A Report on the Recordkeeping Implications of UCLA Faculty and Staff E-mail Outsourcing

David Isom
IS 240: Digital Records Management
Professor Jean-François Blanchette
June 8, 2015

Executive Summary

In 2009, the UCLA Email Outsourcing Task Force (ETF) began researching the possibility of outsourcing certain types of campus e-mail accounts to third-party vendors. In 2011, the ETF issued a report concluding that UCLA should begin outsourcing student accounts via Google's Apps for Education service and advised that it would be possible to do the same with faculty and staff e-mail accounts at a later point in time. In 2012, UCLA began allowing students (both graduate and undergraduate), alumni, and retirees to switch from their Bruin OnLine e-mail accounts to Google-hosted accounts, and all entering students' accounts were switched to the Google-provided service. Faculty and staff Bruin OnLine accounts were not transitioned to Google until April 2015.

Some members of faculty and staff have expressed concern with the outsourcing of campus e-mail. Members of the Department of Information Studies, in particular, were concerned with the recordkeeping implications that this transition could impose. As a result, this report was commissioned to examine the possible consequences entailed by the outsourcing of certain faculty and staff e-mail accounts. In preparing this report, we spoke with staff involved in the decision to outsource campus e-mail and faculty who have voiced concerns about the practice. We considered the recordkeeping implications from the perspectives of records as documents, the workflow of the records created in e-mail systems, issues of legal compliance, and the affective dimension from the perspective of users of UCLA's faculty and staff e-mail services.

Our conclusions are that such concerns are largely unwarranted. While faculty and staff are right to be concerned about possible privacy issues involved in using outsourced e-mail—Google has now acknowledged that even though it displays no advertisements in Google Apps for Education e-mail accounts, it nonetheless scanned the content of e-mail message in such accounts for data acquisition purposes until 2014 (and continues to do so in the commercial version of Gmail)—the use of an outsourced e-mail provider does little to change UCLA's recordkeeping methods and obligations. Perhaps most importantly, the outsourcing of e-mail does not change UCLA's legal obligations under the California Public Records Act (CPRA), and statutes such as CPRA and the Family Educational Rights and Privacy Act (FERPA) do not prevent UCLA from outsourcing faculty and staff e-mail accounts.

Introduction

E-mail is an essential communications tool in today's world—both inside and outside of academia, and for both personal and professional correspondence. For the user, it is extremely inexpensive (with e-mail service often provided free of charge or as a bundled service requiring no additional payment, as with e-mail provided by Internet service providers) and requires no payment on a per-message basis; it is highly adaptable, having evolved from allowing plain-text only to supporting styled text in a multitude of scripts and allowing for digital files to be sent as attachments. Its asynchronous nature—not requiring sender and recipient to be connected simultaneously, as with conversations (either in person or by telephone) or instant messaging—allows users greater flexibility in drafting replies and in dealing with correspondence at their convenience.

Yet few employees today view work e-mail favorably. Workers report that e-mail consumes a significant portion of their workday—a McKinsey study from 2012 claims that the average worker spends 28% of his working time managing e-mail,[1] and research suggests that users attribute feelings of stress and "overload" to managing e-mail.[2] Some employers in the private sector have attempted to remedy the feeling of being always-on-the-clock created by e-mail: Volkswagen AG has restricted the sending of company e-mail to employees using mobile devices to thirty minutes before and after normal working hours.[3]

[1] McKinsey and Company, "The Social Economy: Unlocking Value and Productivity Through Social Technologies," July 2012, http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy, par. 5.

[2] Stephen R. Barley, Debra E. Meyerson, and Stine Grodal, "E-mail as a Source and Symbol of Stress," *Organization Science* 22, no. 4 (2011): 888.

