Google Apps for Education Study Group
Report to the LCACT
1/26/2015

Introduction: In October 2013 a Study Group was called into being by the FEC with the charge of examining some of the issues associated with our transition to Google Apps for Education (GAE). Forty-three faculty had raised concerns about privacy especially but also about the commercial obligations and liabilities entailed by the College's agreements with Google. There can be no doubt that GAE offers many benefits, but there is disagreement about the balance of benefit to risk and/or cost. The Study Group was charged with the task of evaluating implications of the transition for both privacy and cost. The Study Group began its work in Fall Term 2014 staffed by Christopher Chabris [Division III], Felmon Davis [Division I], Mohammad Mafi [Division IV] and Steve Sargent [Division II].

We have reached the conclusion that a full and proper study of the issues posed in our “Mission Statement” is not possible given the limited resources of the Study Group. We will not have access to the commercial agreements with Google or the terms of the contract, so there is little we can say about “entanglements and costs (short- and long-term potentially incurred by educational institutions as they enter into commercial agreements with Google)” or aspects of “the commercial agreement(s) between Union College and Google.” These matters can be pursued at such a time as the Administration sees fit to make these details transparent, consistent with any non-disclosure agreements with Google.

The same lack of access to contract sets limits what one can say about the extent to which Google protects “customers' reasonable expectation of confidentiality” beyond what is public knowledge or the wording of their policy statements. We know for instance that Google complies with FERPA requirements on student privacy and exempts email and other contents from filtering for advertising. Furthermore, it is possible that Google, given its considerable technological clout, is a better steward of security and confidentiality against outside intrusion than the College could be, and this includes arbitrary scrutiny by law-enforcement authorities, as Google and other major corporations have demonstrated some resistance to overly broad demands for 'discovery'.

Nonetheless some concern is not unjustified: terms of contract can shift or even fail to be honored and in the breach our recourse is limited. Without knowing the terms we cannot know what aspects of data security might have been inadvertently overlooked; for instance, Google makes the assurance that “Google's customers own their data, not Google” and our data will not be sold to others for advertising purposes. But does Google generate profiles of students, for instance, to use in its own advertising to students after they graduate? Does it share these profiles of graduates (if they exist – we do not yet know) with its partners and subsidiaries, such as its

---

1 The 'Mission Statement” is appended to this document.
2 Google along with Microsoft and Apple receive a five star rating from the Electronic Freedom Foundation for protecting data from government requests including “Tells users about government data requests” and “Fights for users' privacy rights in courts;” see “Who Has Your Back?” at <https://www.eff.org/who-has-your-back-2014>.
3 See <https://support.google.com/googleforwork/answer/6056650>; on this score the same terms apply to GAE as to Google Apps for Work.
own Picasa service?

But even without answers to questions of this sort, we observe that members of the College community have different tolerance for exposure, especially perhaps our foreign students and colleagues or colleagues working in controversial subject-areas or simply those of us who want an extra layer of safety, and we see no reason why the College cannot serve a broader range of interests, and offer a broader range of services, than the present system does. Part of the charge for the Study Group is to examine these concerns and “[offer] policies to address them as completely as possible.” In this spirit we recommend that ITS offer and support additional services for securing data by way of easy-to-use and easy-to-maintain encryption technologies.

We do not pretend to be security technicians or accountants when it comes to assessing the costs of additional services. Nonetheless it seems reasonable, and in partial fulfillment of our mission, to offer some suggestions for encrypted email and storage for further study and analysis.

**Proposal #1: ITS should provide and support encrypted email service to all faculty who want it.**

The Google letter and the Memorandum of Explanation of October 2013 revealed that the privacy and security of their email communication was of concern to a significant number of faculty members. One straightforward solution is to provide faculty who want it with encrypted email service. That way, from the time an email leaves their computer until it is decrypted at its endpoint, it cannot be read without the use of sophisticated and time-consuming decryption algorithms. Thus, even if intercepted in transit, an email cannot easily be scanned and subjected to data extraction for commercial or surveillance purposes.

One way to implement this proposal is for ITS to buy commercial software that encrypts the email on the user’s computer before it is sent out to the internet service provider. Such software employing PGP (Pretty Good Privacy) encryption already exists for Firefox users as a downloadable extension. But such non-commercial products are not attractive because they lack the support and continuity of professional applications. Therefore the Group recommends that ITS look to commercial providers of encryption services such as Symantec to supply what the College needs, as this is the approach we find most attractive.

As a sidelight to this issue, the Group also recommends that ITS designate and support at least one non-Google email client for faculty Windows and Mac computers. In an email to a member of the Study Group on 11/4/14, an ITS employee wrote that “As an FYI, ITS recommends that all faculty, staff and students access their email from gmail.com rather than using email clients. Therefore we do not support mail client issues that may arise in the future.” Contrary to this policy, the Group believes that ITS needs to support an email client that can access encryption software on the user’s local computer.

