Chapter 2

Making Contact

Any marketing plan depends on contacting current and potential customers and presenting content designed to entice them to use the organization's products or services. Commercial businesses go to great lengths to assemble customer lists that can be used for marketing and promotion.

Effective marketing requires careful planning to send interesting content to carefully defined groups of users. General content blasted indiscriminately to all possible contacts is not likely to generate a positive response and may even be counterproductive. Library outreach and marketing tools tap into multiple sources of potential interested recipients, with the patron database of the integrated library system as a basic starting point.

Libraries may also be able to supplement the contacts available through their integrated library system. Additional sources may include registrations from library-sponsored programs. Some digital content products offered through the library may include online registrations, which can be converted into patron records. OverDrive, for example, works with the library to perform online registrations to gain access to its e-books and audiobooks. Most libraries acquire additional verification to turn these digital registrations into fully authorized patrons.

General or Topical Newsletters

As part of its ongoing marketing efforts, a library may create and distribute newsletters to its patrons. The newsletter may be manually produced, or it may be assembled from content components generated from event management applications, from the website, or from other sources.

Modular Content

A messaging strategy depends on fresh and relevant content. It is possible to compose the text for each piece of communication manually. This approach may work well in many scenarios, but it may not scale to high volume or sophisticated messaging strategies.

Content can also be managed in a modular way, based on small blocks of content and metadata. The content blocks may include text, images, or video describing a discrete event, a collection of library material, or a featured service. When tagged with appropriate metadata, such as a date range, topics, a targeted age level, or a relevant library location, these blocks can be assembled into a newsletter, landing page, or other marketing opportunity.

Segmentation

One of the basic concepts of business marketing relates to dividing the audience into segments to receive relevant messaging. There may be times when the library wants to distribute a general message to its entire database of patrons. A more effective model involves targeted marketing, where selected content is distributed to a narrower set of recipients who are likely to be interested and to respond to the invited action.

In the library context, segments can be dynamically created according to multiple factors:

- age categories: children, young adults, general, seniors
  - data source: ILS (integrated library system) patron record

- gender: probably not an appropriate segment in most cases
  - data source: ILS patron record
- geographic: neighborhoods, closest branch location
  - data source: ILS patron record
- topical: self-identified or inferred through content selections
  - data source: ILS borrowing history (opt-in)
  - data source: reading lists created (set by patron as public)
- activity: categories of use patterns based on the number of library interactions, such as items borrowed, programs attended
  - data source: ILS activity (counts versus specific items; may or may not require opt-in)

Looking beyond data generated within library systems, it is possible to create additional segments by combining library data with other data sources. Addresses from the patron records can be matched with census data and income data to identify additional segments. Such affinity groups as urban, suburban, rural, or demographics of specific neighborhoods may be helpful for planning and targeting library services. Using segments derived from blending library data with data from external sources for targeted marketing messaging may not be consistent with privacy policies.

Libraries must be very careful in how they create segments. Using content interactions as the basis of segmentation may violate privacy policies. A basic principle of library privacy protects any content viewed by a patron as confidential. Should a patron view an item of content, most library privacy policies would preclude using that information outside the bounds of confidentiality. Patrons may choose to enable use of their reading history for the benefit of receiving recommendations or other relevant content.

The Role of the Integrated Library System

The integrated library system provides the foundation for many aspects of the operation of a library. It manages a repository of data representing library patrons, primarily in support of its circulation features. Lending materials involves making links between records representing the item borrowed and a patron record.

Another standard capability of the circulation module of the ILS involves the transmission of notices related to active loans. The ILS will generate notices to library patrons for items not returned before their due date. The specific cycle of notices follows policies set by the library, usually beginning with a reminder that the item will soon be due, followed by notices at multiple intervals for items held past their due dates. Finally, after a lengthier period, a notification may be sent stating that the item is considered lost and that the patron may be responsible for replacement costs.

The notices generated by the circulation module will follow the patterns and wording established in the technical configuration of the ILS. E-mail has largely replaced print messages sent through the postal service. Some libraries may also offer SMS as an alternative transmission. When a library offers multiple transmission options, patrons may set their preferences in their profile as well as updating e-mail addresses or phone numbers.

The built-in messaging capabilities of most ILS products are not necessarily designed to be sophisticated marketing or outreach tools. They follow specific business rules related to circulation events.

