FINAL REPORT

UNIVERSITY OF MARYLAND STUDENT EMAIL COMMITTEE

May 15, 2011
COMMITTEE MEMBERS

Michael Ball, Smith School of Business, Prof & Assoc Dean (Chair)
David Barks, OIT-TSS-Enterprise Internet Svcs, Manager (non-voting)
Patrick Beasley, Alumni Association, Assistant Director of Technology
Anne Bowden, President’s Office, University Counsel (non-voting)
Bill Dorland, Undergraduate Studies - Honors College, Prof & Director
Allison Druin, iSchool, Associate Dean
Jeff McKinney, Electrical and Computer Eng, Director of Computer Services
Dan Navarro, BSOS, Director of Academic Computing Services
Dai-An Tran, Student Affairs Resident Life, Assistant Director
Amitabh Varshney, Institute for Advanced Computer Studies, Prof & Director
Luigi Alvarado, Grad Student
Zach Cohen, Student – BSOS, Legislator SGA
Mariela Garcia Colberg, Grad student
Jacob Crider, Student – ARHU, Legislator SGA
Tomek Kott, Grad Student
Elizabeth Moran, Student, Smith School of Business, Legislator SGA
Morgan Parker, Student, CMPS Legislator SGA
Background

In the Fall of 2010, the University’s Office of Information Technology (OIT) examined alternatives for providing student email services in the 2011-2012 academic year and beyond. This examination was motivated by several factors, including these prominent two:

- the existing Mirapoint-based system was outdated and in need of hardware and software upgrades;
- there were many attractive competing alternatives.

OIT investigated this issue. Their investigation included a survey of students and also an identification and analysis of several alternatives. Their report to the University IT Council is attached (Appendix 1).

The OIT analysis found that a number of important non-technical issues, including privacy and security concerns, should be taken into account in making this decision. Therefore, it was recommended that a campus-wide committee be formed to address this issue. This recommendation was the basis for forming the student email committee. Note that it includes student, faculty and staff members with a broad set of backgrounds. An OIT staff member, David Barks, participated in an ex-officio role. He provided a range of technical input to the committee and, at times, employed OIT staff analysis in providing needed committee inputs.

Dr. Joseph JaJa, Interim Campus CIO, charged the committee in December of 2010. The specific alternatives the committee was asked to consider were:

**Mirapoint Option:** remain with existing Mirapoint system, while making appropriate hardware and software upgrades.

**Forwarding Option:** provide a forwarding-only service, that is, the University would not provide students with an email account, rather, each student would be expected to take responsibility for obtaining an email account, e.g. students could obtain a free account from one of several public email service providers, such as Yahoo, Google, etc.; the university would provide a University-branded address for each student, (student@umd.edu) and mail sent to this address would be forwarded to the email account designated by each student.

**Exchange Option:** give students email accounts on the University-hosted Microsoft Exchange service currently used by faculty and staff.

**Gmail Option:** create a student email system based on Google Apps Education Edition; under this option email storage would be “hosted” at an off-campus site not under the control of the University (For systems of this type it is common to say that email is stored “in the cloud” and such an approach is called a “cloud-based” solution).
Live@edu Option: create a student email system based on Microsoft Live@edu (new name: Live365); this is also a cloud-based solution.

Under all of these options students would have a University-branded account, e.g. either student@umd.edu or student@terpmail.umd.edu. An email was sent to the University community announcing the formation of the committee (see appendix 2).

The committee met several times during the months of January, February and March of 2011. The committee’s deliberations and analysis included the following:

- review each alternative and their features (see Appendix 3);
- review of what other universities had done or were planning (see Appendix 4);
- examination of legal, privacy and security issues (see Appendix 5);
- solicitation and analysis student feedback in many forms:
  - results of survey (prior to formation of committee – see Appendix 1)
  - a repository was set up, for receiving student input via email (605 emails received);
  - focus group;
  - town hall forum.

Part of the student outreach activities also had the goal of informing the student community of the committee’s deliberations and educating the student community regarding important issues related to the decision. This was aided by cooperating with the staff of the Diamondback in their efforts to keep the students informed. In particular, three news articles and one editorial appeared in the Diamondback related to student email and the committee’s deliberations (see Appendix 6).

Findings

1) **Gmail is overwhelmingly popular.** However, the strong support for Gmail is likely due to Google’s “cool factor” and a general familiarity with Gmail on the part of students; i.e. Gmail, Exchange and Live@edu are all very powerful; a close examination of the feature set of each does not indicate an obvious advantage of one over the other, differences are largely one of taste.

2) The attraction of Gmail is not just based on email but the wide array of Google apps, e.g. calendar, google-docs, etc.

3) Extensive storage space is extremely important to students.

4) Privacy/security issues are less important than convenience/availability of features to students; however, some students do have concerns in these areas and strong opinions.
5) Based on feedback it is clear that some – perhaps many – perhaps most students would continue to have their email forwarded even if the University provided a popular option.

6) The e-communications landscape is very dynamic:

- **Most existing students had an email address when they arrived on campus** and there are strong barriers to giving it up or even to maintaining a second account for University business.

- **There appears to be a trend away from email** to Facebook messaging, texting and other types of communications:
  - some students use Facebook groups to coordinate student projects (others use Google tools);
  - the “attachment” to an existing personal email account may be less strong for incoming students than it was for students admitted 4 years ago;
  - some argue that the use of email is dying (this is perhaps an extreme position).

7) Generally, **the contractual terms offered** and the privacy and security **guarantees** provided by cloud-based solutions are vague; **the concerns generally are not legal ones** – rather they involve the degree to which the University is able to protect privacy and guarantee security for students in a responsible manner.

8) There is not a consensus among universities with respect to an approach to privacy and security concerns related to cloud-based email solutions:

- **Some universities have adopted cloud-based solutions**, in spite of privacy/security concerns, e.g. UMBC, UVA.
  - Among these, some have negotiated more favorable contract terms; however, (apparently) there has not been a high degree of flexibility on the part of Google and Microsoft.

- **Some universities have decided not to go to a cloud-based solution** because of privacy/security concerns, e.g. Duke, MIT.

9) The effort required to integrate with learning systems appears to be the same for Gmail/Live@edu; on the other hand, it would be easier to integrate Live@edu with Exchange.

10) If the University-branded email system has a limited feature set compared to the private Gmail then many students would be reluctant to give up their private Gmail account–
“Why convert to the University system if you lose features?” – it appears that the full feature set will be available on the University-branded systems.

Analysis
The committee agreed to use the following set of criteria to evaluate the alternatives.

