget Committee Members:

Imagine a world where your every possession – clothes, cash, books – could be precisely and invisibly tracked. In this world, your purchases, movements, and activities could be monitored in real time or recorded for posterity by marketers or the government, all without your knowledge or consent.

This is the world that RFID (radio-frequency ID) technology could produce if RFIDs and RFID sensors become common. Touted as the new bar code, RFID technology uses tiny computer chips and antennas integrated into "tags" that hold data – at the very least, a *unique* ID number – and report that data when triggered by an electronic scanner, thus enabling the automatic identification and tracking of tagged goods. RFIDs the size of a grain of rice can be near-invisibly embedded in the sweater you're wearing, the disposable razor you've bought, or the book you've just checked out of the library.

Three aspects of RFIDs create problems for personal privacy. First, they're *promiscuous*: they'll talk to any compatible reader. Second, they're *stealthy*: not only are the tags themselves inconspicuous, you can't know when they're transmitting information. Third, they're *remotely readable*: they can be read at a distance through materials like cardboard, cloth, and plastic. That's why U.S. Senator Patrick Leahy called RFIDs "barcodes on steroids" and warned that they herald an age of "micro monitoring."[1]

RFIDs pose several generic privacy threats: the ID linkage threat; the inventory threat; and the tracking threat. The ID linkage threat is pretty self-explanatory – because RFIDs are unique, promiscuous, stealthy, and remotely readable, your personal identity can be linked to your RFID-

[1] Remarks of Senator Patrick Leahy, "The Dawn of Micro Monitoring: Its Promise and Its Challenges to Privacy and Security," Conference on Video Surveillance: Legal and Technological Challenges, Georgetown University Law Center, Mar. 23, 2004, <http://leahy.senate.gov/press/200403/032304.html>.

454 Shotwell Street · San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org info@eff.org

tagged items. It could happen when you use a credit card to buy a tagged good, or when you identify yourself during some other transaction while carrying a tagged good.

The inventory threat is that others can learn what you have or own. It's possible for someone to know what RFID-tagged items are in your backpack or briefcase without your knowledge.

The tracking threat is that others can pinpoint where you are at a particular time or track your movements by reading your unique RFIDs in different places. As RFIDs and RFID sensors proliferate, tracking will be easier and more complete.

For most commercial uses, there's a fairly simple solution – permanently killing the RFID when it reaches the consumer's hands. Library uses are different, because the RFIDs need to be used over and over again.

Because library materials are informational goods, two kinds of privacy threats are especially significant for library RFIDs. The more obvious is the "preference" threat, how others can secretly learn what you believe or think about. Respect for intellectual freedom and First Amendment rights underlies libraries' traditional concern for patron privacy. But because RFIDs are unique, promiscuous, stealthy, and remotely readable, libraries won't be the only ones who can know what books you read.

The other is the "hotlist" threat, where some library material is deemed "of interest" and the authorities try to find out who checked out or was reading that material. Librarians remember the FBI's Library Awareness Program, in which FBI agents visited libraries to find out who was reading materials believed to be of interest to foreign agents.[2] RFID-tagged books make this threat more dangerous, too.

RFID proponents typically make three arguments in an attempt to minimize the significance of these threats. First, they argue that the read range of RFIDs is too short to be useful. The simple response is that we pass through doorways all the time, and RFID sensors can be built into those doorways. If RFID reader gates work at libraries, they'll work in other places.

Second, they argue that no one is interested in who you are, what you have, or where you go. But commercial entities like marketers and insurance companies are acutely interested in the details of our lives. That's why major data aggregators have enormous databases on 95 percent or more of American households, and why "data mining" was a prime focus of Admiral John Poindexter's "Terrorism Information Awareness" program.

Third, they argue that the data on a library RFID tag is meaningless without access to the library's internal databases. But databases are often insecure. Countless news stories about ID theft report that insiders with authorized access misused information or opportunistic outsiders exploited security holes in order to gain unauthorized access. Moreover, many threats, like the "hotlist" or tracking threats, don't require access to internal databases.

---

[2] See generally Ulrika Ekman Ault, The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?, 65 N.Y.U. L. Rev. 1532 (1990).

EFF sees unique, promiscuous, stealthy, remotely readable RFIDs as privacy pollution. We're familiar in the environmental area with the "tragedy of the commons." It might be individually rational for a firm to pollute because it doesn't bear the full costs of pollution; those costs are distributed across many people. But when many firms make that decision, society as a whole suffers; these individually rational decisions are not collectively rational.

The same is true for RFIDs. Libraries see cost savings for them, but what about the privacy risks they will ultimately impose on their patrons? Even worse, library RFID use is likely to legitimize RFID use in general. How bad can RFIDs be if your friendly neighborhood library is using them?

Few big-city libraries in the United States use RFIDs today. EFF believes that San Francisco is a bellwether for library RFID adoption in California and perhaps the rest of the country. San Francisco should be a leader in technology – but only in a socially responsible, privacy-sensitive way. Today's RFIDs do not protect privacy. EFF therefore urges the Budget Committee and the Board of Supervisors to reject the Library's RFID proposal.

Sincerely yours,

Lee Tien

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation
(415) 436-9333 x 102
tien@eff.org

cc via hand delivery, facsimile and email

Supervisor Michela Alioto-Pier
Supervisor Tom Ammiano
Supervisor Bevan Dufty
Supervisor Matt Gonzalez
Supervisor Tony Hall
Supervisor Fiona Ma
Supervisor Sophie Maxwell
Supervisor Aaron Peskin
Mayor Gavin Newsom