Another approach is to use Google’s recently announced Chrome extension, called “End-to-End,” for sending and receiving emails securely. Google acknowledges the legitimacy of the interest in secure email. According to one source, “Google is developing a user-friendly tool for individuals to implement the tough encryption standard known as Pretty Good Privacy (PGP) in
an attempt to fully encrypt people’s Gmail messages that can’t even be read by Google itself, nor anyone else other than the users exchanging the emails. This product is apparently still in the development stage but once it is ready, Google plans to release it on the Chrome Web Store. According to the same article, “The web giant believes that this End-to-End extension for Chrome will make end-to-end PGP encryption quicker and easier for people, so that they’ll get an extra layer of security while communicating via emails. The extension could be released as ”alpha” sometime next year [2015].” However, whether using Google-provided software to avoid surveillance and data mining by Google itself is a good idea will have to be evaluated before this approach is embraced. Moreover, ITS will have to investigate whether Google will provide a site license that will cover all faculty interested in using the extension. There is also the question whether the extension will work in other browsers such as Firefox and Safari.

The Study Group suggests that ITS use these comments as the starting point to evaluate and choose the best product for providing faculty with encrypted email.

Proposal #2: ITS should provide and support encrypted cloud storage for all faculty who want it as an alternative to unencrypted Google Drive.

First approach: secure cloud storage
A number of alternatives were considered for secure cloud storage. In addition to Google Drive, the following cloud services were used for two months to evaluate and compare their many features: Dropbox, OneDrive, iCloud, Mega, Cubby, SpiderOak, JustCloud, and CloudOn.

SpiderOak is the one that stands out from the security point of view. This company has a “zero knowledge” system; the password is not available even to the company employees on their servers. The files are encrypted on the user’s computer and uploaded in encrypted form. They provide 100 GB for the price of $100/year (This price is for an individual. Lower prices can be negotiated for the institution.)

Second approach: local encryption for upload to Google Drive
After an extensive search on the internet and after purchasing, using, and evaluating many features of several systems, the Group member responsible for this study recommends BoxCryptor.

BoxCryptor is a program that allows users to encrypt their files on their computers and then upload them to any of the well-known cloud services like DropBox, Google Drive, etc. BoxCryptor will give a discount to Union College based on the number of people who might use the service. Two quotes from the company – for 100 users and 200 users – are attached.

The study Group suggests that ITS use these recommendations as a starting point to evaluate and choose the best product at the best price for Union faculty’s needs.

---

4 http://thehackernews.com/2014/12/gmail-end-to-end-encryption.html
Proposal #3: We recommend that ITS provide clarification of some of the issues posed by the use of GAE for email, searches, etc.

Among the questions we consider deserving of a policy response are:

a) What is the policy for handling email and any other confidential data stored on Google’s servers (e.g. on Google Drive) when a faculty member leaves Union? At the moment we could find no stated policy on the ITS or Human Resources websites.

b) Does Google build profiles of faculty members which it makes use of after they leave Union?

c) Various bits of personal data can be downloaded from some of Google's services; what does ITS recommend as the best vehicle for backing up one's email specifically? (Some may want to archive it offline; some may want to transfer it to other email services, e.g. upon graduation or after termination of employment or retirement.)

d) What exactly is the relationship between Gmail and other Google services in respect to privacy, for example, in relation to Picasa, YouTube, Google Maps or Google Hang-out?

e) What are best practices for privacy when making use of browsers to do searches and web browsing in conjunction with Gmail? For instance, is there any link between one's Google searches outside of Union's domain and one's Union Gmail account? Will searches one has done while outside of Union using, say, Firefox leak data when one is logged into Union's domain and vice versa?

f) Access to GAE is restricted in certain countries with the result that some colleagues have been unable to perform their college-related duties on time while abroad. We request:
   - an explanation of these access limitations and
   - a complete list of these limitations and of the ones that can be relaxed in negotiation with Google.

We suggest that ITS create a short, easy-to-understand web page that explains clearly what information Google has access to, what information it does not, and what steps users can take if they want to minimize the amount of information that “leaks” into Google’s servers.

Finally, the Group requests that ITS evaluate and act on all three proposals and report back the LCACT concerning the actions they propose to take or have taken.

Christopher Chabris, Department of Psychology
Felmon Davis, Department of Philosophy
Mohammad Mafi, Environmental Engineering
Steven Sargent, Department of History
Google Apps for Education Study Group
Mission Statement

On October 22, 2013 a letter signed by thirty-eight (later increased to forty-three) faculty members requesting the formation of a Google Apps for Education study group was sent to the FEC and LCAST.

On January 13, 2014, the LCAST unanimously approved the following motion, which it then sent to the FEC.

“Resolved that the LCAST recommends to the FEC that the FEC appoint a study group of Union College faculty users of Google Apps

1) to evaluate the following four concerns found in the first part of a letter signed by forty-three faculty members and forwarded to the FEC on 16 October 2013:

- We now know that Google has an active and far from transparent surveillance relationship with the National Security Agency (NSA) and other intelligence services of the U.S. government.
- We have concerns that customers’ reasonable expectation of confidentiality are explicitly secondary to Google’s commercial exploitation of the information that it scans or is lodged on its servers, including the content of emails.
- There are ongoing questions about the entanglements and costs (short- and long-term potentially incurred by educational institutions as they enter into commercial agreements with Google.
- Broader questions about the out-sourcing of and commercial agreements regarding information technology at educational institutions have not been systematically examined.

and 2) to act on the second of three requests made in the second part of the letter:

- to re-evaluate the commercial agreement(s) between Union College and Google
  in such a manner that the study group thoroughly examines the four concerns above and
  offers policies to address them as completely as possible.

Concerning the other two requests made in the second part of the letter,

- that the commercial agreement(s) between Union College and Google governing the use of Google Apps for Education by employees be made available to members of the campus community.
- that the FEC use the lessons of this matter to formulate a campus-wide policy
on the dissemination and circulation of information that empowers members of the Union community to participate in the shared governance of the college,

the LCACT concludes that neither is within its purview or consistent with its charge and thus makes no recommendation concerning them.”

On February 18, 2014 the FEC sent out an email soliciting faculty members to volunteer for the study group.

As of the end of Fall term 2014, four faculty members representing the Humanities (Felmon Davis), Social Sciences (Steve Sargent, Chair), Sciences (Chris Chabris), and Engineering (Mohammed Mafi) Divisions have volunteered.

Following the motion approved by the LCACT, the Faculty Google Apps for Education Study Group proposes the following mission: “1) to examine the commercial relationship between Union College and Google Apps for Education; 2) to consider the possibility of breaches of confidentiality arising from the use of Google Apps for Education; 3) to study the feasibility and costs of offering an alternative email provider to the faculty; and 4) to make recommendations about how the College should address faculty concerns expressed in the letter of October 22, 2013.”
Thank you very much for your request for a quote. Hereby we make you the following offer:

<table>
<thead>
<tr>
<th>Qty</th>
<th>Description</th>
<th>User/Year</th>
<th>Total/Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Boxcryptor Company Package 100 User 1-Year</td>
<td>$ 100.00</td>
<td>$ 10,000.00</td>
</tr>
<tr>
<td></td>
<td>Quantity discount 20%</td>
<td></td>
<td>(2,000.00)</td>
</tr>
<tr>
<td></td>
<td>Subtotal</td>
<td></td>
<td>$ 8,000.00</td>
</tr>
<tr>
<td></td>
<td>Special discount 50%</td>
<td></td>
<td>(4,000.00)</td>
</tr>
<tr>
<td></td>
<td>Net per year</td>
<td></td>
<td>$ 4,000.00</td>
</tr>
<tr>
<td></td>
<td>Incl. 0% VAT</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Total per year</td>
<td></td>
<td>$ 4,000.00</td>
</tr>
</tbody>
</table>

**Terms of payment:** 14 days after receipt of invoice

**Including all upgrades**

**Reverse Charge**

This quote is valid til: 31.12.2014
Union College  
Professor Mohammad Mafi  
807 Union Street  
Schenectady, NY 12308  
USA

Thank you very much for your request for a quote. Hereby we make you the following offer:

<table>
<thead>
<tr>
<th>Qty</th>
<th>Description</th>
<th>User/Year</th>
<th>Total/Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Boxcryptor Company Package 200 User 1-Year</td>
<td>$ 100.00</td>
<td>$ 20,000.00</td>
</tr>
<tr>
<td></td>
<td>Quantity discount 25%</td>
<td></td>
<td>($ 5,000.00)</td>
</tr>
<tr>
<td></td>
<td>Subtotal</td>
<td></td>
<td>$ 15,000.00</td>
</tr>
<tr>
<td></td>
<td>Special discount 50%</td>
<td></td>
<td>($ 7,500.00)</td>
</tr>
<tr>
<td></td>
<td>Net per year</td>
<td></td>
<td>$ 7,500.00</td>
</tr>
<tr>
<td></td>
<td>Incl. 0% VAT</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Total per year</td>
<td></td>
<td>$ 7,500.00</td>
</tr>
</tbody>
</table>

Terms of payment: 14 days after receipt of invoice

Including all upgrades

Reverse Charge

This quote is valid til: 31.12.2014