- Feature set and performance – now and in the future.
- Compatibility with roles and responsibilities of University.
- Student preferences.
- Ability to integrate with other systems.
- Compatibility with future trends, systems, etc.
- Contractual, privacy and security concerns.
- Cost should be considered but in a secondary way.

An important assumption underlying the committee’s analysis is:

At least in the near-term, faculty and staff (including many graduate students) will be using Exchange.

The committee decided early on that Mirapoint is not a viable option. The reasons for this decision is i) Mirapoint is hugely unpopular among its existing user base, ii) it would be very expensive to upgrade and iii) even with an upgrade, its feature set would be inferior to other options being considered.

The committee also eliminated forwarding as alternative. The principal reason behind this decision was the feeling that the University has a responsibility to provide email service to its students. Related to this consideration is the potential public perception that a University that does not provide email services was “short-changing” students.

Some further considerations behind this decision are:

Forwarding can be unreliable: experience indicates that students can give erroneous email addresses or might not update email addresses when there is a change so that, under a forwarding service, there is always a group of students who will not receive messages sent to them.

Integration with other learning systems becomes cumbersome.
@umd.edu is a very valuable/important identifier: while it is easy to allow students to receive student@umd.edu, with the forwarding-only option, it is more difficult to send with this id from third party email addresses.

It should also be noted that there is some support for the forwarding option.

- Specifically, the fact that several providers give free access to (very good) email services leads one to question whether the University “should be in the email business”.
- Some also argue that, looking to the future, it is possible that email will decline and other forms of communication will start to dominate (texting, facebook messaging, etc)

With the elimination of the Mirapoint and forwarding options, thee options remain: Gmail, Live@edu and Exchange. Gmail and Live@edu are both cloud-based solutions and so we organize our discussion into a comparison between the cloud-based options and Exchange and a comparison between Gmail and Live@edu.

**Cloud-based vs Exchange:**
Cloud-based pro’s (+) and con’s (-):

+ Providers can write-off development effort based on millions of users: assured of latest technologies, including latest apps and (most likely) ample storage.

+ Gmail is hugely popular.

+ Good online training.

- Privacy/security issues related to storing data “in the cloud” as well as related contractual concerns.

- subdomains require separate contracts.

Exchange pro’s (+) and con’s (-):

+ Can control data and privacy and security level provided; compliant w FERPA, export control laws; better IP control.

+ Greater control and certainty over contract.

+ Easy integration with faculty/staff systems.

+ Can customize to user base.

+ Only have to integrate one email system w other systems.

- Subject to University resource constraints: Delays in implementing newest features and insufficient storage allocations would seem to be inevitable.
Extra apps may have to be purchased/deployed.

**Gmail vs Live@edu:**
Gmail pro’s (+) and con’s (-):

+ Overwhelmingly preferred by students.
+ High level of familiarity on part of students.
+ Clean, simple interface.
+ Claim to be FERPA compliant for requested accounts.

Live@edu pro’s (+) and con’s (-):

+ Traditionally Outlook (the Live@edu client) has dominated corporate use (this may be changing).
+ Tools very similar to MS desktop products.
+ Integration between live@edu and exchange will be much easier.
- Disclaims any responsibility under FERPA.

**Recommendations**

The main committee recommendation is:

*Give Students a Choice between Google Apps for Education and Exchange.*

Specifically, the University should contract with Google to provide University-branded Google Apps for Education accounts, e.g. student@terpmail.umd.edu, through Google apps@edu. Further the University should continue to maintain its internal MS-Exchange system; faculty and staff should continue to use this system (because of FERPA, Export Control and Privacy concerns). Students should be given the choice between having a University-branded Gmail account and an account on the (faculty/staff) Exchange system.

The committee felt that this “hybrid” solution was attractive because under a Gmail-only solution, the University would still have to maintain Exchange for faculty and staff (including most grad students). Thus, providing students with Exchange as an option would seem to involve very little additional overhead (there would be additional storage costs) and it would enable University to provide higher level of privacy/security to those who desired it.
The deciding factors in the committee’s decision include the fact that providers such as Google and Microsoft can write-off development effort based on millions of users, thereby assuring that a Google or Microsoft solution would include the latest technologies, including the latest apps and (most likely) ample storage. In contrast, it would seem inevitable that a University-hosted solution would run into resource constraints, delaying implementation of the newest features and provisioning of sufficient storage. The choice between Gmail and live@edu was largely based on the immense popularity of Gmail among students. The committee also emphasized that the excellent online training provided by Google was also of importance.

The committee offers the following advice regarding the implementation.

1) The University should seek to obtain favorable terms in the contract with Google; the committee would like to provide some recommendations and priorities in this regard (after meeting again).

2) An important decision will be whether to purchase the Postini add-on, which provides some backup protection and investigative support.

3) Integration between Gmail and University learning systems and between Gmail and Exchange will be very critical to providing value to the students – careful planning and proper resource commitments should be made to these activities.

4) Training and migration support are very important and should be properly funded.

5) One implementation option could be to provide all students with a Gmail account and, in addition, provide those who desire it an Exchange account.

   a. Those with an Exchange account would use this account as their regular email account but would use the Gmail account for certain student projects that made specific use of Google collaboration tools.

   b. Related question: Could faculty assume that all students have and use their University-branded Google account?

6) If Gmail is extensively used by students for communications, projects, etc., faculty may start requesting/demanding Gmail accounts as well. The University should think carefully about how to respond to such requests.

7) The University should decide whether to allow students to keep their accounts after graduation.

8) Google higher ed email service includes access to 6 Google apps: The University should designate Google provided email and calendaring as official services it offers to students. While access to other Google apps under the University email login will no doubt be an important feature offered students, the University should only designate other
apps as official University services after careful study. In particular, the University should consider whether such apps satisfy universal accessibility requirements before officially sponsoring them.

9) If desired, student@umd.edu accounts could be provided under Gmail option but there are many technical (and cost) details that make student@terpmail.umd.edu more desirable (terpmail is a placeholder – other names are possible).

10) Over time, Google could improve its contracting terms and also attitude toward privacy and security so that it may be possible to migrate faculty to Gmail as well.

11) The University of Maryland should participate in University consortia and other means to achieve better contracting terms and privacy and security features from Google.

