TOPIC:

CLOUD CONTRACTING: OUTSOURCING E-MAIL @YOURUNIVERSITY.EDU

INTRODUCTION:

In 1999, many college students received their first e-mail address when they arrived on campus. A decade later, most come to college with years of e-mail, Internet, Facebook, and other digital media experience. And today, some students choose not to use their college e-mail at all.

About five years ago, Google shocked the e-mail world by promising end users a gigabyte of storage at no cost. Until that point, free storage was measured in megabytes, and end users often hastened to delete unnecessary e-mail. At the same time that commercial e-mail has become less expensive and more user-friendly, the cost to a college of hosting e-mail accounts as an Internet Service Provider (ISP) has grown more expensive. And students, faculty and staff use e-mail differently today than they did in 1999, swapping large files and subscribing to content-heavy e-mail services.

Several well-known companies (e.g., Microsoft, Yahoo, and Google) have begun offering colleges and universities a way of dealing with some of these trends—providing e-mail to campus-based end users with a youruniversity.edu address by contract [1]. The technical and legal issues involved in such agreements can be numerous and complex. This NACUANOTE covers some of the key legal issues involved in contracting with a commercial entity providing outsourced campus e-mail.

DISCUSSION:

I. Technology

Not all colleges provide students with e-mail addresses; those that do, have traditionally done so "in-house." These colleges purchase or license a software client (e.g., Webmail, SquirrelMail, Pine, Eudora, Lotus Notes, Microsoft Exchange) and purchase and configure their own servers. The portion of the e-mail address appearing after the "@" is the domain name. The "top-level domain" is symbolized by the digits that follow the domain name and period sign. The top-level domain for colleges and university operations is ".edu." Domains for ".edu" web sites and e-mail systems are licensed through EDUCAUSE. Messages are carried using the Simple Mail Transfer Protocol (SMTP), essentially a language that allows disparate e-mail systems to communicate with each other. Incoming and outgoing mail messages are stored on either a server

and worms, as well as other banes of the Internet, such as phishing schemes (e-mails that spoof an accepted service such as a bank or credit card, requesting the end user's password, but are actually an attempt to steal that password).

Some students fully use the e-mail service provided by their college. But recently more students have chosen to forward their college e-mail to another, personal e-mail address. Colleges sometimes facilitate forwarding by giving students a choice of how they would like to access e-mail.

Another noteworthy college trend is making e-mail an official form of contact. Colleges assume that when an e-mail is sent, the student has read (and will be held accountable for reading) the content. Many campuses also send out student notifications (e.g. the annual Clery Act report) over e-mail. This approach is generally more efficient and saves money and paper. In fact, the Clery Act Handbook on Campus Crime Reporting, specifically allows notification to be sent via electronic mail [2].

When e-mail is outsourced, the college no longer maintains the servers, or purchases or leases software for end users to access their e-mail accounts. This may result in cost-savings, while maintaining many of the benefits of an in-house e-mail system, such as the ability for an end-user to read messages on a server or download the message to his or her hard drive [3]. The college can also retain the e-mail address with the college name as the domain and the .edu top-level domain. Additionally, most e-mail outsource services offer other allied services such as calendaring and document sharing programs.

II. Legal Issues

Several key legal issues exist that should be carefully considered and negotiated with potential service providers before a college outsources its e-mail.

A. FERPA

1. Student E-mails

Student e-mails (that is, e-mails sitting in a student account) are not "education records" subject to FERPA regulations because they are not “maintained" in the sense required by FERPA [4]. FERPA does not cover student e-mails, whether they are kept on the college’s own servers or outsourced to a private company [5]. But this situation changes if a student uses e-mail to communicate with or about other students during the course of part-time or work-study employment on campus. In this case, the message is an education record under FERPA, and should be treated like faculty and staff e-mails.

2. Faculty and Staff E-mails

Unlike student e-mails, e-mails in faculty and staff accounts are maintained by the college. Many of these e-mails have content that qualifies as an education record, such as messages to or from students or that contain personally identifiabl

personally identifiable information from education records [9]

no longer available to either an end user or administrator, such as deleted files. Of course, this potential failing can also occur in an in-house e-mail system. The risk is only slightly elevated with outsourced e-mail because system backups and certain types of metadata may be in the hands of a third-party and not as readily available.

Finally, when a third-party becomes the custodian of data that is relevant to litigation, that third-party itself can be the target of a court's power to require the production of all relevant evidence [17]. If a college is unable to exert sufficient control over its e-mail provider to preserve or produce relevant evidence, a court, regulator, or sometimes even a litigant can compel production of relevant evidence by subpoena. This happened, for instance, in cases involving the Recording Industry Association of America, when courts issued subpoenas to third-party colleges and universities for information related to potential copyright violations by students. But even if a party does not own or control evidence, it may have still have an obligation to give the opposing party notice of the location of that evidence [18].

Should these factors not convince an institution that a particular product gives it sufficient capabilities, many supplementary products are available to archive and backup e-mail and other data. Of course, such products come at a cost, potentially diluting the benefit of outsourcing.

