Biometrics

Or, "Why does the library want my fingerprint?"

- Biometrics refers to the use of unique human characteristics for identification
- The most common biometric identifiers are fingerprints, facial recognition, DNA, and retinal scans
- **1892**: first fingerprint classification system developed
- **1960**: Facial recognition became semi-automated
- **1969**: FBI begins trying to automate fingerprint recognition
- **1994**: Immigration & Naturalization Service develops IDENT as a law enforcement tool

- **Office of Biometric Identity Management (OBIM)**
  - Largest repository of biometric identifiers in the U.S. government
  - Supplies tech for matching, storing, & sharing biometric data
- **Automated Biometric Identification System (IDENT)**
  - Operated & maintained by OBIM
  - Holds over 260 million unique identities
  - Processes more than 350,000 biometric transactions daily
- **Department of Commerce's National Institute of Standards and Technology (NIST)**

In Libraries, Museums, & Archives

- Primarily used to replace/reinforce token- or knowledge-based identification systems
- Fingerprint scanners can be used to provide access to in-house computers, restricted spaces such as special collections, and to automate the check-out process for patrons
  - **Pros**:
    - Greater security than cards and knowledge-based systems, which are prone to loss or theft
    - Greater autonomy when checking out books, especially those on sensitive topics
    - Potential for cost reduction by eliminating need to maintain physical card system
  - **Cons**:
    - Potential for data security breaches
    - Technology can be expensive to maintain/initially acquire
    - Not all patrons may want to sign up, creating a mix-and-match system
    - Concerns around job cuts/using tech to replace employees

How does it work?

- A specialized scanner captures an image or several images of a fingerprint
- The "data" in the print—whorls, loops, and so on—are converted to a series of mathematic data points unique to each user
- This generated formula is stored locally in the machine or stored in the cloud
  - Your fingerprint is **not** stored, only the generated numbers sequence, meaning that even if the data *did* get hacked your print cannot be reverse-engineered
- When a patron scans their print, the machine confirms that the data points match, thus confirming the user's identity
- The scanners can be used in conjunction with a card or user name, or used solo once a patron has opted into the system and provided their biometric data