12) The University will want to “market” this decision to the student community on a number of levels. Once aspect involves convincing students who come with an existing Gmail (or other) account to switch to the University-branded account. Some arguments in favor of doing so include:

- Branding (umd.edu address) – can be kept after graduation.
- Directory services.
- University calendar services.
- No ads.
- Better contractual (privacy and security) terms, incl guaranteed up-time

Addendum

At the time of the finalization of this report, the University had already initiated discussions with Google regarding a contract to provide email and other services. In fact, Google was willing to incorporate several provisions in the contract that substantially lessened many of the concerns originally identified by the committee. Specifically,

The contract will specify that:

1. Data will be stored only on servers located in the U.S., Canada and Europe.
2. The University owns all stored data.
3. A transition period will be provided in case of contract termination.
4. An explicit security standard will be met (see appendix).
APPENDIX 1: OIT Student Email Report
Future of Student E-mail

IT Council
November 10, 2010
Current status of Student Campus E-mail

• Students are housed on Mirapoint Servers
  • 41% student usage
  • Student opinion (25% favor remaining on current e-mail system; n=1287)
  • 100 MB of storage for each student
  • No calendar; No redundancies
  • Annual cost: $235,000
  • Hardware refresh cost: $237,000
Student E-mail Options

- Remain on Mirapoint
- Move students to campus provided Exchange e-mail system
- Migrate students to a managed outsourced service with a University affiliated e-mail address
Pros/Cons – Remain on Mirapoint

• Pros
  – No change in staff and no migration
  – We control the service

• Cons
  – Only 41% of students use the University email system and that number is decreasing
  – Maintenance cost is high
  – Technology is old
  – Replacement cost is high
Pros/Cons – Campus Provided Exchange

• Pros
  • Cost is license and storage
  • Ability to provide additional services on this platform over time
  • Migration is known with in house staff, and we control the service
  • Exchange is most likely what students will use when they enter the workforce

• Cons
  • Need to migrate to Exchange 2010 sooner
  • Need more storage and possibly archiving
  • Need to train students on Outlook/Mac Mail for best experience
Pros/Cons – Managed Outsource Service

• Pros
  • Increasing number of peer institutions are moving in this direction
  • More storage than current system
  • Ability to provide additional services

• Cons
  • Unknown future cost
  • Increased load on network
  • Legal, privacy, data ownership and export control concerns
  • Integration with other university services
  • Effect on collaboration with faculty
Proposed Approach

• Form a Campus Committee to Recommend Future System:
  • Consider e-mail only vs. expanded services for students and faculty/staff/student interactions under the various options
  • Review the legal issues identified
  • Consider return on investment
  • OIT will participate and provide technical support

• Decide by March 2011 for first migration in Fall 2011

• Communicate decision to campus
APPENDIX 2: Announcement to University Community Regarding Formation of Student Email Committee
Dear University of Maryland Community:

I am writing to announce the formation of a committee chaired by Dr. Michael Ball to explore possible options for the student e-mail system at Maryland and to solicit your input to this process. There are four alternatives under consideration:

-- Continue with the current student system, Mirapoint (contracts and hardware would need to be updated).
-- Move students to the university's Exchange system, currently being used by faculty and staff.
-- Transition student e-mail accounts to an outsourced system (such as Google or Microsoft).
-- Provide students with a forwarding service only.

No matter which option is chosen, students will have a university branded e-mail address.

Here is some background information: In November 2010, 41% of students were using their Mirapoint accounts, while 59% of students were forwarding to other e-mail services such as Google's Gmail, Yahoo! Mail, and Microsoft's Hotmail. In the latest Office of Information Technology annual student survey, 36% of the 1,287 respondents stated a preference for a forwarding service only, 35% stated a preference for a UMD-provided Gmail account, 26% stated a preference to remain on Mirapoint, and 2% stated a preference for a Microsoft e-mail service.

I encourage you to provide your input to this process by e-mailing the committee at emailcommittee@umd.edu.

OIT is committed to working with the university community to provide the best technologies for achieving the university's overall vision of excellence in education and research.

I look forward to your contribution to this important process.

Joseph JJa
Interim Vice President and CIO

The Student E-mail Committee members are listed below for your information:

- Michael Ball, Associate Dean of Faculty and Research and Professor, Robert H. Smith School of Business
- Amitabh Varshney, Professor and Director, College of Computer, Mathematical, and Natural Sciences
- Jeff McKinney, Director of Computing Facilities, A. James Clark School of Engineering
- Dai-An Tran, Assistant Director of Information Technology, Department of Resident Life
- Anne Bowden, University Counsel, Office of the President
- Bill Dorland, Honors College Professor and Director, Office of Undergraduate Studies
- Allison Druin, Associate Professor, Associate Dean, and Director, College of Information Studies
- Dan Navarro, Director, Office of Academic Computing Services, College of Behavioral and Social Sciences
- David Barks, Manager of Enterprise Internet Services, Office of Information Technology
- Zach Cohen, Student, College of Behavioral and Social Sciences, Student Government Association
- Elizabeth Moran, Student, Robert H. Smith School of Business, Student Government Association
- Morgan Parker, Student, College of Computer, Mathematical, and Natural Sciences, Student Government Association
- Jacob Crider, Student, College of Arts and Humanities, Student Government Association
- Mariela Garcia-Colberg, Graduate Student
- Luigi Alvarado, Graduate Student
- Tomek Kott, Graduate Student

This note was authorized for distribution to University of Maryland Community by:
Joseph JaJa, Interim Vice President and CIO
APPENDIX 3: Review of Alternatives
<table>
<thead>
<tr>
<th>Feature</th>
<th>email.umd.edu</th>
<th>Google</th>
<th>Live @ EDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Search Attachments</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Virus and spam filtering</td>
<td>Yes (campus controllable)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Listing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Same password and username</td>
<td>Yes</td>
<td>Yes (with possible latency)</td>
<td>Yes</td>
</tr>
<tr>
<td>Calendaring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create multiple calendars and share calendars with other users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Contacts</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Contact editing and personalization</td>
<td>Yes</td>
<td>Yes (Limited)</td>
<td>Yes</td>
</tr>
<tr>
<td>Contact connection through University Directory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Web Space</td>
<td>Yes (can be integrated with additional service)*</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Can be added</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video Chat</td>
<td>Can be added</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group Chat</td>
<td>Can be added</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PC-to-PC voice calls</td>
<td>Can be added</td>
<td>Yes</td>
<td>No (Yes in Fall)</td>
</tr>
<tr>
<td>Desktop share</td>
<td>Can be added</td>
<td>No</td>
<td>No (Yes In Fall)</td>
</tr>
<tr>
<td>Accessible from a mobile phone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sync with Outlook</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sync with Blackberry</td>
<td>Can be added</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sync with iPhone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sync with Android</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create, share, store and publish online documents, spreadsheets, and presentations on a Web-based application</td>
<td>Can be added</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Upload existing documents</td>
<td>Not integrated for students: Can be added</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Offline Address Book</td>
<td>Yes</td>
<td>Yes with email Client</td>
<td>Yes with email Client</td>
</tr>
<tr>
<td>Email organization</td>
<td>Folders</td>
<td>Labels</td>
<td>Folders</td>
</tr>
<tr>
<td>Server Side Rules</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for multiple Browsers</td>
<td>Uneven (full support by Fall)</td>
<td>Yes</td>
<td>Uneven (full support by Fall)</td>
</tr>
<tr>
<td>Message Classification</td>
<td>Flexible (~126 categories)</td>
<td>Yes (multiple labels per email)</td>
<td>Yes</td>
</tr>
<tr>
<td>Federate with other campuses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Yes/No</td>
<td>W/Cost/No</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Back and Restore of lost mailbox</td>
<td>Yes</td>
<td>W/Postini</td>
<td></td>
</tr>
<tr>
<td>Deletion Retention</td>
<td>Yes</td>
<td>W/Postini</td>
<td></td>
</tr>
<tr>
<td>Backup and restore of individual email</td>
<td>Can be added</td>
<td>W/Postini</td>
<td>No</td>
</tr>
<tr>
<td>E-Discovery support</td>
<td>Yes</td>
<td>W/Postini</td>
<td>Yes (Built-in)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbox in GB</td>
</tr>
<tr>
<td>Attachment Size MB</td>
</tr>
<tr>
<td>Storage Space GB</td>
</tr>
<tr>
<td>Photo Storage</td>
</tr>
<tr>
<td>Document Format Supported</td>
</tr>
</tbody>
</table>
### Institutional E-Mail Directions