The UCLA Office of Information Technology created an Email Outsourcing Task Force (ETF) in July 2009, charged with evaluating various options for reducing the cost of providing e-mail services to students, alumni, and retirees; in addition, "the Task Force was asked to be mindful of the future possibility of outsourcing faculty and staff email."[4] Based on an analysis of available e-mail service providers—including solutions from Google Apps for Education, Microsoft Live@edu, IBM, and Zimbra[5]—and surveys of various categories of university e-mail users (undergraduates, graduates, and faculty), the Task Force recommended in 2011 that undergraduate, alumni, and retiree e-mail accounts be migrated to Google in place of the campus' own Bruin OnLine system.[6] The Google-hosted service—a UCLA-branded version of the company's Google Apps for Education,[7] which includes a version of its Gmail e-mail service—went live in 2012, with newly-admitted students required to use the service in place of Bruin OnLine; existing students, alumni, and retirees were permitted to switch as well,[8] though the Bruin OnLine service for this class of users was not discontinued until March 30, 2015.[9]

[3] Hayley Tsukayama, "Volkswagen Silences Work E-mail After Hours," *Washington Post*, December 23, 2011, http://www.washingtonpost.com/business/technology/volkswagen-silences-work-e-mail-after-hours/2011/12/23/gIQAz4HRDP_story.html, par. 2.

[4] University of California, Los Angeles, "Student and Alumni E-mail Outsourcing Task Force (ETF) Report," April 2011, http://restricted.ats.ucla.edu/studentetf/email-outsourcing-report-final.pdf, 3.

[5] Ibid., 15.

[6] Ibid., 4.

[7] "Google Apps for Education," Google Inc., accessed June 8, 2015, https://www.google.com/work/apps/education/.

[8] Jillian Beck, "Hundreds Switch From Bruin OnLine Email Services to Google Apps for UCLA," *Daily Bruin* (Los Angeles), September 17, 2012, http://dailybruin.com/2012/09/17/hundreds-switch-from-bruin-online-email-services-to-google-apps-for-ucla/.

Some faculty and staff were affected by this decision and are now using Google-outsourced e-mail for their @ucla.edu e-mail accounts. Departments are free to continue providing their own e-mail services on their subdomains (for example, the Henry Samueli School of Engineering and Applied Science uses the domain @seas.ucla.edu)—or to arrange their own outsourced e-mail solution, as the School of Law has done[10]—but employees in departments not making such arrangements used Bruin OnLine for campus e-mail.

The ETF Report was primarily concerned with evaluating the possibility of outsourced e-mail from budgetary, feasibility, and popularity perspectives before deciding whether to proceed with an outsourced e-mail solution. In contrast, this report was commissioned by the UCLA Academic Senate after the outsourcing of campus e-mail had already begun, and is concerned with the recordkeeping implications of outsourced e-mail (including the life cycle of the digital records generated by e-mail systems and compliance with laws such as the California Public Records Act which can require disclosure of certain faculty and staff e-mail messages), and the affective dimension of using outsourced e-mail systems.

[9] "4/13/2015: Bruin OnLine Email Servers Retired," UCLA Bruin OnLine, April 13, 2015, https://www.bol.ucla.edu/alert/20150413.html.

[10] "LawNET is now on Gmail," UCLA School of Law, accessed June 8, 2015, https://lawnet.ucla.edu.

1. The Life Cycle of E-Mail Records: The Document Perspective

From their initial conception, the records created in e-mail systems are electronic. Users compose e-mail messages in e-mail clients (either dedicated e-mail clients on computers and smartphones, such as Microsoft Outlook and Apple Mail) or in Web clients (i.e., directly on the Gmail Web site). Drafts of the messages may be saved on the user's computer or remotely, again depending on whether the user is using a dedicated e-mail application or a Web client. Once the user sends the message, the message is routed from the user's outgoing mail server to the recipient's incoming mail server, typically with numerous intermediate steps in between. The recipient views the message using a dedicated e-mail application or a Web client.

The invisible transit of e-mail means that the electronic trails they leave behind are not always obvious. To be sure, most users are aware that outgoing e-mail messages are typically saved in a "Sent Items" folder and know that the recipients of messages they send can save them indefinitely, forward them to other recipients, or cut and paste the content of the messages into other applications or post them on Web sites—but the particular route through the Internet that the message took (including intermediate servers through which pieces of the data were transported)—is not easily determined, if even possible at all.

