The Samuelson Law, Technology, and Public Policy Clinic (the Clinic) at the University of California-Berkeley's Boalt Hall School of Law
RFID Vendor Assessment Tool

In addition to best practices, we have created a privacy assessment tool for libraries to gauge the privacy protection capabilities of particular RFID systems. This question set helps a library evaluate particular systems they may be considering. Guidelines for RFID vendors could call for automatic disclosure of such information.

- Do RFID writers used by the system write any information to tags by default? *The behavior of tag writers should be transparent, so that deploying entities can control the data contents of RFID tags they deploy.*
- Does the system use labeling formats that obscure data to unauthorized readers? *When possible, labeling formats should obscure data. This may conflict with needs to standardize formats for interoperability.*
- Who can rewrite the tags and how is this controlled technically? *Tag writers should maintain some type of access control, such as password protection, to prevent unauthorized and potentially malicious use.*
- What are the read ranges on each piece of RFID equipment? *Longer read ranges can cause problems with packet collision avoidance. More importantly, from a privacy standpoint, long read ranges increase the threat of surreptitious reading and eavesdropping.*
- Is there a wireless interface option between circulation stations and the library database? If so, what measures does the system provide to protect those transmissions? *Systems are most secure when they do not engage in wireless transmission, which due to the broadcast nature of radio, can easily be intercepted. If wireless components are used, efforts should be taken to protect transmission with standard cryptographic techniques. However, even in such situations, it is important to bear in mind that standard wireless protocols that incorporate encryption are often trivial to break.*
- How long does the server retain the cached information? How is cached data accessed? How is cached data protected from unauthorized access? *When components of the RFID system cache information, periodic deletions of records should be performed to prevent the accrual of massive databases which may be subject to unauthorized access at a later time. Data that is being stored should be protected with adequate access controls to limit unauthorized access.*
- Do the security gates generate item logs? Do the security gates log only items that have not been checked out or all materials passing through? *Security gates that cache information about which tags have passed within proximity present a large store of information which if accessed by an unauthorized party could lead to large scale privacy violations. Systems which use security gates capable of logging all books should be configured to log only those with permissions violations. Second, if at all possible, security gates should not access and cache internal library*

records. Most security purposes should require only verification of deactivation of the so-called 'security bit'—a bit which is toggled at check-in and check-out.

- Are pre-programmed tags rewriteable? If so, who is able to rewrite them, and how is this enforced technically? *Tag writers with access control mechanisms should be selected over those without access controls.*
- What is the nature of and purpose of the factory programmed serial number on the tag? How many series does the factory use? *When purchasing preprogrammed tags from an RFID vendor, it is important to discover whether it uses a serial number management system which can easily be reverse engineered, such as labeling tags uniquely in increasing sequence. Privacy is promoted when systems are chosen that provide for redundancy between labels sold to different customers, and that employ a thoughtful process of allocating those numbers in order to avoid easy discovery by unauthorized third parties.*
- What is the nature of the extra memory? *Some systems provide two regions of memory: one which can be rewritten, 'extra memory', and another portion which is read only. Other systems provide only one rewritable section. If your system is the first, your RFID vendor may retain information about your tag labels which you are unaware of. Moreover, without full information about tag contents, assessment of privacy risks may be inaccurate.*
- What is the tag encryption scheme? *None of the tag systems we examined use an encryption scheme. Indeed researchers have noted that strong encryption is not possible in current generation tags due to a lack of computational power. However, systems capable of encrypting tag contents are more desirable from a privacy standpoint than other systems.*
- Can the library lock all or part of the tag's memory? How is this accomplished technically? *When purchasing systems with so-called 'memory locks' libraries should take caution to discover how these locks work. Libraries should not rely on their efficacy until there is independent confirmation of their functionality in controlling all writers, and not just writers from the tags' manufacturer. Some systems claim to use 'memory locks' on tags in order to prevent data from being encoded onto RFID memory without authorization. However, with the systems we examined this is a red herring. Chips contain a 'write bit' which may be toggled. RFID writers from the same manufacture then scan the setting of this bit before allowing or disallowing writing to the chip. A writer from a different manufacturer could simply ignore this bit, or be unaware of it, and write to the contents of the tag in spite of its setting.*