Automated marketing makes use of a different set of business rules to generate messages to library patrons. Rather than the punitive messages related to circulation notices, messages in support of marketing and outreach take a positive, invitational tone. These messages inform patrons about services, programs, or content that may be of interest to them.

Patron engagement tools for libraries generally include connectors to enable interoperability with the ILS to tap into the patron database or other relevant data elements. This interoperability usually takes the form of taking advantage of APIs exposed by the ILS or of the secure transfer of data files in batch processes. In some cases, the patron engagement tool is able to subsume the distribution of circulation notices that would otherwise be sent directly by the ILS.

ILS Patron Records: Core Data for Patron Interactions

Libraries can use the database of patrons managed through their integrated library system as a foundation for their marketing and outreach efforts. These records enable core features of a library management application, primarily related to circulation of and access to library materials.

Patron records contain personally identifiable information and therefore must be treated with extreme caution to ensure privacy. These records contain basic details such as names, e-mail addresses, phone numbers, and physical addresses and will assign a unique identifier. These records may also contain other identification data, such as driver's license numbers or other government-assigned identifiers. In the United States, most libraries have moved away from the practice of including Social Security numbers in patron records, but this was formerly a common practice.

It is also standard practice to record birth dates in the patron record. This information may be required

for minors for any age-restricted materials or programs. Information in categories such as gender, ethnicity, or marital status should be treated very carefully or not collected.

Security: Comprehensive Encryption

Patron records must be held securely to prevent unauthorized access. These records should be encrypted as they are stored within the system and transmitted only when full end-to-end encryption has been activated. Encrypted communication would apply to staff software accessing the system, such as for circulation activities; any information displayed via web browsers, such as when a patron views or updates their profile; or during any batch processing, such as importing or exporting patron records to external applications.

Patron Data Sources

Academic libraries usually receive comprehensive feeds of eligible users from other business systems. These include student information systems and payroll or other administrative systems for faculty and staff members. The core user records received from these external sources will be expanded in the integrated library system with additional fields needed for borrowing materials and using library services.

The number of active patron records held in an ILS will usually be a subset of the total residential population of its service area. One of the main goals of a public library's outreach or marketing effort involves increasing the proportion of registered patrons relative to the total eligible population.

Public libraries build their patron database through in-person or online registration. Eligible patrons include those residing within the library's legal service area. Unlike academic libraries, a public library would have no automatic feeds available to automatically populate its patron database from external sources. Although other municipal or county agencies may have their own databases of residents, these are usually not shared with a library.

Public libraries often must be sure that the individual applying for a library card physically resides within its legal service area. Since public libraries are funded through local taxes, they may have formal requirements to provide free services only to residents.

Patron Registration

Public libraries build their patron databases through the registration of eligible individuals. First-time library users will submit details to the library along with any documentation required by library policy to confirm residency. Most libraries require in-person registration to be able to verify documentation.

It is also expected that an ILS will manage groups of records related to a family unit. It may be necessary to set up a record for a minor with a parent or other designated adult to be responsible for any payments or to receive copies of notices.

Some libraries offer online registration. This process may require additional tools beyond what is provided through the ILS patron management modules. An online registration service may perform several checks to ensure that the individual making the application is eligible. These validations include the following:

- Geolocation of the IP address of the device used to apply for the library card, ensuring it falls within the library's service area. This process has a low level of confidence since IP addresses are only loosely associated with physical locations. Virtual private networks or other network tools further complicate the association between a device and the person's physical location.
- Validation of the street address provided. Tools are available to determine that an address given in a registration application exists and is within the library's service area. This validation may not be adequate for some libraries since it does not confirm that the person resides at that address. It is not difficult to guess or look up a qualifying address.
- Other services that may perform more extensive validation processes that check to see if the individual represented in the online application matches any public or business records associated with the address. This type of online validation is not commonly implemented since it may involve the use of a paid commercial service and may not be accurate if the applicant has recently moved.

OverDrive offers a service for online digital registrations for public libraries. Libraries may opt in to this service to enable their patrons to gain immediate access to e-books without having to visit the library to verify their residency. It is common for a library to allow online registration for access only for e-books or other digital content, requiring an in-person visit to convert a digital registration into a full-featured library card.

Communication Channels

Libraries and other organizations transmit messages through several different communication channels. Each channel has its advantages and disadvantages.