In addition, for many e-mail accounts (including all Gmail accounts, such as UCLA's hosted e-mail), the user's e-mail messages are stored on the mail server. In this arrangement, the "master copy" of the user's folder structure and e-mails are stored server-side, and any copies stored by the user's mail client are simply caches for performance or offline reading of messages; when the e-mail client connects to the server, any changes made on the server will be read and the local copy will be updated to reflect them.

While the user has some control over what messages are kept in his e-mail account—users can flag, file, and delete messages in accordance with whatever stratagem they choose—they have no control over what the e-mail service provider does with the e-mail records stored on their servers. In the case of UCLA's outsourced version of Gmail, for example, neither the accountholders nor UCLA administration has access to Google's servers on which the e-mail is stored. Google itself does have access to these e-mail records; e-mail in standard Gmail accounts is routinely scanned for Google's data acquisition purposes, and while the company has stated that it discontinued scanning e-mail messages in Google Apps for Education Gmail accounts, it acknowledged that it had formerly done so.[11] Moreover, it is not inconceivable that Gmail records could be compromised by "phishing" scams, coordinated cyberattacks, or even employee spying.[12] E-mail stored on mail servers is typically not encrypted, making it more susceptible to being read by a rogue employee.[13]

Data on mail servers is routinely backed up, though the user typically has no control over the details of the backup procedure nor any knowledge of the process. For example, Gmail for UCLA users have no knowledge of how often Google backs up the mail data, the physical location of any of Google's servers, the particular type of storage mechanism used (hard drives, solid state drives, or magnetic tape). Users do not know what country their data is stored in;

[11] Benjamin Harold, "Google Under Fire for Data-Mining Student Email Messages," *Education Week*, March 13, 2014, http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html.

[12] In 2010, Google fired an employee for reading e-mail messages in some of his acquaintances' Gmail accounts; Robert Galbraith, "Google Hit With New Privacy Problem, Fired Engineer," *Reuters*, September 15, 2010, http://www.reuters.com/article/2010/09/15/us-google-worker-idUSTRE68E53R20100915.

[13] Some small, specialized e-mail providers do encrypt mail stored on their servers and use it as a selling point for their services; see, for example, ProtonMail (http://www.protonmail.ch) and Posteo (http://www.posteo.de).

Google does not offer Apps for Education customers the option of choosing exclusive hosting on servers in the United States, even as a paid option.[14]

[14] Julie Austin, Student and Alumni E-mail Outsourcing Task Force Project Co-Chair and Director of UCLA SEASnet Computing Facility, in discussion with the author, May 6, 2015. Ms. Austin stated that she would have been interested in such an option if Google offered it.

