Column Title: posIT

Column Editor: Kenning Arlitsch, Dean of the Library, Montana State University, Bozeman, MT
kenning.arlitsch@montana.edu

This JLA column posits that academic libraries and their services are dominated by information technologies, and that the success of librarians and professional staff is contingent on their ability to thrive in this technology-rich environment. The column will appear in odd-numbered issues of the journal, and will delve into all aspects of library-related information technologies and knowledge management used to connect users to information resources, including data preparation, discovery, delivery and preservation. Prospective authors are invited to submit articles for this column to the editor at kenning.arlitsch@montana.edu

Heeding the signals: applying Web best practices when Google recommends

DALE ASKEY
Associate University Librarian, Library and Learning Technologies and Administrative Director, Lewis & Ruth Sherman Centre for Digital Scholarship
McMaster University, Hamilton, ON, Canada

KENNING ARLITSCH
Dean of the Library, Montana State University, Bozeman, MT USA

Abstract

Google is the single largest driver of traffic to library websites and digital repositories, and librarians would do well to listen when the search giant reveals information about its practices or makes recommendations. Recently, Google announced that it would begin to favor websites that use the secure hypertext transfer protocol (HTTPS) in its search results rankings. HTTPS encrypts data transmission and one of Google's stated reasons for this change is to help make the Web safer and minimize data theft. Similar announcements by Google have sometimes been ignored by librarians, to the peril of the visibility and use of library products and services on the Web.

Keywords

HTTPS; Google; search engine results rankings; search engine optimization; privacy; data security; IT skills

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

Introduction

From time to time Google announces tactical changes to carrying out its core mission of "organizing the world's information and making it universally accessible and useful" (Google, Inc., n.d.). While its methods for crawling and indexing the Web remain a closely guarded secret, occasional pronouncements by insiders, speculation, and testing by search engine optimization experts have yielded lists of approximately two hundred "signals" that influence the algorithms that make Google's search engine the most popular in the world (Dean, 2014). In a break with its previous practices the company recently announced that it would now favor one such signal (HTTPS), and while its immediate impact will be small libraries would be well advised to pay attention and begin planning accordingly.

Similar announcements made in the past have had dramatic effects on the traffic that Google directs to library websites and digital repositories. In 2008 Google quietly announced that it would no longer support the Open Access Initiative Protocol for Metadata Harvesting (OAI-PMH) to harvest metadata from library repositories, stating that the resource requirements simply weren't worth the return (Mueller, 2008). Digital repository managers who had relied on OAI-PMH to get their metadata into Google's index should have been shocked and dismayed, but the announcement went largely unnoticed in the library community until it became apparent that traffic to most digital collections was suffering. The lack of support for OAI-PMH by Google was a factor in this low traffic; while librarians were busy preparing their repositories for the OAI-PMH bitstream they were not focused on more common search engine optimization practices that facilitate search engine crawlers.

In 2011 Google Scholar announced that institutional repositories (IR) should "use Dublin Core tags as a last resort" because the schema isn't appropriate for describing scholarly works (Google Scholar, 2011). The Dublin Core definition doesn't include unambiguous fields for each part of a bibliographic citation, especially elements like volume, issue number, first page, last page, and a consistent field where a URL to the publication PDF can be entered. Nor are there appropriate fields that distinguish an article from a preprint, a dissertation from a thesis, or a book chapter from a book. In short, Dublin Core cannot provide the necessary bibliographic information that Google Scholar gets from commercial publishers through other schemas and that it needs to deliver accurate citations to its users. Subsequent research revealed that Google Scholar's dismissal of Dublin Core is a major factor in the poor visibility of open access IR content because most had defaulted to Dublin Core for their metadata schema (Arlitsch & O'Brien, 2012).

HTTPS as a ranking factor

The Google HTTPS announcement came in the form of an understated August 6, 2014 post (Bahajji & Illyes, 2014) on Google's Webmaster Central Blog, which the company bills as "official news on crawling and indexing sites for the Google index." In this post Google announced that while traffic being served via HTTPS had previously been slightly disadvantaged for ranking purposes, the company now intends to reverse its practice and will slightly favor sites using HTTPS encryption.

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

This announcement should have come as no surprise to those with a sharp eye for details. Google has in recent years moved most of its core services to HTTPS, including its basic search engine and more sensitive services such as Gmail and Drive. The post notes that they also announced their plan at Google I/O 2014 and that their action is part of a broader effort toward keeping "everyone safe on the Web." Helpfully, the post even lays out some basic suggestions for implementing HTTPS and points toward more fulsome documentation in Google's Help Center (Google, Inc., 2014).

The general reaction in the industry was marked by acceptance and agreement. There was some grumbling about costs and technical issues, but most commentators seem to find it a useful step in the evolution of Web practice. The Backblaze blog characterized efforts to create a more secure site as "providing a better user experience was worth the risk of lost rankings … instead of getting punished, Google actually changed their tune and might end up giving us a small reward" (Budman, 2014). TechCrunch noted that "the revelation that the NSA has been tapping the cables, so to speak, to mine user information directly has prompted many technology companies to consider increasing their own security measures," and that "Google is helping to push the rest of the Web to do the same" (Perez, 2014).

Alas, in library circles the announcement seems to have gone largely unheeded. No major library news source covered this announcement. Even on technologically-progressive lists such as code4lib or library technology news blogs such as LITA's, the switch failed to generate any discussion. In a profession that is otherwise fairly attuned to the comings and goings of Google--there are, to name one example, myriad articles in our literature discussing Google Glass--this silence is unsettling. It does however, fit the pattern described at the outset of this article, even though the changes involved in this case are far less difficult to implement than those required to address Google's changes to its harvesting practices and metadata preferences.

HTTP vs. HTTPS

For those familiar with the technical arcana of running a complex website, the two dominant transfer protocols for Web-delivered content have been well known for years. The hypertext transfer protocol (HTTP) is as old as the Web itself, with the first version resulting from a 1991 proposal by Sir Tim Berners-Lee (Berners-Lee, 1991). In 1995, Netscape extended the properties of HTTP to include encryption, resulting in the establishment of hypertext transfer protocol secure (HTTPS). The new standard layered HTTP with a security method known as secure sockets layer (SSL), which ultimately gave way to TLS (transport layer security) encryption, although SSL is still commonly used as a shorthand for secure Web transfers, not least by various security certificate resellers (sslcheap.com, ssls.com, et al.).

The key benefit of HTTPS over HTTP is simple: data sent between the browser and the server is encrypted at both ends before transmission, making it far less susceptible to man-in-the-middle attacks or packet sniffers. Hacking technologies that make it easy to capture

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

unencrypted data are continually under development, as with the Firefox Firesheep add-on that was released in 2010. “Firesheep made sniffing Web traffic point-and-click simple — it was suddenly dead easy to do something that used to require a good bit of hacking knowledge” (Gilbertson, 2010).

Website designers of the 1990s who raised the possibility of HTTPS with systems administrators often met with mini-sermons about the increased server-side overhead, which would surely have apocalyptic results. Such concerns are still regularly voiced in 2014, often stated axiomatically without reference to actual figures or substantive concerns. While there is, in fact, a performance hit, the degree to which this impacts traffic has been studied many times and found to be nominal in terms of user experience.

As early as 1998, three NYU researchers concluded that “encryption ... increase[d] the response time of two popular Web servers ... by at most 22%,” adding that they considered the delay “moderate” and encouraged “websites to routinely use secure communications,” language that is strikingly prescient given that it came 16 years before Google’s recent announcement (Goldberg, Buff, & Schmitt, 1998). In the intervening years there have been myriad improvements in all aspects of Web technology, from the server where content resides to the networks that carry it, and the devices and software that request the data. A 2011 experiment conducted by a Dutch graduate student demonstrated, for example, that Web servers based on Apache--globally the most common platform--see only a 12-15% degradation in response time with TLS enabled, with the range dependent on the encryption scheme (Kleppe, 2011). His study also showed only 3% and 0.5% increases in inbound and outbound network traffic, respectively. While these are noticeable and measurable differences, unless a library site is running on poor hardware over drastically throttled networks, the addition of a secure protocol should not represent significant challenges.

