NACUANOTES
December 16, 2009
Volume 8 No. 4

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 maintained by the college, on the end user's personal computer, or on both. As messages and message size grows, colleges purchase additional servers, encourage deletion, use short retention periods, or some combination of these methods. The size of individual e-mail messages is also constricted by the hardware and software limitations, varying among campuses.

Most colleges purchase hardware and software that can assist in detecting and rooting out spam, viruses

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 identifiable student information. FERPA requires obtaining consent prior to sharing the content of any education record with third parties—including outside contractors—but with some important exceptions [6]. The key exception in the context of e-mail outsourcing allows the content of education records to be shared with a contractor "to whom an agency or institution has outsourced institutional services or functions [7]." Such a contractor "may be considered a school official [8]" —and thus eligible to receive certain education records without student consent—if it:

1. Performs an institutional service or function for which the agency or institution would otherwise use employees;
2. Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
3. Is subject to the requirements of [34 C.F.R.] § 99.33(a) governing the use and redisclosure of

personally identifiable information from education records [9].

Most e-mail outsourcing service providers can meet these criteria. The first one is not problematic, since the whole point is to outsource something that was previously done in-house. The second one is more difficult, but can be accounted for contractually by making clear that the college owns its data, that such data are only to be used for the purpose of providing services under the contract, and through the use of acceptable information security protocols (*see* Section D, *infra*). The third requirement can best be accounted for by having the provider explicitly agree to abide by FERPA. At a minimum, the provider must guarantee that it will not share information with a third party or use the information for purposes outside the scope of the contract—such as data mining—except with student consent, or as otherwise permitted by FERPA.

B. E-Discovery [10]

In 2006 the Federal Rules of Civil Procedure were amended to accommodate e-discovery and electronically stored information. Currently, lawyers engaged in or anticipating litigation go to their client's IT office and expect to obtain all “reasonably anticipated" discoverable information, metadata and all, on a CD or flash drive. But when the e-mail sent and received on campus is stored in the “cloud" [11], the client's IT department may not have any more access to the underlying data than a typical end user. This is not only because the IT department no longer maintains the system itself, but also because storage capacity in the cloud can be used and traded almost like a fungible commodity [12], making it difficult to trace the transmission and storage history of specific data.

This new dynamic makes lawyers uncomfortable. But the data storage differences between cloud computing and using institutional servers should not impede outsourcing. These differences merely demand that cloud computing be approached with caution. There are several reasons. First, the Federal Rules [13] do not mandate any specific technological capabilities that an entity must have in place before it can communicate and store information electronically (but it is important to check whether your state spoliation of evidence law imposes additional obligations) [14]. The Rules simply require that whatever capabilities are available for business purposes must also be marshaled to comply with discovery obligations [15].

The crucial exception to this general standard is the requirement that a college must have the ability to institute a litigation hold, freezing relevant data under its control as it exists upon a determination that litigation and/or a government investigation is reasonably anticipated [16]. Because end users are not always reliable and may even have a personal interest in thwarting a litigation hold, an institutional administrator should also have the ability to place a hold on electronically stored data, including e-mail, to guarantee the preservation of relevant information.

So, for e-discovery purposes, an institution *could* have a policy stating: all e-mails will be immediately deleted after they are read, unless a litigation hold is initiated prior to such deletion. Obviously, many other legal record-keeping requirements exist that apply to different data sets on a college campus, but it should be those requirements, rather than e-discovery concerns, that govern data-storage decisions prior to a litigation hold. Nevertheless, colleges should seek the strongest possible contractual guarantees from providers that their e-mail system will allow for the easy migration of data onto institutional servers and that the providers will support the implementation and maintenance of litigation holds. These capabilities will inevitably help colleges meet their records management obligations, even if they are not strictly necessary from an e-discovery standpoint.

The second reason that e-discovery is unlikely to be an impediment when it comes to outsourcing e-mail is that discovery is primarily concerned with the production, not storage, of a party's data. As long as all of the relevant information can be accessed and turned over to an opposing party or oversight agency, it matters little whether it is stored on a server in Bangalore or Buffalo.

Most products that colleges consider as potential e-mail systems are likely to come with reliable methods for ensuring end users can access their saved data. The important thing is to ensure that an institutional administrator has similar control. The limits to this approach surface when a litigant seeks information that is

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 carefully evaluated to ensure that the contract dictates adequate safeguarding [22] of data and institutional control [23], among other things.

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 administrators as well as legal issues about the proper use of records under FERPA. As discussed earlier, faculty, staff, and sometimes student, e-mail may be covered by FERPA. Inasmuch as the e-mail outsourcing provider is serving as a school official with a legitimate educational interest in this information [25], the contract must limit the provider's use of the information to “the purpose for which disclosure is made.” In this case, it is solely for the provision or enhancement of e-mail services, not for data mining or improving advertising [26].

F. Confidentiality

Confidential information encompasses all end user data. Any such data that is legally protected under privacy statutes should be exempt from any exceptions applied to confidential information more broadly (e.g., some information may no longer be considered confidential as a matter of contract after it is made public). The contract with the e-mail provider should bar it from using confidential data for any purpose unrelated to its contractual duties (e.g., data mining) and should require it take the most stringent information security measures available for this class of data. Most providers will want reciprocal guarantees against the use or

disclosure of their information, but public institutions should consider including an "unless required by law" provision to accommodate freedom of information laws.

G. Indemnification / Limitations on Liability

Colleges are unlikely to win any significant concessions regarding indemnification because of the negligible direct revenue stream that e-mail providers receive from hosting e-mail. That said, although e-mail is often an evidentiary tool for litigants, the actual use of e-mail itself is rarely the source of litigation because the communication itself rarely causes compensable damage. Even when it does, providers are not considered speakers or publishers of material transmitted over their systems [27]. As such, this area is not a fertile ground for third-party indemnity claims and the lack of significant indemnity protection should probably not be a major concern. And remember, with an in-house system, a college has no indemnity protection in the first place.

The best result a college can hope for may be silence on the issue of indemnity. However, if a college is contractually required to indemnify an e-mail provider it should avoid agreeing to cover attorney's fees (which can be substantial even if no ultimate liability is found), fines and penalties from regulators (which the provider is in the best position to avoid), and costs associated with an information security breach (*see* Section D, *above*), at a minimum. Most providers will seek indemnification against trademark infringement actions based on unauthorized domain names—which is reasonable.

Providers may also seek some level of protection against liability arising out of the acts of end users. This is another place that colleges should take a firm stance. As a rule, students are a group for which legal responsibility should be avoided when possible. One potential compromise is for a college to agree to require end users to indemnify the e-mail provider themselves before they receive access to an account. The typical end user of any major e-mail provider already has to "click through" their provider's Terms of Use, which include this sort of provision, so such a compromise imposes little, if any, added burden on students and faculty (most of whom already have an outside e-mail account).

As for third-party claims directed at a college, it is unlikely that an e-mail provider will contractually cede any level of protection. Here too, the best result may be leaving the contract silent and allowing common law principles to dictate responsibility. Since a college administering its own e-mail system is not shielded from third party claims, a silent contract simply maintains the status quo (or even reduces liability, since the college has less involvement and thus less exposure).

Due to the lack of a guaranteed or direct revenue stream, most providers will seek some limitations on their liability. Contractually, these limitations will often be cloaked in a three-hundred word clause that essentially limits the provider's exposure to a nominal amount. Any simplification of this clause is a victory for a college because it sets the table for honest negotiation.

One possible strategy is to propose limiting liability between the parties to the amount of consideration exchanged. This type of clause appeals to the provider because it results in very limited exposure when the services are free or low-cost [28]. However, if an e-mail provider begins to charge higher fees, or if the college contracts for additional or supplementary services, the protection afforded to the provider diminishes. Such provisions make some sense because the common types of supplementary fee-based services offered by e-mail providers (e.g., records management, archiving, enhanced security) can increase the potential harm to a college exponentially if the providers fail to meet their obligations in providing those services. That said, the potential liability will still exceed the consideration exchanged.

Another important consideration is which types of inter-party liability to exempt from the contractual limitations. Indemnification obligations, liability for breaches of information security, and liability for violations of confidentiality provisions should all be considered.

Ultimately, colleges should be aware that it is possible that an e-mail provider will insist upon significant limitations on their potential liability. But this is a perennial problem with technology-related contracts.

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 [29]. But the college must weigh its need for stability against the provider's desire to be unbound. Consequently, contracts should provide for an initial term and disallow unilateral provider termination for at least 3–5 years, barring major unforeseen impediments, such as materially adverse changes in law, insolvency, etc.

On the other hand, a college should be able to discontinue the service if it proves sub-par or otherwise untenable. It can accomplish this contractually by including a clause stating that the college is under no obligation to use the service. Tactical silence may also accomplish the same result. But a college should be able to return to hosting its own e-mail—or choose another provider, if the contract is non-exclusive—should things do not go as expected.

Considering what happens post-termination is equally important. Specifically, the contract should ensure that all necessary data migrates back safely to a location designated by the college and that the provider properly disposes of any remaining data. The college provider should also contractually require the provider to assist in the transfer process and allow the college and its users access to their data for a reasonable period of time until it is accomplished. The college's IT department can advise its lawyers regarding the amount of time that is reasonable for a full transition.

CONCLUSION:

Using free or low-cost email outsourcing services appeals to college and university policy makers who confront increasing pressure to cut costs, while maintaining, or even enhancing, these services. Often these upgraded services offer students and employees more storage, greater functionality, and improved e-mail account portability, making the outsourcing of these services an unstoppable trend. Although there are many legal issues to consider when negotiating these agreements, most of them are already familiar to college and university lawyers. Hopefully, as the service providers also gain familiarity with these legal issues, contractual negotiations will become less arduous and more routine.