**RUCC Survey Results**

March 2010; BDV complied

<table>
<thead>
<tr>
<th>Institution</th>
<th>Current E-mail Platform</th>
<th>Considering Cloud?</th>
<th>Considering Google/MSLive?</th>
<th>Factors</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSU</td>
<td>MS Exchange</td>
<td>Done (G)</td>
<td>Yes</td>
<td>Cost, Control, Policy/Legal, Acceptance, Governance</td>
<td>Students done; Institutional 2011-12</td>
</tr>
<tr>
<td>Iowa</td>
<td>MS Exchange</td>
<td>Yes</td>
<td>No</td>
<td>Cost, Control, Policy/Legal, Acceptance</td>
<td>Students 2010; institutional uncertain</td>
</tr>
<tr>
<td>NCSU</td>
<td>Groupwise</td>
<td>Done (G)</td>
<td>Yes</td>
<td>Unified communications, control</td>
<td>Transition - a few years; may start next year</td>
</tr>
<tr>
<td>Indiana</td>
<td>MS Exchange</td>
<td>Done (G&amp;M)</td>
<td>No</td>
<td>Savings not found for hosting MSEx</td>
<td>Renovating with Exchange 2010 now</td>
</tr>
<tr>
<td>Stanford</td>
<td>Zimbra</td>
<td>Yes</td>
<td>Yes</td>
<td>Security, privacy, control of data</td>
<td>2011 or 2012</td>
</tr>
<tr>
<td>Case Western Reserve</td>
<td>Google</td>
<td>Done (G)</td>
<td>Done (G)</td>
<td>Done (G)</td>
<td>Completed Jan-2010</td>
</tr>
<tr>
<td>Arizona</td>
<td>Open/Source</td>
<td>Done (G)</td>
<td>Yes</td>
<td>No</td>
<td>Security, DR, US-based, Control, Purge, etc.</td>
</tr>
<tr>
<td>Michigan State</td>
<td>OS-Horde</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Not at the moment</td>
</tr>
<tr>
<td>Institution</td>
<td>Software</td>
<td>Status</td>
<td>Completed</td>
<td>Adopted</td>
<td>Focus Areas</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------</td>
<td>---------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Virginia</td>
<td>Exchange/IMAP</td>
<td>Done (G)</td>
<td>Yes</td>
<td>Yes</td>
<td>Cost, Privacy, Policy, Control</td>
</tr>
<tr>
<td>Washington</td>
<td>IMAP/Exchange</td>
<td>Done (M)</td>
<td>Yes</td>
<td>Yes</td>
<td>Cost, comprehensive solutions, privacy, policy</td>
</tr>
<tr>
<td>Duke</td>
<td>SunMail/Exchange</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Small savings, privacy, policy, legal, control</td>
</tr>
<tr>
<td>Iowa State</td>
<td>Exchange/IMAP</td>
<td>Done (G)</td>
<td>Yes</td>
<td>Yes</td>
<td>Functionality, Cost, Policy/Legal</td>
</tr>
<tr>
<td>UC Davis</td>
<td>Cyrus-OS/Exchange</td>
<td>Done (G)</td>
<td>Yes</td>
<td>Yes</td>
<td>Security, data-mining concerns, culture</td>
</tr>
<tr>
<td>Colorado State</td>
<td>UnixMail/Exchange</td>
<td>Done (G)</td>
<td>Yes</td>
<td>No</td>
<td>Unified communications, control</td>
</tr>
<tr>
<td>Hawaii</td>
<td>Netscape/Sun</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Cost/Quality, Privacy, Legal, Policy, Use of data</td>
</tr>
<tr>
<td>Boston U.</td>
<td>CyrusLinux-Horde/Exchange</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Cost, Control, DR, Privacy, Legal</td>
</tr>
<tr>
<td>Colorado (B)</td>
<td>Mirapoint/Exchange</td>
<td>Yes (M)</td>
<td>No</td>
<td>No</td>
<td>Legal/Privacy</td>
</tr>
<tr>
<td>UNC-Chapel Hill</td>
<td>Exchange (in progress)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Functionality, Cost, Policy/Legal</td>
</tr>
<tr>
<td>UBC-CA</td>
<td>Exchange</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Observing</td>
</tr>
<tr>
<td>Institution</td>
<td>Service/Alternative</td>
<td>IMAP/Exchange/others</td>
<td>Observing</td>
<td>Cost, Flexibility of change, et al</td>
<td>Fall 2012</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>-----------</td>
<td>-----------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Yale</td>
<td>Service, Privacy, Control, Security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>2010 students; institutional if successful</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>SunMail</td>
<td>Yes</td>
<td>Yes</td>
<td>Observing</td>
<td>Cost, Privacy, Policy, DR, Control, standard-based, integration</td>
</tr>
<tr>
<td>Maryland</td>
<td>Exchange/Mirapoint</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Cost, Mobility, integration w/Cloud Collab. apps</td>
</tr>
<tr>
<td>PennState</td>
<td>HomeGrown/Exchange</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Age of current system (supportability); Privacy, security, data ownership, etc.</td>
</tr>
<tr>
<td>Dartmouth</td>
<td>Blitzmail' HomeGrown, Exchange</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Technology, Security, Legal/Policy, Privacy, Unified Comm, etc.</td>
</tr>
<tr>
<td>MIT</td>
<td>Cyrus Imap-Horde/ Exchange</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Reexamine post 2011</td>
</tr>
<tr>
<td>Columbia</td>
<td>Cyrus/Exchange</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Not yet evaluating</td>
</tr>
<tr>
<td>Princeton</td>
<td>SunIMPA/Exchange</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Technology, Security, Legal/Policy, Privacy, Unified Comm, etc.</td>
</tr>
<tr>
<td>Institution</td>
<td>Exchange Model</td>
<td>Migrated (x)</td>
<td>Primarily Cost</td>
<td>Data Ownership Concerns</td>
<td>Consolidated Exchange Year</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>-------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Illinois</td>
<td>Express/Exchange</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Primarily Cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reexamine F/S in the future</td>
</tr>
<tr>
<td>Ohio State</td>
<td>Exchange</td>
<td>Done (M)</td>
<td>No</td>
<td>No</td>
<td>Consistency</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Ownership concerns</td>
<td>in-house Exchange</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>now</td>
</tr>
<tr>
<td>Northwestern</td>
<td>Several/Exchange</td>
<td>Done (G)</td>
<td>No</td>
<td>No</td>
<td>Legal (Counsel)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Costs, security, E-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>discovery, uptime guarantees</td>
</tr>
<tr>
<td>Virginia Tech</td>
<td>SunJava/Exchange</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>2010-2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11/31 respondents</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>have migrated student e-mail to the cloud. Most have chosen Google although some have chosen Microsoft</td>
</tr>
</tbody>
</table>

**Definitions**

Means have migrated to 'Cloud' ... G for Google, M for MSLive

**NOTE:**
<table>
<thead>
<tr>
<th>Yes</th>
<th>Mostly means 'Yes, considering' ... some considering more vigorously than others, so check the Timing column and Comments for details</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Mostly means 'No, not considering' ... some may mean 'not yet' and some may be 'maybe' and some are most definite</td>
</tr>
<tr>
<td>Observing</td>
<td>Mostly means watching what others are doing, observing trends, etc.; not as firm as a 'No' but not in the 'Yes' category either (see above)</td>
</tr>
</tbody>
</table>

Not meant to be exhaustive by Institution, just the primary ones mentioned. Most of us share a common set of considerations/concerns on Cost, Control, Policy/Legal aspects, DR, User Input, etc.
| Timing | Indicates when consideration may bear implementation fruit; see Comments for more detail or contact the individual |
APPENDIX 5: Discussion of Legal and Privacy Issues
PRIVACY AND SECURITY ISSUES RELATED TO CLOUD COMPUTING AND CHOICE OF STUDENT EMAIL SYSTEM
**Where is the data stored?** Could be in another country ➔ certain vulnerabilities; legal issue for those working on government contracts.

**Long term viability:** what happens after contract ends and/or service provider is bought out? Will data be destroyed? Will it be properly protected? Will it be sold?
Data recovery and security: University does not have control or guarantee regarding how data is handled and what personnel handle it; cannot determine specific level of security desired.

Service termination: Provider can terminate contract/service for “convenience” or might terminate contract/service because of actions of a few users ➔ University would abruptly be left without service.
Investigative support: there are situations, e.g. death, national security events, criminal acts, where it would be necessary to perform an investigation that required access to email – there may be difficulties or limitations in the ability to do this for certain cloud-based solutions.

Use of data by service provider: Service provider retains right “to use non-personally identified information”.

To what degree should we be concerned about getting legal guarantees regarding the issues discussed?

Two perspectives:

*Contractual guarantees*

*vs*

*Marketplace pressures to provide satisfactory service*
APPENDIX 6: Diamondback Articles
E-mail host change stirs concerns of security

Students vote Gmail most popular choice

Staff writer

Published: Tuesday, February 22, 2011
Updated: Tuesday, February 22, 2011 00:02

A faculty and student committee is nearly a month away from deciding how to implement a more feasible university student e-mail system, but committee members say the alternative most popular among students may come with some privacy risks.

The Student E-mail Committee has met several times since December to explore the possibility of updating or replacing the unpopular Mirapoint student e-mail system in time for the fall semester, with the goal of making a recommendation to the University Senate Information Technology Council by the end of March. To gather further student input, the committee is hosting a town hall meeting March 2 to discuss the various alternatives. Members will also meet with a student focus group tomorrow to glean more insight as to how students use various technologies, such as Gmail, Facebook and Twitter.

The committee has already received about 500 e-mails from students weighing in on the options: operating student e-mail accounts through a system such as Google or Microsoft, moving accounts to the system used by faculty and staff, providing a forwarding-only service or continuing to use the existing system. The Student Government Association and the Graduate Student Government posted discussion boards on their Facebook pages about the e-mail options.

The feedback has revealed that an overwhelming majority of students favor the option of outsourcing student accounts to Google, but committee members have expressed concern with some of the security and privacy issues such a switch may involve. E-mail data would no longer be owned by the university, while outside vendors may store data in foreign databases rather than on the campus, according to committee chairman Michael Ball. Google’s contract also states that e-mails may be subject to data mining — in which the company sells users’ information to firms hoping to profile potential customers — and neither vendor would accept
responsibility for deleting user information if the university chooses to switch vendors in the future.

University Counsel Anne Bowden, who sits on the committee, said while it would not be illegal to sign a contract with these stipulations, they are cause for concern.

"It's a risk decision, and it's a policy decision," Bowden said. "None of these issues is sufficient to say, 'We can't sign the contract.' We have to make a business decision to see if the risks are outweighed by the advantages."

Ball, a management science professor, said these privacy risks concern unlikely scenarios and said many students already accept the risks by using their own Gmail accounts. But he added the committee has to consider that tighter security may be expected from a university account.

"We really do want what the students want," Ball said. "At the same time, with some of these issues like privacy, we have to decide the kind of responsibilities the university has in that area, and we need to be careful."

GSG physics representative Tomek Kott, who also serves on the committee, said these issues are of particular concern to graduate students. If teaching assistants' e-mails are data mined, he said, information such as students' grades may no longer be private, and there is no guarantee e-mail communications on research would be stored in the country, as is required by law for certain fields.

"We've discussed maybe the possibility that the undergraduates go on Google and Microsoft and then the graduate students go on Exchange [the service used by faculty and staff] because most graduate students TA or do research," Kott said. "But then the question is, what about the undergraduates who do research or TA? ... We're starting to look at an option that's split along some groups, but we don't know what those groups might be."

While members said they do not believe such issues are severe enough to take the option of outsourcing off the table, they will be reaching out to students to determine how they can best proceed.

"We need to have a dialogue with students, because this is an issue that is very unique in that the impact is primarily on students," said SGA behavioral and social sciences legislator Zach
Cohen, a committee member. "This is not just going to affect next year's students, but students 10 and 20 years from now."

Despite the issues, Office of Information Technology representative David Barks said he is confident students will have a better e-mail system by next semester.

"It's all about what's going to give students the best experience," Barks said. "As long as we make a decision that is long-term viable ... I think we'll be in a better place than we are now."

The student e-mail forum will be held March 2 from 4:30 to 6 p.m. in room 1243 of the Biology-Psychology Building.
For many students, one of the most frustrating and reviled aspects of this university is not dining hall food or Route 1 traffic. It's e-mail. For years, the e-mail service used by the university has frustrated students with its slow delivery time and outdated design.

But after months of work by a committee made up of faculty and students, the Mirapoint student e-mail system could become a thing of the past come fall semester. However, a new concern has emerged, not out of disdain for the existing system, but about what system should replace it. Some have suggested that student accounts be moved to the more reliable system used by faculty and staff, while others have advocated for student accounts to be operated by Microsoft. But for students, the most popular alternative is a system many of them already use: Gmail.

Operated by Google, Gmail would allow students to access their umd.edu accounts through the popular e-mail system, increasing reliability and dependability. But despite strong feedback in favor of a Google-based system from students, who were polled last semester, serious concerns remain.

Indeed, Google has come under particular scrutiny in recent years for what some perceive to be lax privacy policies. Google's rapid growth and popularity have earned it a reputation as a top company but also a reputation verging on Big Brother.

And while some concerns with Google's practices may be overblown, hesitation about switching to Gmail are valid. After all, Google's own contract stipulates that student e-mails could be subject to data mining in order for Google to sell students' information to outside companies for customizing purposes. Also, Google has refused to delete user information if the university were to ever switch its e-mail platform again. Such data could also be stored in databases removed from the campus and would no longer be owned and protected by the university.

Those privacy concerns may seem minor, particularly considering how many students already use Gmail for their personal e-mail accounts. But for students and teaching assistants who may be corresponding about confidential information such as grades, privacy is imperative.
Moreover, it may be required by law. Some pieces of federal law require certain types of research to be stored exclusively in the United States, something Google could not guarantee.

That said, Gmail has become one of the most popular e-mail systems in the world, growing exponentially in recent years and seeking to surpass popular platforms like Yahoo Mail and AOL Mail. And given the responses of students, nearly 500 of whom have written to the Student E-mail Committee weighing the options, Gmail remains the favorite.

As the committee continues to gauge student opinion in the coming weeks, the members should be sure to educate students about the options before them. Concerns about Google’s privacy policies are legitimate, and while they may rarely cause trouble, their potential to do so should not be ignored or swept under the rug. But if students continue to support the Gmail option after learning about these issues, the decision to switch to a Gmail-based system should be easy.

For too long students have grappled with a difficult and frustrating e-mail service that seems to be anything but a service. With e-mail continuing to be a major form of communication in academia, a system that works with ease is imperative. And while security concerns should be weighed, ultimately what will best serve students — and what is most popular — should be the obvious choice.
For the second time, students told a committee yesterday what kind of university e-mail service they want to see in place next year: Gmail.

About 20 university community members, most of whom were students, came to a town hall meeting hosted by members of the Student E-mail Committee yesterday to voice questions and concerns over what service will ultimately be chosen to replace the unpopular Mirapoint student e-mail system.

Much of the discussion centered on the privacy and security risks surrounding switching accounts to Microsoft or Gmail, which was the preferred system chosen by students in a recent poll.

The committee, which aims to make its final recommendation to the University Senate Information Technology Council this month, began meeting in December and has been gathering feedback from students on the alternatives being considered. Undergraduate behavioral and social sciences legislator Zach Cohen, who sits on the committee, opened the forum by telling students the committee was there to hear directly from them.

"The decision we make here will have long-term impact, which is why we're reaching out to students across the campus," he said. "There's pros and cons to everything we're considering, so what we really need to hear from you is which pros are the best and which cons are easiest to mitigate."

Throughout the forum, three of the four options — moving student accounts to the system used by faculty and staff, providing a forwarding-only service or continuing with Mirapoint — were largely absent from the discussion. Instead, students seemed most interested in the final option:
outsourcing to either Google Apps for Education or Microsoft Live@edu, which will be called Live 365 next year.

Committee members explained each of the vendors’ features and also discussed some of the privacy and security risks associated with outsourcing. Because vendors may store the data in foreign databases, Google’s contract states e-mails may be subject to data mining — in which the company sells users’ information to firms hoping to profile potential customers — and neither vendor would accept responsibility for deleting user information if the university chooses to switch systems in the future.

The committee members fielded questions about the risks and two student representatives of Google were present to address these concerns. They said the e-mail data would still be owned by the university and that Google would not access the information without its permission.

Ultimately, most students said the benefits of the Google service outweighed the risks. But committee members said while students often disregard such privacy risks when signing onto their own Google accounts, they were still matters the university had to consider seriously.

"Right now many of you are like, ‘It's not big deal. So what?’ and it's fairly benign," committee chairman Michael Ball said. "But at some point it might be something of concern in the future, you just never know."

And when the committee polled the audience on who wanted a Google account next year, hands went up all over the room. When asked who wanted the Microsoft system, only one student responded.

Junior biology and neurophysiology major Havi Schwav, who objected to Google as a provider, said she would prefer to stick to an on-campus e-mail system.

"I don't like going to big companies and who are going to take my information and use it for their own purposes," Schwav said.

However, Google campus ambassador and senior computer science major Jonathan Newmuis said in an interview after the meeting that Mirapoint comes with its own security risks, as well.

He said the system often gets flooded with spam and noted that scammers have taken student account information through their e-mails.
"I would feel a greater sense of security with a large and reputed corporation having access to the data," he said.

Committee members said the student responses reflected what they had seen in original feedback.

"Originally, it was all just Gmail, Gmail, Gmail," computer science and mathematics major Morgan Parker said after the meeting. "Now it's more of a more educated, informed thought process than the gut reaction."
University makes switch to Gmail provider

Students given the option of using Gmail’s service or signing up for an account on the email service

Senior staff writer

Published: Wednesday, March 30, 2011
Updated: Wednesday, March 30, 2011 00:03

Student email accounts will be switched from the outdated Mirapoint system to Gmail next year, but users concerned with potential security risks will be given a choice to switch to the system used by university employees, the Student Email Committee announced last night.

After several months of discussion and gathering student input, the faculty and student committee determined Gmail, overwhelmingly favored among students, was the best option for the university's student email system. The system will maintain its umd.edu branded identifier.

Committee members said the alternative — an account under the Microsoft Exchange program that faculty and staff use — would also be available to students who are concerned about their emails being subject to data mining. These concerns, which were discussed with students at a town hall forum earlier this month, did little to dissuade the student body from supporting a switch to Gmail.

"At the end, it was the students' input which led to the decision to outsource to Gmail," interim Vice President and Chief Information Officer Joseph JaJa wrote in an email to The Diamondback last night. "I strongly support the committee's recommendations."

Elizabeth Moran, a student representative on the committee who also serves as a business school legislator in the Student Government Association, said the final decision came down to how best to appease all parties — those who wanted Gmail and those who raised concerns about privacy and security.

"I've heard everything from, 'I might want to run for president in 25 years, and I don't want my information floating around in a cloud somewhere' to 'I'm working on government projects while I'm here,'” Moran said. “So I see this as the best of both worlds.”
Graduate Student Government physics representative Tomek Kott, who also sits on the committee, said having the secondary option is especially gratifying for graduate students, who may deal with research that requires a higher level of security and privacy than Gmail can provide.

Office of Information Technology manager David Barks noted the university will be working to ensure that the Gmail accounts, which will serve the majority of the student body, are as secure as possible.

"Security and privacy are of paramount concern, however we feel we can mitigate the risks with a solid contract and strong privacy and security policies and Google is willing to work with us on this," he wrote in an email to The Diamondback yesterday.

OIT has already begun to implement the switch to ensure that accounts on the Gmail host will be ready and available to incoming freshmen when they arrive at orientation in July and August, JaJa wrote.

"They've got a lot of work ahead of them," Moran said. "Now we just get to sit back and wait, and we come back in the fall, it will be ready for us."
Appendix 7: Security Standard to be Included in Contract with Google
These 2 new terms will be added to the base contract:

1.6 Security Standards. As of the Effective Date, Google abides by the security standards set forth on Attachment A ("Security Standards"). During the Term of the Agreement, the Security Standards may change but Google agrees that any such change shall not cause a material degradation in the security of the Services.

1.7 Security Breach. To the extent a state or federal security breach law applies to a Security Breach, Google will comply with the applicable law. To the extent no such law applies to a Security Breach, Google will notify Customer of a Security Breach, following the discovery or notification of such Security Breach, in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Google will send any applicable notifications regarding a Security Breach to the Notification Email Address.

Attachment A will be incorporated as part of the contract in its entirety.

Attachment A: Google Enterprise Products Security Standards.

1. **Personnel.** Google has, and will maintain, a security policy for its security personnel, and requires security training as part of the training package for Google security personnel. Google’s security personnel are responsible for the ongoing monitoring of Google’s security infrastructure, the review of Google products and services, and for responding to security incidents.

2. **Data Storage and Handling.** Google will maintain all data on Google-owned servers and disks. Google will replicate data across multiple systems, and will store all decommissioned disks in a secure facility until wiped or destroyed.
3. **Data Transmission.** Google will transfer all data via internet standard protocols. Gmail, Calendar, Docs and Spreadsheet, and Google Talk offer Customer the ability to encrypt data during transmission using SSL and TLS.

4. **Business Continuity Planning/Disaster Recovery.** Google will replicate data across multiple separate systems to enhance business continuity in the event of disaster and system failure. Google will maintain a data center infrastructure that is geographically distributed to enhance system redundancy. Google will also maintain a geographically distributed staff to augment system availability in the event of a disaster.

5. **Incident Response.** Google will monitor a variety of communication channels for security incidents, and Google’s security team will react promptly to known incidents.

6. **Computer Room Access.** Google will store all production data in physically secure datacenters. Google will restrict access to the datacenters on a need-to-know basis to authorized staff.

7. **Data and Application Security.** Google will logically separate data from different End Users from each other, and only data for an authenticated End User will be displayed to that End User. A central authentication facility is used across all applications to increase uniform security of data.

8. **Data Isolation and Architecture.** Google will store data in a multi-tenant environment on Google servers. Google will logically isolate data on a per End User basis at the application layer. Google will also logically isolate data on a per organization basis, and each organization will be given control over specific data sharing policies.

9. **Change Management.** Google will continue to employ a code review process to increase the security of the code used to provide the Services. Google will also continue to employ a security review process to enhance the security products in production environments.

10. **Server Operating Systems.** Google servers will use a hardened Linux implementation customized for the Google application environment. Google data is stored using Google proprietary algorithms to augment data security and redundancy.
11. **Access Control and Privilege Management.** Google employs a centralized access management system to control personnel access to Google production servers, and will only provide access to a limited number of authorized personnel. Customers or End Users must authenticate themselves via a central authentication system or via a Customer’s single sign on system in order to use the Services. Each application checks credentials in order to allow the display of authorized data to that End User.

12. **User Accounts.** Customer will have control over the creation, deletion, and suspension of End User accounts on Google infrastructure.

13. **Password Policy.** Customers can use their own password and authentication policy in conjunction with Service using the Google single sign on functionality.

14. **Network Connectivity Security Requirements.** Google will protect its infrastructure with multiple levels of network devices at multiple layers.

15. **SAS 70.** Google has obtained a SAS 70 type II audit report.

16. **Data Center Environment and Physical Security.** The following is a general description of Google’s various data center environments and efforts to ensure physical security in these environments.

   a. **Google Data Center Infrastructure.** Google maintains a vast number of geographically distributed data centers located primarily in the USA and the European Union.

   b. **Physical Security Staffing.** Each Google data center maintains a security organization responsible for all data center security functions 24 hours a day, 7 days a week. The security organization monitors Closed Circuit TV (CCTV) cameras and all alarm systems. Internal and external patrols of the data center are performed regularly. The data centers are housed in facilities that require electronic key access, with alarms that are linked to guard stations.
c. **Physical Security Access Procedures.** Formal access procedures exist for allowing physical access to the data centers. All entrants to the data center are required to identify themselves as well as show proof of identity to security operations. Valid proof of identity is a photo identification issued by Google and a governmental entity. Only authorized Google employees and contractors are allowed entry to the data centers. Data center managers must approve any visitors in advance for the specific data center and internal areas they wish to visit. Only authorized Google employees and contractors who permanently work at the data centers are permitted to request card access to these facilities. Data center card access requests must be made through e-mail, and requires the approval of the requestor’s manager and the data center director. All other Google employees and authorized contractors requiring temporary data center access must sign in at the guard station, present a Google badge (Google employees or contractors) or ID issued by their employer (authorized contractors) and reference an approved data center access record identifying the individual as approved.

d. **Physical Security Devices.** Data centers employ electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual’s access to perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual’s job responsibilities. All entrants to the data centers must pass through a mantrap. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. The CCTV equipment is connected by secure cables throughout the data centers. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

e. **Environmental Safeguards.**

i. **Redundancy.** The data centers are designed with resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks. Infrastructure systems have been designed to eliminate single points of failure. Dual circuits, switches, networks or other necessary devices are utilized to provide this redundancy. Critical facilities infrastructure at the data centers have been
designed to be robust, fault tolerant and concurrently maintainable. Preventative and corrective maintenance is designed to be performed without interruption of services. All environmental equipment and facilities have documented preventative maintenance procedures that detail the procedure and frequency of performance in accordance with the manufacturer’s or internal specifications. Preventative and corrective maintenance of the Google data center equipment is scheduled through a standard change process. Preventative maintenance is performed on all infrastructure systems according to documented procedures.
ii. **Power.**

a. The data center electrical power systems are designed to be fully redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for every critical infrastructure component in the data center. This redundancy begins with dual utility power feeds, primary and alternate, to parallel utility switchboards sized so that any one can provide power to the entire facility. The output power is routed to supply all building loads including uninterruptible power supplies (UPS), building and mechanical services, and heating, ventilation and air conditioning systems.

b. Backup power is provided by various mechanisms including, but not limited to UPS batteries. Backup power is designed to supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted for any reason, backup power is designed to provide transitory power until the diesel generator systems take over. In the event of unavailability of both electrical utility and diesel generators, backup power can provide emergency electrical power to run the data center at full capacity for up to 10 minutes.

c. Diesel engine generators are in place to provide power to critical equipment and customer loads. The generators are capable of providing enough emergency electrical power to run the data center at full capacity typically for a period of days. These generators automatically startup and are able to provide power within seconds in the event of a power outage.

17. **Firewalls and Intrusion Detection.**

a. Google employs multiple layers of network devices and intrusion detection to ensure that our external attack surface is protected.

b. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Many companies make extensive use of
third-party technologies (e.g., Network Intrusion Detection Systems - NIDS, Host-based Intrusion Detection Systems - HIDS) to look for known attacks against commonly-installed software, and Security Operations Centers (SOCs) to respond when they arise. We take a different approach by:

i. Tightly controlling the size and make-up of our attack surface through preventative measures;

ii. Employing intelligent detect controls at data entry points; and

iii. Employing technologies that automatically remedy dangerous situations.

c. Most of our Internet-exposed attack surface is comprised of Google-created software and the environment involves a large number of servers. Traditional IDS products are not economical, efficient or useful in these situations and we rely on smarter methods of detecting exploitation.

d. When we approach intrusion detection concepts, we break down our attack surface according to anticipated input vectors (i.e., how hackers will attempt to break in). Google’s hosting infrastructure is custom-built so we have the ability to tightly define our perimeter and the entrance points into our network. Some of the major areas of coverage that achieve the goals above are as follows:

i. As mentioned previously, the OS on every system is stripped down, modified, and hardened to minimize third party vulnerabilities on running systems;

ii. All IP traffic is routed through custom front end servers that detect and stop malicious requests;

iii. Traffic is examined for exploitation of programming errors via methods such as cross-site scripting, and high priority alerts are generated when such an exploit is found;

iv. To prevent buffer overflow attacks, all open source software that is Internet facing or that processes external data goes through several levels of code review, audit, and modification before allowed into production. All changes are contributed back to the open source community.

v. Systems are checked continually for binary modifications, and any unrecognized modifications are purged;
vi. Router ACLs are used to provide perimeter defense, and an internally routable IP space is used to make sure external connections are never made to internal systems;

vii. Layer 3 filtering is used to mitigate packet-level attacks.

18. **Internal Data Access Processes and Policies – Access Policy.** LDAP, Kerberos and a Google proprietary system utilizing RSA keys provides Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, customer information and configuration information. We require the use of unique user IDs, strong passwords, and carefully monitored access lists to minimize the potential for inappropriate usage of accounts. The granting or modification of access rights is based on a user’s job responsibilities on a need to know basis and must be approved by data owners. Approvals are managed by workflow tools that maintain audit records of all changes. Furthermore, it is Google’s policy to provide system access to individuals who have been trained and require this level of access to perform authorized tasks. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication at Google (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., Credit Card data), Google uses hardware tokens.

19. **Data Replication, Disaster Recovery, and Data Disposal.**

   a. **Data Replication.** Data redundancy is built into all database and file system architectures, and all data that is written to disk is replicated on separate systems. Docs, Spreadsheets and Postini database data is also replicated between multiple data centers to prepare for full data center loss. Such protections help ensure that a customer’s data is protected in the event of a disaster. In most cases, customers can also perform their own backups for individual message recovery or archival purposes. Through the mail gateway, a customer can intercept all incoming and outgoing mail, and these can be archived based on any customer criteria. Additionally, each component of the service generally has an API. As a result, an organization can typically pull data out of the service into their own backup whenever needed.

   b. **Distributed Data Center Architecture.** Google does not rely on just one datacenter to run our applications. We operate a geographically distributed set of datacenters to keep services running in the event of incidents and disasters at a single datacenter. All datacenters are connected via high-speed private links to ensure secure and fast data
transfer between datacenters. Datacenter locations are undisclosed to the public, and data centers are unmarked to ensure optimal data security. Google’s data center management staff is also distributed in multiple geographies to ensure around the clock coverage and system administration that is not location dependent.

c. **Deleted data.** After an End User confirms deletion of a message, the message in question is immediately deleted from the customer’s Google interface and the data is no longer accessible or recoverable by the End User. Pointers to the data on Google’s active and replication servers are removed. Dereferenced data will be overwritten with other customer data over time.

d. **Media disposal.** When retired from Google’s systems, every disk containing customer information is subject to a series of data destruction processes before leaving Google’s premises. Operational disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the drive’s serial number for tracking. Finally, the erased drive is released to inventory for reuse and redeployment. If, due to hardware failure, the drive cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the disk erase policy.

e. **Customer Data Removal from Google Enterprise Products.** At any time, an Administrator can delete an End User and their data from Google. Alternatively, an Administrator can suspend an End User or change their password such that their data is accessible to the organization but not the End User. Google provides APIs to most of its Enterprise applications so an Administrator may migrate End Users and data off of Google Enterprise Products at any point. For customer protection, a Google Enterprise product domain can only be cancelled and deleted by calling our support center. The support staff will verify the caller’s status as an Administrator and will delete the account. The account can take up to five days to delete within the system.