Privacy Concerns

Marketing or outreach activities must be consistent with any applicable privacy policies. Commercial marketing techniques make extensive use of personal information. Libraries must take a more tempered approach, ensuring protection of patron privacy. Any use of patron data must thoroughly conform to the privacy policies that govern how any personally identifiable data can be stored, accessed, used, or shared. Although privacy policies vary among different libraries or their parent organizations, there are some general prevailing concerns.

Any use of statistics must ensure the privacy of the individuals involved. To preserve patron privacy, reporting or analytics is usually based on fully anonymized data sets. Ideally, any data collected removes personal information before it is recorded. When personal details are needed for essential operational processes, the data sets can be anonymized as soon as transactions that require those details are concluded. Anonymization generally involves removing details identifying a person, but preserving the patron types, item categories, or other relevant nonpersonal data. The anonymization of transactional data should not significantly impede reporting and analysis.

Storage and Transmission

Any sensitive data should be encrypted to prevent unauthorized access. This technique ensures that even if an intruder gains access to the internals of the system, the data itself will not be accessible without the required digital credentials. Most modern database management systems have built-in capabilities to store data with encryption. When data is transmitted from one system to another or accessed through an application such as an ILS, use of encrypted protocols such as HTTPS provides strong protection from interception of data on the internet or other networks. Even if privacy policies do not address data encryption, this level of protection falls within the area of standard security practices for any type of sensitive data.

Data Collection and Retention

Another type of data is created through the operation of a computer application. An integrated library system, for example, creates a record for every circulation transaction. These circulation records hold data relating to a specific patron and a collection item. These records are essential to managing borrowed items. The library needs to be able to track what items are in use and not available to other patrons and may need to contact the current borrower to send circulation notices. Most ILS catalogs offer the ability for the patron to sign in and view the status of all items currently borrowed.

In addition to the circulation transaction record, some ILS products include a field in an item record that retains the identity of the last patron who borrowed it. Patron records may also include fields that retain items charged or requested. This data may be related to reading lists, created automatically or at the option of the patron. Data related to a patron's use of an item may be created in many aspects of an ILS, and it is essential that all these representations of a circulation transaction be managed consistently according to privacy policies.

While it is necessary to maintain data linking a patron and an item during the course of the loan, another set of data retention issues apply once the item is returned. From a strict privacy perspective, no records should be retained that make it possible to reconstruct the use of that item by a specific patron at a specific period. These strict privacy practices prevent the disclosure of a patron's borrowing history, even when legally requested.

Rather than completely removing circulation transaction records, it is a common practice to replace

personally identifiable data with placeholders that may retain specific characteristics of the patron who borrowed the item, but not the specific identity. These anonymized circulation history records can be used for statistics and analytics while respecting privacy requirements.

Such a strict approach to privacy limits the data available to the library to deliver personalized services to its patrons and to implement some forms of marketing. The history of a patron's use of the collection gives important clues to topical interests that could be used for future reading recommendations or to send notifications of relevant library programs or new content acquisitions.

The most restrictive approach to privacy may hinder libraries from offering personalized services. Patrons may appreciate the ability to view the materials they have previously borrowed or other lists of items. Many ILS products give options for the retention of borrowing history or reading lists.

There are four approaches that libraries can take in relation to patron privacy:

- **Strict privacy:** The library configures the ILS to never retain circulation history in transaction files or borrower records.
- **Full retention:** The library configures the ILS to always retain circulation history in transaction files and borrower records. Libraries in corporate

or military settings may use this approach where no privacy of library use is expected.

- **Optional retention:** Patrons can choose to have the system retain their borrowing history and other data that may enable personalized services and their own ability to view lists of previously borrowed items. Unless the patron specifically opts in to retention, the system follows the strict model of privacy for transactions related to that account.
- **Optional privacy:** Patrons can choose to have the system remove or anonymize their borrowing history and to not be offered personalized services or be able to view lists of previously borrowed items. Unless the patron specifically opts in to strict privacy, the system follows the full retention model of privacy for transactions related to that account.

Which of these privacy models the library chooses will have an impact on its strategies for personalized services and marketing when using products that depend on circulation history data.

Even under the strictest privacy models, libraries can implement effective marketing and outreach services. The level of personalization and granular audience segmenting will be more limited than seen in the commercial arena, but the approach may be less intrusive and be better received by library patrons.