E-mail Delivery Protocols and Standards

The July 2020 issue of *Smart Libraries Newsletter*, in response to a reader's question, addressed the technical characteristics directly relevant to e-mail distribution of notices and marketing communication.

"What are some of the e-mail transmission standards and protocols that a library should implement to ensure privacy and reliable delivery? Can libraries depend on reliable e-mail delivery for important communications such as circulation notices? How does e-mail fit into marketing campaigns?"

The main questions with e-mail concern are trust and reliability. How do you know that the message is from its stated sender? Is the message sent and received intact, or has it been intercepted and altered in transit? Is the message private, or can others intercept and read it? Does the message contain meaningful content, or has it been generated through bulk advertising? Does it contain malware or link to a malicious site with malware? Is it a message that tempts the receiver to divulge personal information or to fall prey to some type of scam? Many attacks rely on social engineering to take advantage of naive victims. All these scenarios are so common that they diminish trust in e-mail as a communications medium. Fortunately, the e-mail ecosystem has evolved to provide multiple layers of protection for each of these possible types of misuse. To be considered trustworthy, mail services must implement a complex set of protocols and standards that validate the identity of the sender and the integrity of the message and guard against most patterns of unwanted or dangerous solicitations.

Gmail, Microsoft Outlook and Exchange, Yahoo Mail, and other major providers of e-mail services have implemented sophisticated infrastructure based on the latest security practices and protocols to safely send and receive messages. Major mail services pass each message through sophisticated algorithms to categorize them according to risk level, automatically rejecting those that fall into obvious categories of unwanted mail and flagging those deemed suspicious. These services offer an option to automatically place suspicious messages into something like a "Junk E-mail" folder or to automatically delete them.

The Apache SpamAssassin, a widely implemented open source application for mail filtering, evaluates a complex list of factors to assign each message a score representing the likelihood that it is spam (see https://spamassassin.apache.org). Errors in technical implementation of mail delivery, suspicious patterns of content, or an origination from a source known to be associated with spam generation results in scores that may fall below the mail service's threshold for trustworthiness. There are circumstances where libraries need to generate messages to their users or community members. Notices from the library's integrated library system are the classic example. Other scenarios include messages related to event registration, program announcements, or general marketing and publicity. The applications that generate these messages must be configured to format and transmit e-mail messages in strict conformance to the applicable standards and protocols and to follow practices that will ensure their classification as safe for delivery and not rejected as spam.

A number of standards and protocols are involved in the secure and reliable transmission of e-mail messages. Though a bit technical, it is important to have at least a general understanding of the e-mail ecosystem when implementing or evaluating products that involve the generation of e-mail messages to patrons or community members.

In order to generate an e-mail message, the application needs access to a message transfer agent (MTA) that uses the SMTP protocol to transfer the message to the intended recipient(s). Examples of MTAs include sendmail in the Unix environment or Exchange on Microsoft Windows servers. SMTP uses a series of conversational directives where the application provides mandatory header fields (To: From: Subject: Date:), optional supplemental fields, and the body of the message. It is essential to control access to the MTA by requiring some type of strong authentication before initiating a SMTP sequence. Failure to do so results in an "open relay," which enables unauthorized agents to generate mail via the institution's domain.

Sender Policy Framework

SPF, or the Sender Policy Framework, describes a set of configuration practices that confirm that the MTA is authorized to deliver e-mail on behalf of the domain name representing the organization. This framework includes entries in the DNS (Domain Name System) configuration for that domain. Since DNS configuration details are strictly controlled and can be made only by authorized domain administrators, these configuration entries can be considered as trustworthy. Basic configuration details related to e-mail include the creation of an MX record specifying the mail server authorized for the domain and a PTR entry that enables a reverse DNS lookup, which is useful to e-mail validation. SPF goes beyond these basic DNS entries and involves the creation of a TXT entry in the DNS record for the domain that lists the IP addresses or domains of the authorized MTAs. Receiving mail systems will perform a DNS lookup that validates that the MTA that originated the message properly appears in a TXT entry for that domain. (Example: **librarytechnology.org. 37 IN TXT v=spf1 ip4:xx.xx.xx.xx**).

SPF provides a basic level of assurance that the e-mail agent that generated the message is authorized to do so, but does not address every possibility for abuse.