C. Export Controls [19]

Outsourced e-mail is not a good primary data transmission method for researchers engaged in sensitive or highly-regulated subject matter. The United States' export control regime forbids the transmission of controlled items, software, and information to certain countries without a license. These export control prohibitions apply to controlled items even when transmitted primarily for storage or for further transmission purposes. Most e-mail providers store information in the cloud and do not limit storage or transmission to servers and systems within the United States. And it is unlikely that a provider can or will agree to limit transmission domestically because using the borderless cloud is such a fundamental part of their business model. Data encryption will probably not solve the problem, because of restrictions on the exportation of encryption technology. For these reasons, researchers working with controlled material should be instructed to use another secure means of data transmission if campus email is outsourced.

This "new" regime may not be as burdensome as it sounds. Under the so-called deemed export rules, some foreign nationals cannot be permitted access to controlled items and data even when they are in the United States [20]. Because many campus IT departments lack the necessary controls to segregate these individuals (e.g., the Russian graduate student working at the helpdesk) from data that may be subject to deemed export regulation, sending such data over institutional systems could already place the college at risk of a violation. Therefore, as a best practice, departments that tend to be subject to export control rules may already use (or should consider) alternative means of data transmission.

Strengthening the security of these transmissions is important for other reasons as well. It can provide the occasion to identify and correct inadequate controls and transmission practices involving data subject to non-disclosure agreements. Furthermore, an e-mail sent from an existing in-house college e-mail system may be stored, forwarded, or transferred through another country or on an insecure system by the recipient’s e-mail account. So, imposing restrictions on sensitive e-mail traffic may provide an opportunity to review your overall IT security.

D. Information Security / Privacy

Most of the major e-mail providers that will be considered by campuses as serious e-mail outsourcing vendors (i.e. Google, Microsoft, Zimbra, etc.) are aware of their responsibility to comply with privacy protection laws. Nevertheless, many laws covering colleges and universities require them to insert compliance guarantees in their contracts with outside vendors [21]. The applicability of these laws should be

What constitutes compliance is complicated because the standard is constantly evolving, making it impractical to specify the precise standard in the contract. But most providers already have robust protection schemes in place and one of the key advantages of outsourcing is putting another party in control of data protection. Instead of focusing on specific data protection standards, the contract should concentrate on defining “confidential data” as broadly as possible (ideally everything in every end user's account) and ensuring that the provider puts adequate resources into protecting that data. A provider's reputation and history should also be taken into account and independent audits and/or evaluations by the college's own IT professionals or consultants should be considered. At a minimum, the provider should have a solid reputation and should guarantee that it will protect the institution's confidential data, and that of its end users, to the same extent that it protects its own confidential data.

Experience teaches that compliance with applicable laws and protocols does not guarantee the safety of sensitive data. So contracts with outside e-mail providers should also address the parties' respective liability for dealing with a breach. Each party should accept responsibility for cleaning up after a breach arising out of its conduct or occurring while the data is under its control. But specifying the particulars of an acceptable response to a breach is hampered by the lack of a clear legal standard governing the breaching party’s responsibility. At a minimum, the contractual language should require that the at-fault party comply with all applicable laws.

Ideally, the contract will also require the at-fault party to promptly notify any individuals affected by a breach so that they can take steps to mitigate their exposure through credit freezes and other measures. Providers may be reluctant to agree to such required notifications because identifying and contacting affected individuals can be costly and bad for public relations. However, such notifications are generally required by state law, so it is best to prepare for them even if the contract does not require it [24]. Since most students and their parents do not distinguish between a college and its vendors, a college should contractually require the provider to seek its approval before issuing any direct communication to student and parent users regarding a breach.

E. Data Mining / Advertising

Reputable e-mail providers are also aware of the legal and policy issues associated with advertising and data mining. Colleges tend to find advertising placed in the end user’s interface display unseemly and inappropriate. And e-mail outsourcing companies may agree not to display it, if a college objects. But colleges should read the advertising portion of the contract carefully. Some contracts will exempt student e-mail but place advertising on faculty and staff email or on those end user accounts falling under a "sub-domain." For instance, if for the purpose of providing alumni with an e-mail link to their alma mater, a college were to create the sub-domain "alumni.youruniversity.edu", the alumni might be greeted by e-advertising when they logged on. If this is not desired, colleges should include these alumni end users in their primary domain, or seek to negotiate this issue with the e-mail provider.

Data mining is a separate issue. It tends to raise policy concerns among college administ TD /C.Eoru Ayo the4lngraise

H. Amendments & Termination

Generally, a college and its e-mail outsourcing partner should mutually agree to any contract amendments. But, the e-mail provider may have general use policies and notices, often embedded in URLs, that it applies to all of its end users, campus-based or not. The provider may wish to change these policies periodically without directly renegotiating with each institutional partner. In a fast-evolving area like cloud computing, allowing the provider to make these changes is not unreasonable, per se. But, contracts should require the provider to notify the college prior to any policy changes, so that the college can opt out, or in extreme cases, terminate the agreement.

E-mail providers are unlikely to allow themselves to be bound to supply free or low-cost services indefinitely p r o v i d e o b l i g (a a r

FN3. It should be noted that there is an ongoing debate about whether outsourcing of technology actually

NACUA Resources:

x NACUA Virtual Seminar, Outsourcing Email & Other Institutional IT Services: Cloud Contracting, December 10, 2009.

Additional Resources:

x David Navetta, Legal Implication of Cloud Computing – Part One (the Basics and Framing the Issues), September 12, 2009

x Tracy Mitrano, Outsourcing and Cloud Computing for Higher Education, August 14, 2009

x Educause Resources on Outsourcing

"To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve."