Oct. 1, 2003

**To:** **San Francisco Public Library Commission**

**Subject:** **Privacy risks of Radio Frequency Identification "tagging" of library books**

The Electronic Frontier Foundation (EFF)[1] respectfully submits these comments and attached document to the San Francisco Public Library (SFPL) Commission with regard to Goal 16.1 of the SFPL Strategic Plan 2003-2006 (Aug. 21, 2003 Final Draft).[2]

Goal 16.1 states that the Library plans to "[i]nitiate implementation" of Radio Frequency Identification (RFID) technology for books and other library materials. Goal 16.1.2 states that the Library plans to "[i]ncorporate funding for implementation as part of the 2004/2005 Library budget process" with "[i]mplementation to begin in 2005/2006."

EFF writes to oppose the Library's plan to implement an RFID system for tracking books and other library materials. As we explain below, RFID technology raises great privacy concerns because insecure RFID tags will permit inventorying of people's possessions and tracking of people via their possessions. These risks are especially great where books and other reading materials are concerned, because both privacy *and* freedom of expression are at stake. Furthermore, we are doubtful that RFID technology will be more cost-effective than existing technologies and practices for check-out, inventory control, and loss prevention.

Libraries have long been very protective of library patron privacy given that surveillance of reading and borrowing records chills the exercise of First Amendment rights. In the famous *Tattered Cover* case, an American Library Association official testified about "the chilling effect that results from disclosure of library circulation records." The Strategic Plan itself notes that the Library "advocate[s] for and support[s] policies and procedures that protect privacy of all library user records." Concern for privacy of reading records has only increased with the enactment of Section 215 of the USA-PATRIOT Act, which allows the government to subpoena reading records while preventing libraries from saying anything about this invasion of patron privacy.

Accordingly, EFF opposes any use of RFID technology unless the planned implementation includes mandatory deactivation ("mandatory kill") of the RFID tags at the point at which the patron leaves the library. In our view, a "mandatory kill" policy is the only measure that would allow RFIDs to be used by the Library internally, while giving the public the necessary time to consider whether and to what extent they want RFIDs to proliferate.

EFF is very concerned that the Library may not have fully considered the privacy and civil liberties implications of implementing RFIDs and may not yet have received information or opinions about RFIDs from sources independent of the RFID industry. Our comments, to be sure, are tentative because we cannot tell from the Strategic Plan exactly what the Library intends or what RFID technologies are being considered. Has the Library already spoken to well-known vendors like Checkpoint or 3M? If so, have any decisions been made?

Indeed, we are concerned that the Library's plan to adopt RFID technology will unintentionally tend to legitimize RFID use in other parts of society. We fully expect that if the Library adopts RFIDs, the RFID industry will use that fact as part of a public-relations effort to persuade the public that RFIDs are both innocuous and inevitable. *Business Week* has reported, for instance, that "rather than tailoring the technology to address [privacy] concerns," the RFID industry's public-relations firm Fleishman-Hillard "calls for a proactive plan to 'neutralize opposition' and 'mitigate consumer backlash.' The documents advise product spokespeople to emphasize the 'inevitability' of the technology and recommend characterizing RFID as a simple evolution of the bar code, rather than a new technology with futuristic capabilities."[3]

Thus, EFF strongly urges the Commission to reject Goal 16.1 of the Strategic Plan or, at the very least, to postpone adoption of RFID technology pending further study and research into its privacy implications and cost-effectiveness.

Discussion

Imagine a world where your every possession -- your clothes, your books, your car, your cash -- could be tracked with precision: a world where every citizen's purchases, movements, and activities could be monitored by marketers, snoops, stalkers, or even the government, at a level of heretofore-unimaginable granularity. The implications for personal privacy and free speech would be dire. Yet this is the world that will be created by RFID technology, if it is deployed without adequate regard for its social and political implications.

The basic idea behind RFIDs is simple: Tiny tags embedded into products would store information about the product as well as a unique ID number. Radio waves broadcast by RFID readers or scanners would make the RFID tags transmit that information. For businesses, RFIDs represent a "next-generation barcode" solution to the problems of inventory control. An entire warehouse could quickly be scanned to find out how many and what items it contains. RFIDs could also be used as nearly invisible replacements for anti-theft tags.

Unfortunately, RFID technology raises serious privacy problems outside the warehouse and sales floor setting. Because people carry or possess objects, RFIDs also allow people to be tracked via their things. As far as EFF has been able to determine, today's RFIDs are optimized for low-cost, high-rollout production; they are unobtrusive, "dumb," and lack any form of encryption that would prevent unauthorized persons from reading them. Thus, although future RFIDs may permit user control, it is our understanding that RFIDs will lack any information security or privacy safeguards for the foreseeable future.

Accordingly, RFIDs present at least two privacy risks. First, insecure RFIDs permit "inventorying": anyone with a compatible RFID reader can surreptitiously learn what RFID-tagged things you have or wear. Second, insecure RFIDs permit different kinds of "tracking." If an RFID contains information that identifies the person, the person can be tracked via the RFID.

Even if the RFID does not contain personally identifiable information, a person can be tracked through links to other records. If the government had access to a library's borrowing records, it could link a person to the books he or she has borrowed even if the RFID itself does not identify the person. As Beth Givens of the Privacy Rights Clearinghouse has observed,

objects don't necessarily need to be matched with personal identifying information to be used for profiling and location tracking. Imagine a political demonstration in which thousands of people participate. As demonstrators mingle, law enforcement officers with hidden readers capture the unique RFID codes on clothing worn by the participants. Later, when participants perhaps pass through checkpoints, board public transportation, or travel by airplane, the codes can be matched and demonstrators can be detained and/or then identified.[4]

It may be argued that these risks are speculative and hypothetical today. But there is nothing hypothetical about the fact that RFIDs make it easier to track things and people. And if there is one lesson society has learned from computerization, it is that technologies do not stand still. Any socially responsible technology policy must anticipate how technologies spread throughout society and grow in power.

EFF therefore believes that these risks will grow if RFIDs become more common. RFID adoption is being "pushed" from many directions. Governments are using or thinking about using RFIDs. The European Union is planning to use RFIDs in its currency, with obvious implications for financial privacy. The U.S. Postal Service is considering the use of RFIDs for "Intelligent Mail." This "I-Mail" initiative contemplates attaching to every piece of mail a unique, machine-readable identifier. Such identification would not only include postage amount and basic routing information, but the "digital signature" of the sender, including "name, address, or [even] biometric data" to convey the " 'who, when, and where' of the mailer." The implications for anonymous speech through the mails are obvious, too.

When today's consumers learn about plans to deploy RFIDs, they think about society will be like when RFIDs are widespread, and they make extremely reasonable assumptions about what both business and government will do with this power to track. It should therefore be no surprise that businesses like Wal-Mart, Gillette, and Benetton encountered significant public outcry when they announced plans to use RFIDs outside of the internal supply chain.

In fact, the RFID industry is well aware of these consumer privacy concerns; an industry document summarizing the results of focus-group research stated that "Virtually all groups spontaneously said they wanted a choice and that 'the chip should be able to be killed.'"[5]

Here are some consumer concerns, as described by RFID industry research:

1. Will individuals benefit?

"The store will benefit more than the consumer."

*Study comment*: "there are currently no clear benefits by which to balance even the mildest negative, so any negative press coverage, no matter how mild would shift the neutral to a negative."

2. Will RFIDs be misused?

"I am playing cynic for a moment, I can guarantee that they will be able to read through steel."

"I don't think it will be restricted to products. . . it will be linked to personal information."

"The limited range? I reject that promise. . . In the future, the technology will develop. It will leave you naked."

*Study comment*: "Their biggest concern is abuse."

3. Will individuals be tracked?

"I could be tracked by the clothes I'm wearing."

*Study comment*: "Clothing was a major inflamer. Consumers assumed that tags would be embedded into clothing . . . . Tagging their clothes was tantamount to tagging them personally. This was by far the greatest concern expressed in groups."

4. Will individuals be inventoried?

"I'd feel naked if people know what I'm wearing."

"Companies or the government will be able to monitor everything I buy and spy on me."

"Someone could see everything I buy by reading my trash."

5. "Personal security"

"muggers could know what is in my shopping bag or if I'm wearing a Rolex."

"the technology will improve to allow people to read through walls."

EFF reiterates that these consumer concerns are not limited to the here and now. When consumers think about RFIDs, they think about what will happen to their privacy and security if RFIDs and RFID readers become commonplace. The general public is acutely aware of how rapidly technology improves, and they know that privacy-invasive technologies often start small but usually spread more quickly than "experts" predict. The time to think about these privacy concerns is now, before RFIDs become part of the fabric of everyday life.

Contrary to popular belief, RFID technology is still in its infancy in consumer-facing applications. As a national newspaper recently reported, "Wal-Mart Stores Inc. and Gillette Co. abruptly yanked a pilot program for the technology" and quoted a Wal-Mart spokesperson as saying that it will be "many years" before tagging individual items is practical or profitable.[6] The Public Library Association of the American Library Association reports that "RFID systems are still relatively new in libraries" and that "[f]ewer than 50 had been installed as of the third quarter of 2001," with only two sites labeling more than one million items each.[7]

Finally, we are doubtful that it is worth it for the Library to implement RFIDs as a cost-saving measure given these privacy concerns. How much will this cost? Does the Library know how its contemplated RFID system will work? How much will RFIDs really facilitate users' self-service check-out of library materials as compared to existing barcodes? How much will RFIDs really improve inventory control or loss prevention over existing methods? How will they prevent loss? Has the Library been getting its information from RFID industry representatives, or has it consulted independent technologists? Has the Library performed a technology assessment? Is there any evidence that RFIDs will provide a net marginal benefit over less privacy-invasive technologies? The public deserves answers to these and other questions before, not after, the Library decides to use RFIDs.

Conclusion

EFF's general position on RFIDs is simple. Because they pose inventorying and tracking risks and lack meaningful information security, current RFID technology, if it is to be used on consumer-facing products, must be permanently disabled or "killed" at the point of sale. We also urge industry to make "kill" technology cheaply and readily available to consumers, so that individuals can be sure that RFIDs truly have been disabled.

Accordingly, EFF urges the Commission to reject Goal 16.1 of the Strategic Plan or, at the very least, to postpone adoption of RFIDs pending further study and research into its privacy implications and cost-effectiveness.

Respectfully submitted,

Lee Tien

Senior Staff Attorney

Electronic Frontier Foundation

Addendum

EFF has been informed that the Library is amending the language of the Strategic Plan to reflect that the Library has not yet decided to implement an RFID system. While this is good news, it does not answer the concerns and questions we have set forth above. EFF hopes that the Library intends to open the matter of RFID implementation to public discussion, and looks forward to participating in any such discussion.

---

[1] EFF is a non-profit, civil liberties group based in San Francisco with more than 10,000 members. Our website is at <http://www.eff.org>.

[2] EFF does not express any opinion about other parts of the Strategic Plan.

[3] Jane Black, "Playing Tag with Shoppers' Anonymity," *Business Week Online* (July 21, 2003). http://www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm

[4] Beth Givens, Privacy Rights Clearinghouse, *RFID and the Public Policy Void* (Aug. 18, 2003) (presented to Joint Committee on Preparing California for the 21st Century, California Legislature, Sen. Debra Bowen, Chair), available at http://www.privacyrights.org/ar/RFIDHearing.htm (see enclosure).

[5] Auto-ID Centre, *Executive Briefing, Public Policy: Understanding Public Opinion* 6 (Feb. 1, 2003), <http://cryptome.org/rfid/cam-autoid-eb002.pdf>.

[6] James Covert and Christina Cheddar Bork, "Tracking Chips Stir Privacy Concerns," *Wall Street Journal* pg. 1 (Jul. 29, 2003, eastern edition).

[7] http://www.ala.org/Content/NavigationMenu/PLA/Publications_and_Reports/Tech_Notes/RFID_Technology