FOOTNOTES:

FN1. Jeremy Caplan, *Google and Microsoft: The Battle Over College E-Mail*, TIME, Aug. 14, 2009.

FN2. *See*, THE HANDBOOK FOR CAMPUS CRIME REPORTING 12.

FN3. It should be noted that there is an ongoing debate about whether outsourcing of technology actually leads to cost saving. Often, while data is outsourced, the responsibilities of maintaining the data remain with the college. Usually, in the case of e-mail outsourcing, the college is still responsible for administering end user accounts.

FN4. *See* 34 C.F.R § 99.3.

FN5. FERPA covers student records that are maintained by the college. The college does not maintain these student e-mail records, any more than it maintains students'students' paper mail in their residence hall mailboxes, or their class notes which they keep in their school lockers. All the school is doing is providing a place where students can, if they wish, store their personal property. The view that student e-mail is not covered by FERPA is based on this theory.

FN6. *See* 34 C.F.R. § 99.31.

FN7. 34 C.F.R. § 99.31(a)(1)(i)(B).

FN8. 34 C.F.R. § 99.31. The school official with a legitimate educational interest exception to FERPA is a powerful FERPA information-sharing tool. By denoting an outside vendor (permitted under FERPA) to be a school official, any information for which that vendor has a legitimate educational interest may be shared, provided that the vendor takes the same precautions with the information that the college would take. Outside of this exception, it would be extremely difficult to share education records covered by FERPA with an outside entity.

FN9. 34 C.F.R § 99.31(a)(1)(i)(B).

FN10. *See generally* Wendy Butler Curtis & Caroline M. Mew, NACUANOTE, *Preparing for E-Discovery*, Vol. 6, No. 2 (February 2008).

FN11. The "cloud", a common metaphor for the Internet, especially when the data is stored remotely, is a current topic of discussion among corporate and educational leaders. *See, Hope or Hype on the Cloud; see also Dilbert* comic strip for November 18, 2009.

FN12. *See generally*, David Navetta, *Legal Implications of Cloud Computing - Part One (the Basics and Framing the Issues)* (September 12, 2009); *Above the Clouds: A Berkeley View of Cloud Computing* (February 10, 2009).

FN13. *See* FED. R. CIV. P., Title V.

FN14. A discussion of individual state rules is beyond the scope of this Note.

FN15. *See generally* FED. R. CIV. P. 34(a)(A), (b)(2)(e); *but cf.* Phillip M. Adams & Associates, L.L.C. v. Dell, Inc., 621 F.Supp.2d 1173, 1193–1194 (D. Utah 2009) (opining that an organization must have reasonable information management policies in order to avoid sanctions for spoliation of evidence).

FN16. *See generally*, In re NTL Securities Litigation, 244 F.R.D. 179, 198–99 (S.D.N.Y.2007); Zubulake v.

UBS Warburg LLC, 220 F.R.D. 212, 216–218 (S.D.N.Y. 2003); *see also* Goodman v. Praxair Services, Inc., 632 F.Supp.2d 494, 514–518 (D. Md. 2009) (discussing the impact of third-party control over evidence).

FN17. *See, e.g.*, In re Fannie Mae, 552 F.3d 814 (D.C. Cir. 2009).

FN18. *See* Goodman, 632 F.Supp.2d at 514–518.

FN19. *See generally* Nelson Dong & Lawrence Ward, NACUANOTE, *International Academic Travel and U.S. Export Controls*, Vol. 7, No. 10 (August 2009).

FN20. *See* 15 C.F.R. § 734.2(b)(2)(ii).

FN21. *See, e.g.,* Gramm-Leach-Bliley Act; Privacy Act of 1974; Family Educational Rights and Privacy Act; Health Insurance Portability Accountability Act.

FN22. *See* 16 C.F.R. § 314.4(d)(2).

FN23. *See* 34 C.F.R. § 99.31(a)(1)(i)(B)(2).

FN24. *See* National Conference of State Legislators, *State Security Breach Notification Laws*

FN25. *See* 34 C.F.R. § 99.31; *see also* 34 C.F.R. § 99.33.

FN26. Because of these limitations, end user data should also not be used to support advertising on the provider's other services, such as search, YouTube, news readers, Picasa, etc.

FN27. *See* 47 U.S.C. § 230(c).

FN28. Generally, the limits proposed by the e-mail provider are so low that they are essentially worthless.

FN29. Despite arguments that there is no such thing as a "free lunch," some technology theorists believe that successful digital domain companies will continue "free" access to digital content, earning their profits indirectly. *See generally* Chris Anderson, FREE: THE FUTURE OF A RADICAL PRICE (2009).

AUTHORS:

Seth F. Gilbertson, Assistant Counsel, State University of New York

Joseph C. Storch, Assistant Counsel, State University of New York

RESOURCES:

NACUA Resources:

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

Additional Resources:

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

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

- Educause Resources on Outsourcing