2. The Life Cycle of E-Mail Records: The Workflow

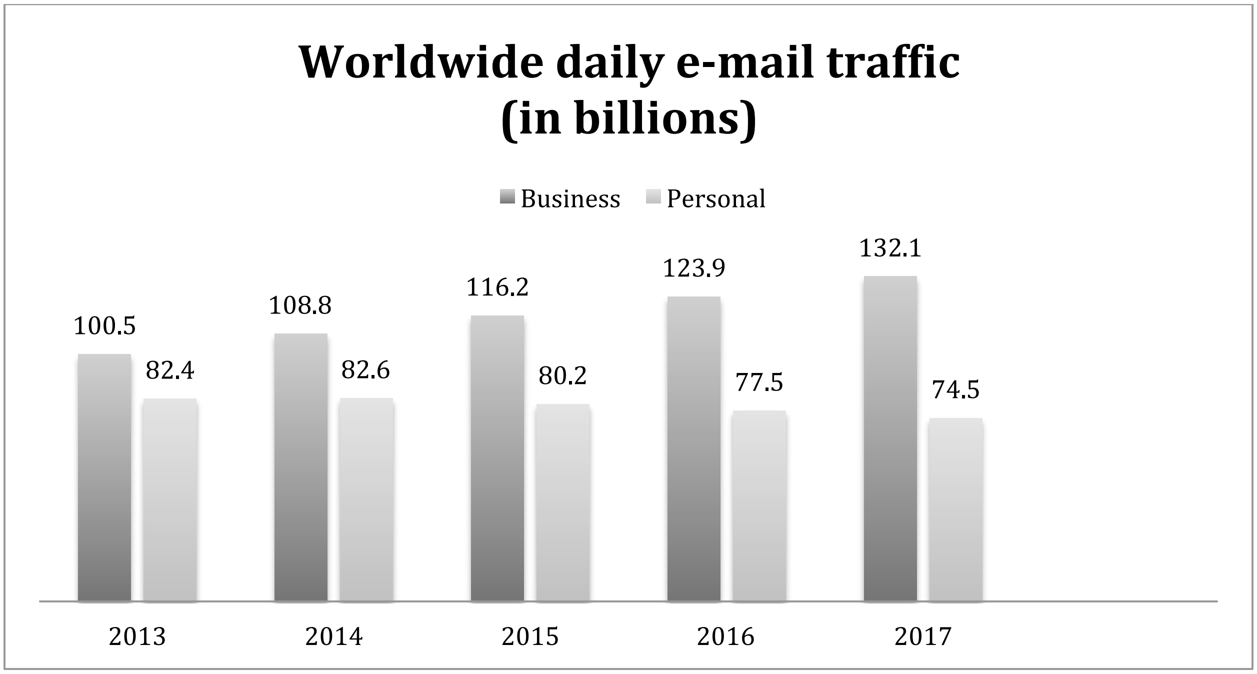
As noted above, e-mail is a major communications platform in both private- and public-sector jobs today. Indeed, it is nearly-ubiquitous in an office environment, having supplanted or displaced other communication methods, such as letters, memoranda, and the telephone. But its use is hardly confined to business environments: e-mail is widely used for personal correspondence, as well. The importance and popularity of e-mail is difficult to measure, but an Ipsos/Reuters poll in 2012 claimed that 85% of the world's Internet users used e-mail;[15] a 2014 report from the Radicati Group estimated that there are some 3.9 billion e-mail accounts in the world, with 108.8 billion business e-mail messages and 82.6 billion personal e-mail messages sent daily.[16] Radicati expects business e-mail volume to increase and personal e-mail volume to decrease in coming years (see chart on page 11).

The growth in the use of business and personal e-mail has been accompanied by a blurring of professional and personal boundaries in two respects. Firstly, many users prefer to use a single e-mail account for the sake of simplicity. Indeed, it can be inconvenient to maintain multiple e-mail accounts; if a user is trying to find a particular e-mail message that he vaguely recalls, it takes more time and effort to search two or more accounts than it would a single account. Moreover, some e-mail messages (perhaps a personal invitation to another faculty member) may blur the lines between professional and personal, thus it is unclear which e-mail

[15] Patricia Reaney, "Most of World Interconnected Through Email, Social Media," *Reuters*, March 27, 2012, http://www.reuters.com/article/2012/03/27/net-us-socialmedia-online-poll-idUSBRE82Q0C420120327.

[16] Mathias Brandt, "Private Email Traffic is Declining," *Statista*, February 7, 2014, http://www.statista.com/chart/1872/number-of-emails-sent-and-received-each-day/. Radicati predicts a decrease in the volume of personal e-mail due to the rise of new communication platforms such as social networks and instant messages.

account should be used. Finally, maintaining a separate list of contacts for each e-mail account may be tedious.



Data courtesy Statista/The Radicati Group.

The ascent of e-mail has also blurred business and professional boundaries by allowing work to intrude further than ever into employees' personal place and time. Whereas in the past an employee could not answer a business telephone line if not at work, newer communication platforms such as e-mail allow a worker to send and receive messages quite easily from any location with an Internet connection. This is especially the case when accessing e-mail via smartphones, which enable users to send and receive e-mail wherever they go.