DomainKeys Identified Mail

DKIM, or DomainKeys Identified Mail, provides an additional layer of features that ensure the integrity of the message. It addresses the concern that the message received has not been modified in any way from its original form. DKIM accomplishes this validation via encryption technologies involving public and private keys. The application generating the e-mail message produces multiple cryptographic signatures that can be used to validate the integrity of the delivery headers and the body of the message. Hashes are generated using the private key, which is never shared publicly. The DKIM routines then insert an additional header into the message, which is used by the receiver to validate the message. Validation of a cryptographic hash requires access to the public key, which is published in the DNS entry in the sender's domain record in a TXT entry.

Example of a DKIM TXT entry:

dkim._domainkey.librarytechnology.org: v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM IIBCgKCAQEAvP/zFa1IAR3HZM6i44ksmvvxOr BMztncbYiqPXWnNljRoOg6x2CMwZPVaODsETpAfSIDff42j0tkP2ZQ0SYNJu6bGlKFKJSvsp+g6FAcnslw3S SN6lDLATQS4zsjLTiZeS/WfsjRMcxL67usCuH80/fy Bnt0piTnbOx5QmQpAittwGzctm6ICkHPB8h6oXiVjaab8XBRStOrhDUe76ILVkDr0ppIlqhkf404mSOsowLfU6c5RDmcrYh5xij1sxS/apR/gzSdd4hSuaoIMeeVX4+DHllsYLuPO4AsbkHVqn0djYIL6+rh/q70CYvID6 ZI40flhvLjQ8QRmeUAGc3TwwIDAQAB;

Example of a DKIM signature provided in a message header:

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=librarytechnology.org; h=to:from:subject:date:mime -version:content-type:content-transfer-encoding; s=dkim; bh=Xs6hjsnOsLry/yDSCPIoYzsRK+ddfUi+o99n3sD7L gI=; b=S8EHFNpthh+A8phZuuQX1UTGyRK0koYo+gq Dt2gQC329sn2tMURGXiQUxSPbCvB7m3lgsUB4LuOp/ olZbz0IbUeVamQxkk6dKXGJbir8yhA0349jLzmLyNa ATX2DsLsGukpoLtEArRPDYJ0r0kiJXWHiGXv1oAt 22ziFZMy57I724cQQw5RcaOct2HpFyfGNOCiW0AD +i+64UHxMThj25LKrDbQsbocjhPweWlpwkF7nCP D0kA36bNCyPCi8zmE0v9W3k+njA0vPs0j+p0ITxTyI Y7cfSj9G7GU0R6jpsgLN4HjnPtkSt398FTHThXpNg/ J58pEE7gQkOBUKkEhzQ==

This signature includes multiple components, including the DKIM version, the algorithm for canonicalization for message body and headers prior to generating the hash and signature, the selector referenced in the DNS entry, and the base64 hashes for the message body and for the full message. The body hash applies only to the message body and can be validated without reference to the public key. If the body hash is valid, the receiving mail system will perform a DNS request to access the public key for validation of the digital signature of the message. If all these steps are successful, the DKIM signature is considered valid. Implementation of DKIM is a bit complex, but gives strong confidence to the integrity of the message.

Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (DMARC) builds on SPF and DKIM, adding an additional layer that enables reporting and accountability in the e-mail ecosystem. Also implemented as a TXT entry in the DNS, DMARC aligns to existing SPF and DKIM entries and provides addresses to send and receive e-mail performance and exception reports. These reports enable a mail administrator to know if unauthorized or invalid messages were sent on behalf of their domain.

Multiple Interrelated Protocols Increase Trust

The implementation of this full suite of e-mail protocols can be a bit complex, even for experienced systems administrators. Fortunately, most libraries will not need to implement them directly. In most cases the vendor of the ILS, event management system, or automated marketing solution will attend to these details. Libraries should, however, require that these vendors demonstrate that these protocols have been implemented and produce fully validated messages. This is especially important if the messages are sent using the library's own domain, which is the preferred approach. Libraries would generally prefer that the messages sent on their behalf come from an e-mail address like circulation@mylibrary.org rather than something like circ.mylibrary@vendor.com.

These protocols and procedures provide a basic technical foundation for a library's e-mail messaging environment. With this foundation in place, e-mail can better serve as a component of an overall messaging strategy that includes other channels such as mobile messaging and social media. Many libraries are working toward communications strategies that go beyond support of transactional interactions, such as circulation notices, to also encompass broader campaigns in support of stronger engagement with existing patrons and to reach more broadly into their service community.

