Is Email Really Private?
Some people have concerns about how to protect the privacy of their email. These concerns tend to be focused on using one email system or another to ensure email privacy. Unfortunately, this focus misses the area where some of the most serious threats to your email's privacy actually occur. The purpose of this is to explain where these threats actually occur.

The fundamental tool used by email systems to ensure privacy is encryption. Good email systems require that you send and receive email through an encrypted connection to their servers. This means that your communication to the server cannot be read by outsiders who might be eavesdropping on your connection. Because of this encryption, your email's privacy is subject to very little risk during the sending process.

The greatest risks to your email's privacy occurs on the receiving end. You have no control over how the person receiving your email could be handling it. She or he could be forwarding your email to other addresses, or sending it to other people. There is also a risk in the way that the recipient stores your email. The person could be making multiple copies and saving them to insecure devices, like laptops, PDAs, public desktop computers, or memory sticks. If an intruder happened to get access to one of those devices they would also have access to all of the emails you had sent that person.

Because these serious risks occur on remote email systems there is little you can do to protect against them. The best measure anyone can take to reduce the risks associated with email is to use it responsibly, with knowledge of its pitfalls and dangers. A good rule of thumb is, any conversation you feel comfortable having on a cell phone in public would be an appropriate conversation for email. You probably wouldn't talk about confidential information over a cell phone because you cannot guarantee the conversation's privacy. For similar reasons, some documents are too sensitive to send through regular University mail.

When using any communication system, you must strongly consider if it's level of privacy is adequate for your correspondence. Email communication poses risks to the privacy of your messages. Does this mean you should never use email, or never send information in email attachments? The answer to both of these questions is no. Email is a great form of communication, but before you send a message consider the consequences if its privacy is breached.

Has a Privacy Impact Assessment (PIA) on the potential risks of using Gmail been performed?
Yes, it has been completed, submitted and accepted by the Alberta Office of the Information and Privacy Commissioner.

Does the PIA include all Google Apps for Education applications, or is it limited to only the email and calendar apps?
The PIA considers all information and data flows and therefore includes all applications available through the University of Alberta Google Apps for Education service. These include Google Docs and Google Sites.
Does the US Patriot Act allow the US government to access my personal information?
Yes. The Patriot Act allows for the US Government to access personal information that is held or accessible by anyone within the United States or any US citizen by two different methods. The first tool which the US Government possesses is found in Section 215 of the Patriot Act. Under this section the relevant Government agency must apply to a court for an order allowing them to access the personal information in question. The information which can be collected pursuant to this court order is very broad. The second tool which the US Government has is found in Section 505 of the Patriot Act. It is under this section that the Government can issue National Security Letters whereby they can request that personal information be disclosed to them. The information can be accessed where it meets the following criteria: that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. No court order is necessary for a National Security Letter to be issued; however, the type of information that is retrievable is more limited than through that available in a Section 215 (see above) order.

How does the US Government's ability to access my personal information differ from the Canadian Government’s ability to do so?
In Canada, like in the United States, the Government has wide abilities to view personal information that is held in email accounts. The Canadian Government's ability to do this is found in various pieces of Canadian legislation including the Criminal Code, the Canadian Security Intelligence Service Act, the National Defence Act, and others.

The key difference between Canada and the United States is that, in general, the Canadian legislation requires that all warrants for the seizure of personal information must be issued by a judge. However, it still remains that the application to the court for this order/warrant will be made without the knowledge of either the holder of the information or the person who is the subject of the information.

There have been a number of recent bills introduced in the Canadian House of Commons which would increase the scope of information that is available to the Canadian Government and also decrease the number of restraints preventing the Government from accessing that information.

Should you wish to see further information regarding the Canadian system for intelligence gathering you can visit the website for The Office of the Privacy Commissioner of Canada and review a Position Statement produced by that office.

Does the US Government have access to intelligence and personal information that has been collected by the Canadian Government?
Yes, the US and Canadian governments readily share intelligence of this nature pursuant to bilateral agreements which have been entered into and pursuant to existing legislation which permits the sharing of information.
If I use Gmail will my personal information be more readily available to the US Government?
The information may be physically located in the United States, which would allow the US Government to obtain direct access to that information. If the information is located in Canada, the US Government would have to approach the Canadian Government to obtain that same information.

Also, information which is held in an email account has no guaranteed privacy. Any email exists not only in the account it has been sent to, but also in the account it was sent from, in any accounts to which it was forwarded, and likely on many servers which are situated in the United States. If an email user wanted to ensure that their account was not subject to US Government surveillance they would also need to ensure that those with whom they are corresponding have also ensured that their own accounts have no US exposure.

Is Google able to provide assurances to the University of Alberta and all of the potential Gmail users that they will not release personal information to the US Government?
The contract with Google provides the University assurances that it will not release any personal information unless it is required to do so by law. Where possible Google will notify the University of any requests/demands for personal information. Requests/demands for personal information will often include a requirement that the holder of the information not advise any other party, other than their own legal counsel, that such a request/demand has been made. The effect of this is that the University would have no notice of its information being accessed by the US Government.

Will the use of Gmail increase the probability that my name will be added to a no fly list?
It is not clear how the so-called no fly list is composed and therefore the University is unable to provide any comment on how or why any one person is added to this list.

Does the University's change to Gmail infringe on my privacy rights?
No. The Office of the Privacy Commissioner of Canada has reviewed similar scenarios where email is provided to an organization by a US based companies and has determined that there is not an automatic infringement of privacy rights. The Commissioner's findings provide a useful overview of the privacy implications where email is provided by a US based company and the University encourages any interested person to review those findings.