Wyman Miles
Mar 5
to me

So ... is your question around university surveillance and monitoring, that conducted by the commercial vendors to whom we're increasingly outsourcing our e-mail services, or what allegedly conducted by the US government? I've heard all three questions raised in different forums.

With respect to the first, I think language carries a great deal of power, particularly around sensitive subject areas. We don't do, or even use the terms, surveillance or monitoring. They imply an intent that doesn't exist in our environment.

The debate about antispam/antivirus filtering being content inspection is so tired and over that I won't belabor it here; almost everyone accepts that their e-mail is subject to electronic screening to remove virus threats and unsolicited commercial e-mail. Since the screening is done by an emotionless computer according to a specific set of known rules, it's not really a privacy issue.

The big principle is: IT does not have access to e-mail without appropriate process and executive approvals. Period.

I'd say a few broad principles apply to employee e-mail, currently hosted by Microsoft's cloud service, Office 365:

- it's university data and the university has strict policies around access to that data
- the university anticipates and does not object to a certain amount of personal use (de minimus use) of university e-mail
- Microsoft considers the data to belong to the university and will abide by a certain set of rules (more on this later)

Student e-mail is outsourced to Google but the principles are ever so slightly different:

- it's part of the academic mission and the university could, under certain emergency circumstances or legal compulsion, exert its administrative access to the e-mail
- the university realizes Google wants to mine that e-mail for the purposes of targetted advertising, but that is contractually disallowed
- Google treats the mail as belonging to the university and will abide by a certain set of rules similar to those imposed on Microsoft

So, what are our policies?

- the university has a process whereby if it is believed an e-mail account holder is in imminent jeopardy or creates a threat of bodily harm to himself/herself or others, appropriate university officials (policy and mental health services) can swiftly access e-mail without obstruction or delay
- apart from that, access to e-mail requires the approval of a university executive who has purview over the constituency in question -- Human Resources for employees, Student and Academic Services for students; these cases tend to range from administrative investigations to business continuity (need access to the e-mail to keep the work going) to deceased persons to legal inquiries. So, for example, if a faculty member dies unexpectedly, the Dean of Faculty or the VP-HR or someone of similar authority and accountability can direct IT to make the e-mail available to another person designated by the department. This is all covered under University Policy 5.5:
http://www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/mailstewardship.cfm
Cornell University: 5.5, Stewardship and Custodianship of Electronic Mail
5.5, Stewardship and Custodianship of Electronic Mail
Read more...

- last but not least, UP 5.9 (linked off the same site as above) gives IT the right to review network traffic, log data, and other non-content sources to make sure the e-mail service is working properly.

As for our providers, things get interesting there.

First off, we expect both to abide by their obligations under FERPA. We expect them to notify us when they have been asked, through legal channels, to provide account content -- provided they have the legal ability to do so. We expect them to keep the data in data centers subject to US law (data residency).

We have a risk assessment process in conjunction with University Counsel to review technical procedures, security practices, contract language, and other indicators given to us by the e-mail provider to understand the university's risk and help make an informed decision around e-mail hosting.

As for alleged monitoring by the US government, I don't have any better information than anyone else. I think it does happen, I'd like to believe under appropriate legal due process. One of the considerations we discussed before moving to O365 and Google was whether

hosting the e-mail here -- where we would simply be forced by the limits of technology to know if monitoring was underway -- outweighed the other virtues of outsourcing the mail. I think, obviously because we did outsource, that that wasn't an overwhelming argument.

Does that help?

Wy

Wyman Miles
Director of IT Security, Cornell University
wm63@cornell.edu, 607-255-8421
From: Emily Rose <rose_emily@wheatoncollege.edu>
Sent: Wednesday, March 04, 2015 11:54 AM
To: Wyman Miles
Subject: Re: Fw: Research Project Questions

Hi there!
Thank you so much for getting back to me so quickly! I'm a senior at Wheaton College in Massachusetts and for my computer science senior seminar, I'm conducting a case study on faculty and staff email monitoring in higher education. For the most part, I'm looking for information on Cornell's employee privacy policies in regards to their official Cornell email, but I'm also looking for any personal opinions/knowledge/perspective that you may have on the subject as an employee of the university. The project is supposed to be a fairly short research paper, so I don't need a ton of information, but anything you might have on hand or that may easily come to mind would be much appreciated!!

Emily S. Rose

Wheaton Equestrian Captain & Treasurer
Archives Assistant
Music, Mathematics, and Computer Science Major
Wheaton College '15

On Wed, Mar 4, 2015 at 11:24 AM, Wyman Miles <wm63@cornell.edu> wrote:
Hi!

By way of introduction, I'm responsible for IT Security and Policy here at Cornell. Between those two areas, I can (hopefully!) help answer questions about the policy issues around content inspection as well as the day-to-day practicalities of what happens here at Cornell.

Do you have a list or questions or would it be better to chat by phone?

Thanks!

Wy

Wyman Miles
Director of IT Security, Cornell University
wm63@cornell.edu, 607-255-8421
From: Barbara Friedman
Sent: Tuesday, March 03, 2015 7:24 PM
To: Wyman Miles
Subject: FW: Research Project Questions