Marshall Breeding, "Smart Libraries Q&A," *Smart Libraries Newsletter* 40, no. 7 (2020): 4, https://librarytechnology.org/document/25338.

Printed Messages Sent through the Postal Service

Sending print messages incurs significant costs in terms of paper supplies, printer maintenance, postal fees, and personnel costs. A portion of notices will not be successfully delivered due to address changes. The proliferation of unsolicited mail reduces the chances that a notice received will be read.

E-mail

E-mail has become the primary means of communication between libraries and their patrons. The composition and distribution of e-mail messages can be entirely automated and do not involve direct costs. Delivery of e-mail messages will be hampered by changes in recipients' e-mail addresses, which are much more volatile than physical addresses. Delivery of e-mail cannot be guaranteed. Many destination e-mail services will reject messages that contain technical errors, that do not conform to all mail security protocols, or that are delivered through mail servers with insufficient reputation. E-mail can also be blocked through anti-spam services that recipients may subscribe to.

Some e-mail delivery services implement techniques that improve the delivery rates of messages and can track whether messages have been opened. These techniques include using the notifications for message receipt and message opening built into SMTP (Simple Mail Transfer Protocol). These receipt requests may or may not be honored by the recipient's mail service. Other techniques include tracking pixels that a mail messaging system can use to detect when a message has been viewed.

E-mail messages can be sent as plain text or can be formatted in HTML to enhance formatting and include images for a more visually appealing presentation. While most modern e-mail services support HTML formatting of mail messages, it is essential to create e-mail messages with both plain and HTML versions. The technical composition and delivery of e-mail messages with HTML formatting can be complex and may not be possible in some messaging environments, such as circulation notices generated from an ILS. Some of the marketing applications discussed later in this report can offload the circulation messages from an ILS and deliver visually appealing notices with graphics rather than the plain text messages that would otherwise be distributed. Messages including HTML content are assembled with the "Content-Type: multipart/alternative" mail headers, with strings that indicate the borders between the plain text and HTML versions of the message. These details illustrate the technical complexity involved in creating visually appealing e-mail messages with high rates of successful delivery.

SMS

In many contexts, text messages received on mobile devices have supplanted e-mail as a preferred messaging channel. Many individuals have moved away from e-mail to text messages due to the excessively high rate of unsolicited e-mail. Delivering library messages via SMS involves additional technical components or paid services. These services usually charge a fee for each message delivered. For libraries with a high volume of message traffic, the costs can be significant. SMS messages tend to have a much higher success rate than e-mail, provided the library has current mobile phone numbers for its patrons. Notices sent via SMS must be succinct and direct and with no distracting formatting.

Transmission of library messages via SMS will usually be used only if specifically selected by the patron. Many individuals use text primarily for personal communications and may not want to receive other kinds of messages. Unsolicited messages have degraded e-mail as an effective communications medium, and text messaging may be similarly polluted as unwanted messages proliferate.

Library Use and Performance Data

Public libraries strive to assess the quality and quantity of their services. These statistics not only inform the administration of the library in the allocation of staffing and other resources but also are usually required by their boards as well as local, state, and federal agencies. Libraries collect statistics on many different areas of activity, such as the following:

- circulation transaction counts for check-outs, renewals, returns (ILS)
- web visits, segmented by resource and user characteristics (web logs and analytics)
- digital downloads for e-books and audiobooks (vendor usage reports)
- use of electronic resource packages (library ERM [electronic resource management] or LSP [library services platform] + vendor COUNTER statistics)
- print and electronic materials acquired (ILS acquisitions)
- materials weeded (ILS)
- number of programs offered and attendance (event management system)
- new patron registrations (ILS patron maintenance)
- detailed collection statistics and analytics (ILS or LSP analytics or third-party analytics like collectionHQ)

- registered patrons and demographics (ILS patron analytics, OrangeBoy Savannah, Gale Engage)
- entrance and exit counts for each library building (people counters, security gates)
- use of public computers (PC reservations application)
- Wi-Fi sessions (network analytics)
- use of makerspaces (informal statistics, sign-in data)

Statistics tracked over time present important information on the use patterns or trends needed to assess the impact of the library, to inform resource allocation in support of any given area of activity, and to guide outreach strategies. In an outreach and marketing context, much of this data can be used to identify areas of desired improvement and to measure the impact of marketing activities.