Some UCLA faculty members have expressed concern with such encroachment into their personal time. Professor Rob Rhoads of the Department of Education expressed frustration with the personal demands that work e-mail places on him; he feels obliged to respond to e-mail from students as quickly as he can, for example, but this means that he has little choice but to access his e-mail when he is not on campus.[17]

Outsourcing faculty and staff Bruin OnLine accounts to Gmail has led to little, if any, change in how e-mail fits into their professional lives. While UCLA no longer is responsible for maintaining all of the mail servers used by students, alumni, retirees, faculty, and staff, there is no evidence that this has altered the way that these groups fundamentally use e-mail. The uses of business e-mail and its encroachment into employees' personal lives is no different when the mail server is operated by UCLA itself or by an outside vendor.

[17] Professor Rob Rhoads, UCLA Department of Education, in discussion with the author, May 5, 2015.

3. Compliance

As employees of the State of California, UCLA faculty and staff fall under the requirements imposed by the California Public Records Act (CPRA).[18] First passed in 1968 and modified as recently as 2013, the CPRA was motivated by the belief "that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[19] The CPRA defines "public records" as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics"[20] and states that "[p]ublic records are open to inspection at all times during the office hours of the state or local agency and every person has a right to inspect any public record," except as otherwise provided.[21] Public agencies—including UCLA and other public colleges and universities in California—are required to disclose requested records within 10 days, though there are provisions for extensions under certain conditions.[22]

The scope of the CPRA is expansive. While certain types of documents are specifically excluded from public disclosure—including but not limited to "[p]reliminary drafts, notes, or interagency or intra-agency memoranda"; "[r]ecords pertaining to pending litigation to which the public agency is a party"; and "personnel, medical, or similar files, the disclosure of which

[18] Cal. Gov. Code § 6250 et seq.

[19] Cal. Gov. Code § 6250.

[20] Cal. Gov. Code § 6252(e).

[21] Cal. Gov. Code § 6253(a).

[22] Cal. Gov. Code § 6253(c).

would constitute an unwarranted invasion of personal privacy”[23]—the language of the statute suggests that suppression of records under the CPRA is the exception, and disclosure the general rule.

While a full discussion of how the CPRA affects faculty and staff generally is beyond the scope of this report, its impact on e-mail should be examined. Nothing in the language of the statute itself specifically exempts e-mail from disclosure; indeed, the CPRA states that it applies to any “writing containing information relating to the conduct of the public's business”;[24] it further defines a “writing” as

> any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.[25]

On its face, then, the CPRA would appear to require the disclosure of faculty and staff e-mail messages should they be requested. The CPRA exempts “personal information” from disclosure, but defines the term narrowly:

> “Personal information” means the following information related to an individual that is maintained by a public agency: social security number, physical description, home address, home telephone number, statements of personal worth or personal financial data filed pursuant to subdivision (n) of Section 6254, personal medical history, employment history, electronic mail address, and information that reveals any electronic network location or identity.[26]

E-mail of a strictly personal nature sent through campus e-mail accounts thus is not explicitly denoted as a type of “personal information,” provided that it does not reveal an e-mail address or

[23] Cal. Gov. Code § 6254(a)-(c). For additional exemptions, see § 6254 generally.

[24] Cal. Gov. Code § 6252(e).

[25] Cal. Gov. Code § 6252(g).

[26] Cal. Gov. Code § 6254.18(b)(2).

network location (such as an IP address). While such information is readily apparent in e-mail headers, it would be trivial to redact such information to comply with the CPRA, and faculty and staff therefore should operate under a presumption that any e-mail sent from a UCLA e-mail address might be subject to disclosure under the CPRA.