There are two other technical drawbacks to HTTPS that are frequently cited in online discussions. The first is the lack of caching with HTTPS. Caching compensates for the latency inherent in long-distance networks by allowing servers between the host and the user agent to store (cache) elements of sites. This allows the user agent (typically a Web browser) to construct a page without having to retrieve all of the content from the remote host, which could be on the other side of the planet. While this could be of slight concern, most users of a given library are likely in close proximity (in networking terms) to the host server; moreover, constant improvements in bandwidth render the gains made through caching far less critical for response time.

Another commonly voiced concern is the inability to use HTTPS in a shared hosting environment, i.e.- when running a website from a typical commercial host where a physical server hosts hundreds or thousands of sites at a single IP address. Few libraries of any significant size would attempt to run their sites from such a platform, and this type of Web architecture is seldom found on university campuses.

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

Why adopt HTTPS for a library site?

There are many inherent advantages to running a site over HTTPS, not least in organizations such as libraries, which take a strong interest in privacy and the right of users to conduct research without fear of eavesdropping. These advantages stem largely from three notions.

1. Website creators are prone to making mistakes, and may not encrypt pages where they should. Library websites are often the domain of a loosely regulated yet large segment of the staff who possess a wide range of technical abilities and understanding, and this represents a fairly significant risk. Site managers would have to regularly conduct audits to ensure that any page where a user can submit information has been properly encrypted, an unlikely scenario.
2. The other side of the coin is that no site owner can control the behavior of users. For example, it may seem unnecessary to run HTTPS on a site that has a Web form to enable users to submit suggestions or comments. Textual warnings that visitors should not submit any personal information or passwords via such forms are common, but intuition, experience, and research all tell us that people routinely disregard such common-sense warnings. Using HTTPS negates this risk.
3. The third reason emerges from our professional ethos that users should be able to conduct their research ‘anonymously,’ i.e.- even though we must, for a variety of contractual and policy reasons, authenticate users before they can use certain resources, the nature and topics of their research is entirely their business. Many libraries commonly allow non-HTTPS access to a wide range of search tools, which means that search queries and results are passing in clear text between the server and the browser. This should offend our sense of privacy and lead us to take action to prevent this form of digital surveillance. Given the Edward Snowden revelations, it is clear that this type of traffic sniffing is far from just a theoretical concern.

The issue of security is also an opportunity for libraries to demonstrate leadership and foresight in the technical arena, not just on our campuses, but on the broader Internet. Research conducted by Douglas Stebila at the University of Queensland in 2009 clearly articulated the woeful state of Internet security and the prevailing haphazard approach to Web encryption. His work clearly demonstrated that even major Internet sites, including financial institutions, often fail to observe best practice with regard to the proper encryption of login credentials. Any experienced Web worker will note that his work merely puts the numbers to what we all see via direct observation, which is that HTTPS is poorly understood by users and that matters are not helped by sloppy implementations (Stebila, 2010). The risks of poor encryption are not well understood, and it is logical to assume that many sites will continue to show less than optimal handling of sensitive information of various types. Given the relative simplicity of applying HTTPS to an entire site--which essentially transfers the burden of security from people, whether users or content creators, to machines that we can scale to address any performance issues--this is an area where library practice could be exemplary. The library would also likely be one of the first entities on any given campus or within an institution that would make such a move, which represents an opportunity to position the library as a security-conscious organization that

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

puts the safety of users ahead of the ‘health’ of machines. The side benefit is to demonstrate technology leadership and savvy to the campus, rather than being a late adopter. Put plainly, nothing is more satisfying than replying to a campus IT security dictum with a casual “oh, we implemented that months ago.”