The matter is far from settled, however. While the language of the statute itself does not specifically exempt such e-mail and while we are aware of no court cases ruling on the issue, it seems unlikely that a court would compel disclosure of strictly personal e-mail messages even if sent from UCLA e-mail addresses. Moreover, UCLA's Academic Personnel Office (APO) has taken a strong stance against broad disclosure under the CPRA, in response to perceived "onerous, politically motivated, or frivolous requests" which "may inhibit the very communications that nourish excellence in research and teaching, threatening the long-established principles of scholarly research."[27] Moreover, the APO contends that "[e]mail communications that are wholly personal in nature do not relate to the conduct of the university business and, thus, are not 'public records'" under the CPRA.[28]

Professor Christopher Kelty, who holds joint appointments in the Institute for Society and Genetics, the Department of Information Studies, and the Department of Anthropology, has spoken of the "chilling effect" that the potential of disclosure under laws like CPRA can have on faculty at public universities like UCLA: "If you are the kind of scholar that knows about this . . .

[27] "Statement on the Principles of Scholarly Research and Public Records Requests," UCLA Academic Personnel Office, September 2012, https://www.apo.ucla.edu/resources/academic-freedom, "Preamble."

[28] University of California, Los Angeles, Academic Personnel Office, "Faculty Guide to Public Records Responses," September 2012, https://www.apo.ucla.edu/resources/recordrequest, 2.

it does change your practice with colleagues: 'Should I write this email, should I keep this email, should I delete this part of the email?' . . . I feel as an academic I have the right to say what I want to say. . . But (records requests are a) concern."[29]

The outsourcing of campus e-mail services to Google changes very little under the terms of the CPRA. The fact that a public institution employs a third party for a records-generating service such as e-mail does not change the institution's obligations under the CPRA. In this respect, e-mail outsourcing is no different than contracts with wired or wireless telephone providers, or with a paper records storage outsourced to a private records management company. In all of these cases, records may be kept under the control of a private company, but the obligations of the public institution are unchanged.

The only respect in which the outsourcing of campus e-mail may affect requests made under the CPRA arises with respect to the size of users' e-mail quotas. Bruin OnLine accounts were limited to 1 gigabyte (GB) of data, after which newly-arriving incoming messages were returned to sender.[30] In contrast, Google Apps for Education offers a data cap of 30 GB shared across its various components (e.g. Gmail, Google Drive, Google Docs, etc.).[31] While the amount of space available for e-mail will vary according to how much data the user saves in other components of Google Apps, 30 GB is a generous allowance by current standards and thus most users will have more space available for e-mail than with Bruin OnLine. As a result, users

[29] Kylie Reynolds, "Task Force Tackles Concerns on Public Records Requests," *Daily Bruin* (Los Angeles), February 28, 2013, par. 25, 28.

[30] "BOL Email Account Quota," UCLA Bruin OnLine, accessed June 8, 2015, https://www.bol.ucla.edu/services/accounts/quota/, par. 2.

[31] "Google Apps for Education: The Tools Your Students Want," Google Inc., accessed June 8, 2015, https://www.google.com/work/apps/education/products.html, "Inbox space for everything, and no ads."

will likely have less incentive to delete old e-mails to free up enough space to remain under quota than with Bruin OnLine accounts. More e-mail will thus remain on the server that could be required for disclosure under the CPRA.

Weighing in on compliance issues, the University of California Office of the General Counsel stated in February 2010 that it saw no legal barriers that would campuses from outsourcing e-mail services to Google.[32]

[32] UCLA, ETF Report, 18, “Regulations and Compliance,” par. 1–2.

4. Affective issues

The most significant consequences of the outsourcing of faculty and staff Bruin OnLine accounts to Google will be *affective* in nature: some users are upset with the transition of a previously-in house service being replaced with a service provided by a for-profit corporation known for aggregating and exploiting its user's data. Such unhappiness should not be casually dismissed: UCLA values the opinions of its employees, and the project will not be successful if it is unpopular. Indeed, the ETF Report noted that faculty are heavy users of UCLA e-mail accounts, using them "much more than any other account"; moreover, the branding provided by a UCLA e-mail domain was "extremely important" to faculty.[33] There will be little point in providing UCLA-branded Gmail if few faculty members end up using the service as a result of dissatisfaction with either the business agreement with Google or with the quality of the product.

Professor Rhoads expressed concerns about the arrangement in an interview.[34] Already uneasy with Google's business practices and information gathering, Rhoads worried about the possible privacy implications of relying on the company for a service that has become such a critical communications tool. As noted above, such a concern is not merely speculative, since Google acknowledged that it had in fact been scanning e-mail in Google Apps for Education accounts.

[33] UCLA, ETF Report, 18. The Report reached these conclusions from faculty interviews and surveys, with some 523 responses (from a total of 7,732 surveys sent to faculty); 77. Some 44% reported "regularly" communicating with students via Bruin OnLine e-mail accounts; a further 15% did so "occasionally"; 79. Note that these figures refer specifically to Bruin OnLine e-mail accounts, and not department-supplied accounts on unique subdomains; 74% of faculty reported using such departmental addresses to communicate with students; 18.

[34] Rhoads, in discussion with the author, May 5, 2015.

From a legal perspective, Google's former scanning of e-mails which faculty and staff exchange with students potentially raises issues under the Family Education Rights and Privacy Act (FERPA),[35] which protects the privacy of student records. As the UCLA Registrar's Office advises faculty and staff, "[p]resume that all student information is confidential, and do not disclose information without a student's consent except to University officials who have a legitimate educational interest in the information. Consult with the Office of the Registrar to understand which information the University can properly disclose."[36]

More broadly, the issue of whether it is appropriate for a public institution to contract with a private company for such an important tool is a separate question from the legal compliance issues. But the ETF Report surveys showed that only 34% of graduate students and 35% of undergraduate students reported using UCLA provided e-mail accounts, with 55% and 48%, respectively, already using Gmail accounts as their primary e-mail addresses.[37] Given such unpopularity of campus-provided e-mail accounts and the popularity of Google services in general, some on the ETF saw a switch to UCLA-branded Gmail as doing a favor to students—allowing them to continuing using a service which they preferred (Gmail) but with a UCLA domain and enhanced functionality (increased storage space and a lack of advertising, as compared to Google's standard Gmail service).[38]

[35] 20 U.S.C. § 1232g.

[36] University of California, Los Angeles, Registrar's Office, "Privacy of Student Records: Essential Information for Faculty, Teaching Assistants, and Readers," March, 2014, http://web.registrar.ucla.edu/ferpaquiz/Documents/FERPAforFaculty.pdf, par. 2.

[37] UCLA, ETF Report, 64–65.

[38] Austin, in discussion with the author, May 6, 2015.

5. Recommendations

In light of the considerations discussed in the previous sections, we advise faculty and staff to abide by the following guidelines for using e-mail:

1. Do not use UCLA-supplied e-mail accounts for personal e-mail.

While there is no doubt that using multiple e-mail accounts is less convenient than a single account, the best solution for any UCLA employee to ensure the privacy of personal communication is to employ multiple e-mail accounts: a personal e-mail account (be it from Google, Microsoft, an Internet service provider, or a specialized e-mail provider) for personal communications, and a UCLA-supplied address (either departmental or through the outsourced Gmail service) as provided by the employee's academic or business unit. In the event of compelled disclosure of work e-mail messages, using separate e-mail addresses ensures that the employee's personal e-mail messages will be safe from review. Personal e-mail addresses are widely available at no cost or for a small fee, and configuring e-mail clients on computers and mobile devices is normally a simple process; alternatively, an employee can access personal Web-based e-mail using a Web browser. Employing separate e-mail addresses also helps avoid the appearance of possible impropriety.[39]

[39] See, for example, the case of Hillary Clinton, who used a private e-mail server for all of her e-mail (both official and personal) while Secretary of State: Michael S. Schmidt, "Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules," *New York Times*, March 2, 2015, http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html.

2. Assume anything written in e-mail messages sent from a UCLA address could be made public.

While it is highly unlikely that all of the e-mail messages in a UCLA employee's account would be publicly released, it is possible that particular messages could be released under a CPRA request; messages to students or the general public could also be "leaked" by the recipient. Keeping these unlikely but possible scenarios in mind will serve faculty and staff alike in maintaining professional decorum in their work e-mails and in avoiding topics better discussed through other means of communication.

3. Use department-maintained e-mail accounts if available, particularly if discussing sensitive research data.

Faculty and staff concerned with the privacy implications of outsourced e-mail and who work in business and academic units which still provide e-mail addresses on their own subdomain (not outsourced to Google) should use such departmental accounts, rather than Google-outsourced accounts. This is particularly the case for faculty doing research with possible commercial applications, national security implications, the use of humans as test subjects, or other sensitive fields. Using departmental accounts aids compliance with regulation that may require such sensitive data to be stored on servers located in the United States (which Google does not guarantee) and eliminates the possibility of Google scanning such e-mails. Note, however, that using departmental servers does not guarantee security from cyberattacks.[40]

[40] See, for example, the recent hacking attack on the Pennsylvania State University College of Engineering, which originated in China. Nicole Perlroth, "Penn State's College of Engineering Hit by Cyberattack," *New York Times*, May 15, 2015, http://bits.blogs.nytimes.com/2015/05/15/penn-states-college-of-engineering-hit-by-cyberattack/.

4. Choose a retention policy and abide by it; should you receive a public records request, *do not delete any remaining e-mails (incoming or outgoing)*.

Faculty and staff should not feel compelled to keep all e-mail (both incoming and outgoing) simply because of the possibility of a CPRA request. However, under no circumstances should faculty and staff delete e-mail which they believe could be subject to exposure under a CPRA request. The results of deliberately destroying such records could be far worse than its disclosure.

Instead, choose a retention policy for your e-mail and consistently abide by it. In other words, if you like to have a complete record of all of your incoming and outgoing e-mail and prefer not to delete anything, feel free to do so. On the other hand, if you prefer to keep a small and tidy mailbox, deleting all messages after one or two months, you may do so as long as this method is consistently applied.

5. Notify the UCLA Records Management and Information Practices Office if you are contacted regarding a CPRA request or have questions about compliance.

Faculty and staff with questions about the CPRA should contact the UCLA Records Management and Information Practices Office (RMIP). In addition, the RMIP will handle the details of any CPRA request that is made; should faculty and staff receive notification of a CPRA request, they should contact the RMIP immediately and take no further action until otherwise directed. The UCLA Academic Personnel Office has prepared a guide for faculty explaining how to respond to CPRA requests.[41] Faculty and staff may also address compliance questions to the UCLA Office of the Campus Counsel.[42]

[41] UCLA Academic Personnel Office, “Faculty Guide to Public Records Responses.”

[42] University of California, Los Angeles, Office of the Campus Counsel. http://www.campuscounsel.ucla.edu.

Conclusion

The decision to outsource UCLA campus e-mail services was not taken lightly. This was especially the case for faculty and staff e-mail accounts, since there are additional compliance requirements not typically applicable to student e-mail and because faculty and staff voiced more concern regarding privacy aspects of an outsourced e-mail solution than did students. After researching these issues, we conclude that outsourced e-mail presents no major complications from a recordkeeping standpoint. We do not dismiss concerns about the privacy of outsourced e-mail solutions, but find that many members of faculty and staff can avoid such issues by using alternative e-mail addresses (using private accounts of their own choosing for personal e-mail, and using departmental accounts (if available) in lieu of outsourced accounts), and in following our guidelines for e-mail best practices. We advise against eliminating *all* campus-operated e-mail accounts (i.e., department-operated accounts), as certain departments' particular requirements are not met by Google Apps for Education. Finally, the question about the ethical appropriateness of outsourcing an essential communications tool is legitimate and worthy of debate, but largely beyond the scope of this report.