Aside from a marketing opportunity that highlights leadership, libraries could also incorporate HTTPS implementation expertise into services they offer. An earlier column in this journal described “new knowledge work” based broadly on search engine optimization and semantic Web services that libraries can offer to other organizations on their campuses, and that suite of services can be complemented by helping other sites implement HTTPS (Arlitsch, Obrien, Clark, Young, & Rossmann, 2014).

Last, but not least, there is the “Google” argument. For better or worse, Google sets the tone for the entire Web, so resisting them on this issue seems futile. While Bing has announced that for now they will not follow Google’s lead (Newman, 2014), this is likely more a case of corporate rivalry than a sensible decision. Google’s announcement has already spurred many sites to move to HTTPS, and as momentum builds, others will follow suit. Yahoo encrypted its Webmail earlier this year, and Facebook and Twitter have encrypted their sites (Tung, 2014).

Downsides to HTTPS

There are, to be fair, two issues related to HTTPS that Web administrators must recognize and address. The first is a cost issue. The uninitiated may operate with the mistaken assumption that security certificates entail significant expense. This impression is not helped by articles on sites such as Ars Technica that make loose allusion to “the high cost of secure certificates” and claims such as “obviously that's not as much of an issue with large Web services that have millions of dollars,” without bothering to note that there are a wide range of certificate types and price points (Gilbertson, 2010). The price corresponds to what one intends to do and the level of trust required, not necessarily the security nor the type of encryption.

In brief, there are three types of security certificates: domain validation (DV), organization validation (OV), and extended validation (EV) (Arnbak, Asghari, Van Eeten, & Van Eijk, 2014). While businesses such as Amazon or financial institutions have extremely high security concerns given the nature and stakes of their business, libraries typically do not engage in e-commerce nor sensitive financial transactions. The former will likely pay thousands for an EV certificate; libraries can generally safely apply DV certificates that can be purchased for as little as $20. As Arnbak’s 2014 analysis shows, there is little to recommend that libraries spend more than necessary given the current governance of HTTPS and the characteristics of the certificate market. What is critical is that traffic be encrypted, which even the most basic certificates assure.

To provide a simple example, the McMaster University Library uses a simple 128-bit encryption DV certificate to encrypt various domains through which we serve our content (main site, journals, blogs, digital collections, etc.). Most of these cost between $10 and $100 annually depending on various details. To encrypt Gmail, Google uses a certificate that provides 256-bit encryption, for which they presumably pay more than $100. Setting aside the differences in encryption--128-bit is not trivial to penetrate, and libraries are infinitely less interesting targets than Gmail--we offer our users the same experience as does Google: bidirectional encryption and a clear indication in the browser that HTTPS is in use.

A recently published analysis of HTTPS by Arnbak and peers that clearly lays out the flaws in the HTTPS governance and implementation models describes the other issue one must acknowledge. While their report makes clear that there is need for reform, they do not question the basic premise that Web traffic benefits from encryption. Their intent is to encourage sensible technical solutions and a more stringent certificate authority (CA) regime that moves the market past a critical “too big to fail” issue, where massive CAs have such significant market share that when breaches do occur it is impossible to revoke certificates without causing chaos on the Web. At the end of their withering critique, they underscore again that while they find the governance model and market severely out of step with current reality, the need for reform is driven by the fact that HTTPS is “an absolutely critical technology used every second of every day by every Internet user” (Arnbak et al., 2014). This means that libraries should not avoid HTTPS, but rather stay up to date with changes and revisions in best practices for Web encryption.

Practical Tips for Implementing HTTPS

The technical details for applying a security certificate to a domain vary based on the systems in use, so a guide would require multiple scenarios that exceed the scope of this column. Nevertheless, there are several key points worth noting when implementing HTTPS.

First, as previously discussed, costs should be kept to a minimum by shopping around. The security certificate market is large, global, and competitive, and as Arnak and colleagues note, there is little to recommend one issuer over another and prices do not necessarily correspond to any real value, but rather merely perceived value (Arnbak et al., 2014). Given this state of affairs, it seems prudent to suggest that price shopping is a wise tactic. There are many certificate resellers that bundle and discount certificates, which creates opportunities for anyone inclined to hunt around for the best value. While the McMaster University Library tends to use Comodo-issued certificates, we rarely purchase these from Comodo, but rather through resellers such as ssls.com. Brand and vendor allegiance really do not have much value on the HTTPS market.

Another cost-saving maneuver involves the use of so-called wildcard certificates, which can be applied to numerous subdomains. In other words, a certificate issued for *.somelibrary.org would work equally well for blog.somelibrary.org, branch.somelibrary.org, etc. Wildcard certificates do come at a higher price, but when compared to the cost and hassle of securing individual subdomains, they may make good economic sense. There are purists who look askance at wildcard certificates as being too generic and not capable of extended validation. Given the flaws in HTTPS governance and implementation, such concerns seem relevant only for organizations that have critical needs for security and confidentiality and are likely targets for hostile and persistent attacks. Using a wildcard certificate in a library could hardly be construed as cavalier.

Lastly, a common pitfall to avoid with security certificates is the mixing of HTTP and HTTPS content on a single Web document. This often occurs with image files such as logos, which are called and inserted from an external store rather than from the server issuing the HTML document. This leads to something most of us have seen in various browsers, where an alert appears in the address bar or status bar indicating that some content on the page originated from an insecure source. While the actual security concern is generally trivial, the alert makes the site administrators look incompetent and undermines the confidence of users who notice such details. The easiest way to avoid this, of course, would be to take the recommendation Google has issued and apply it. If all of the library's content is served via HTTPS, the problem is largely solved.

A Library Administration Concern

We hold forth Google's new emphasis on HTTPS as an example of larger issues that should concern library administrators. Despite the dominance of information technology in our profession, and despite the overwhelming presence of Google and other search engines as discovery mechanisms for information resources, the lack of awareness and response to these technological imperatives by librarians can be unsettling. Librarians should know about issues that relate to access of their collections, even when the access is provided by external mechanisms. The organization needs these skills, and if it doesn't have them then administrators need to find out why.

Potential long-term loss of referrals from search engines is only part of the problem that should concern library administrators. As mentioned earlier, privacy and anonymity, long-cherished pillars of library values, are equally at stake. As the deadline for this column submission draws near there is breaking news about Adobe Digital Editions (ADE), the "recommended application for patrons wanting to borrow electronic books (particularly with the Overdrive e-book lending system), because it can enforce digital rights management rules" (Gallagher, 2014). Adobe, Inc. finds itself the target of librarian attacks concerned with privacy and security as it has been revealed that "the latest version of ADE apparently sends information 'in the clear,' (that is without encryption) back to Adobe, including reader account information, device ID, and pages read" (Albanese).

Of course there is no small irony in knowing that while librarians are expressing upset at a vendor for failing to exercise caution with patron data, our own libraries have plenty of similar failures in our websites and repositories. Few libraries (our own included) have implemented HTTPS for all public websites, including discovery layers, catalog, IR, etc. In some cases we even give the illusion of security by using HTTPS-encrypted authentication that then leads right back to an insecure site that sends data in clear text transactions. We have the responsibility to

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

encrypt at all times whether we think transactions contain private (personally identifiable) information or not.

HTTPS is not iron-clad, but it's the best we've got and libraries are fortunate in that they are not currently big targets of malicious hacking. But every piece of information has potential value to a hacker, and they may use information that they gather from unencrypted data transactions to exploit other security vulnerabilities. Even the capture of a user's IP address could provide sufficient data that enables a savvy hacker to connect secure traffic with unsecured traffic, thus potentially revealing a user's identity. If in doubt, encrypt.

Summary

Google and its various domains (Scholar, Images, News, etc) drive more traffic to library websites and digital repositories than any other single source. As a result it is not only useful to incorporate search engine optimization practices that help Google to reach, harvest, and understand libraries' Web presence, but it is also important to pay attention and act accordingly when the search engine company recommends changes to website practices. While converting to HTTPS will likely pay only small dividends in terms of search engine rankings for the near future, the practice also makes sense in the larger safety and security concerns of the Web and aligns very well with traditional library concerns around privacy and anonymity. Heeding this signal from Google represents an opportunity for libraries be on the forefront of technological progress and to demonstrate leadership in an area that should come naturally to us.

Arlitsch, K., & O'Brien, P. S. (2012). Invisible institutional repositories: Addressing the low indexing ratios of IRs in Google Scholar. *Library Hi Tech*, *30*(1), 60–81. doi:10.1108/07378831211213210

Arlitsch, K., Obrien, P., Clark, J. A., Young, S. W. H., & Rossmann, D. (2014). Demonstrating Library Value at Network Scale: Leveraging the Semantic Web With New Knowledge Work. *Journal of Library Administration*, *54*(5), 413–425. doi:10.1080/01930826.2014.946778

Arnbak, A., Asghari, H., Van Eeten, M., & Van Eijk, N. (2014). Security collapse in the HTTPS market. *Communications of the ACM*, *57*(10), 47–55. doi:10.1145/2660574

Bahajji, Z. A., & Illyes, G. (2014, August 6). HTTPS as a ranking signal. Retrieved from http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

Berners-Lee, T. (1991). HyperText Transfer Protocol Design Issues. Retrieved October 13, 2014, from http://www.w3.org/Protocols/DesignIssues.html

Budman, G. (2014, August 8). SEO Serendipity: Our Road Back to HTTPS Leads to Google Love. Retrieved from https://www.backblaze.com/blog/seo-serendipity-our-road-back-to-https-leads-to-google-love/

Dean, B. (2014, August 8). Google's 200 ranking factors: the complete list. Retrieved from http://backlinko.com/google-ranking-factors

Gilbertson, S. (2010, November 29). Secure Firefox with new HTTPS everywhere. Retrieved from http://www.webmonkey.com/2010/11/secure-firefox-with-new-https-everywhere-add-on/

Goldberg, A., Buff, R., & Schmitt, A. (1998). A comparison of HTTP and HTTPS performance. *Computer Measurement Group, CMG98*. Retrieved from http://ftp.cs.nyu.edu/artg/publications/Goldberg_Comparison_of_HTTP_and_HTTPS_Performance_1998.pdf

Google Scholar. (2011). Inclusion Guidelines for Webmasters [Inclusion Guidelines]. Retrieved October 4, 2011, from http://scholar.google.com/intl/en/scholar/inclusion.html

Google, Inc. (2014). Secure your site with HTTPS. Retrieved October 13, 2014, from https://support.google.com/webmasters/answer/6073543?utm_source=wmx_blog&utm_medium=referral&utm_campaign=tls_en_post

Google, Inc. (n.d.). About Google. Retrieved October 12, 2014, from https://www.google.com/intl/en/about/

Kleppe, H. (2011). *Performance impact of deploying HTTPS* (p. 4). Universiteit van Amsterdam. Retrieved from https://www.os3.nl/_media/2010-2011/courses/lia/harald_report.pdf

Mueller, J. (2008, April 23). Retiring support for OAI-PMH in Sitemaps [Blog]. Retrieved from http://googlewebmastercentral.blogspot.com/2008/04/retiring-support-for-oai-pmh-in.html

Newman, J. (2014, October 3). Unlike Google, Bing gives no rankings boost for encrypted websites. *PCWorld*. Retrieved from http://www.pcworld.com/article/2691613/unlike-google-bing-gives-no-rankings-boost-for-encrypted-websites.html

Perez, S. (2014, August 7). Google Says Website Encryption – Or Lack Thereof – Will Now Influence Search Rankings. Retrieved from http://techcrunch.com/2014/08/07/google-says-website-encryption-or-lack-thereof-will-now-influence-search-rankings/

Stebila, D. (2010). Reinforcing bad behaviour: the misuse of security indicators on popular websites. In *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction* (pp. 248–251). Brisbane: ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1952275

Tung, L. (2014, January 8). Yahoo finally enables HTTPS encryption for email by default. Retrieved from http://www.zdnet.com/yahoo-finally-enables-https-encryption-for-email-by-default-7000024922/

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu