Guidance on the Use of Cloud Applications by Individuals

Many of us use “cloud apps”, whether we email through a Hotmail account, share photos through Facebook and Flickr, move documents between home and work computers through Dropbox and MobileMe, videoconference with colleagues and loved ones in different time zones with Skype and AIM, blog through WordPress and Blogger, upload our lives through video clips on YouTube or collaborate on writing a paper with Google Docs.

If we use these apps, it’s because they can save us time or money, or offer us the ability to do something we couldn’t do otherwise. As a bonus, it means someone else has to worry about those annoying computer tasks like backing up data, ensuring enough disk space, etc.

But the fact that your data is now in someone else’s hands has all sorts of implications, not all of them to your advantage, when there is no contract or agreement between the University of Scranton and the company offering the service.

Whether a given cloud app is appropriate to use for your University of Scranton activities (or even for your personal use) is a matter of understanding the risks and making an informed decision. This document is intended to help you be a savvy consumer of these services should you choose to utilize them in connection with University of Scranton activities.

Ground Rules

1. It is your responsibility to take privacy and security into consideration when making decisions about when it is and is not acceptable to use free/low cost services. All University and campus policies apply to all University data, whether on University of Scranton or non-University of Scranton systems. Most of these services typically include “click-to-accept” agreements that have not been reviewed or approved by the University of Scranton and so may introduce security risks for your information and to the University. If you need help assessing these risks, don’t hesitate to ask.

2. Restricted and confidential information must never be stored, received, processed or published on non-University of Scranton systems unless you have worked with the Information Security Office and/or the Office of General Counsel to ensure that a University of Scranton-approved agreement is in place that addresses information security and privacy requirements and

concerns. Similarly, don't rely on external information systems or services for critical University business processes unless a University of Scranton approved agreement is in place.

3. The University cannot protect the privacy of your communications if you use one of these services, as it has no control over what occurs outside its borders.

Situations in which non-University of Scranton services are (likely) inappropriate

The following are serious indicators of situations in which use of a non-University of Scranton service without a University of Scranton-approved agreement being in place is inappropriate. If one or more of these conditions apply to your circumstances, consider whether the University offers a solution you could use instead, or work with Planning and Information Resources to negotiate an agreement with the service provider before using the service.

a. You will be conducting University business that should not be disclosed to the general public;

b. Restricted or confidential information will be involved;

c. You need a high level of security;

d. Privacy is a concern;

e. There are things that wouldn't be acceptable for the company to do with your information;

f. The company will or may store data outside of the United States, or data will cross US borders to reach the user. For example, some of Google's data centers are not within US borders, potentially placing University data under foreign jurisdiction and possibly subject to inspection by foreign governments;

g. You have specific requirements for availability of data and electronic communications that the service can't guarantee;

h. Credit card data is involved;

i. It would be a problem if the service suddenly changes or is no longer available, either temporarily or permanently.

Issues to consider

When you use cloud apps, the non-University of Scranton company has access to your data, communications, account information, etc. A company may have entirely reasonable privacy, security and business continuity protections in place, but you shouldn't assume they meet the University of Scranton's standards. How important this is depends upon on your specific use of these services.

To help make this determination, consider the issues listed below. If any of them raise concerns, using a non-University of Scranton service without a University of Scranton-approved agreement in place may be ill-advised.

Privacy issues

Be mindful that your privacy and the privacy of everyone using the product or service are dependent on the non-University of Scranton company.

1. It is best to assume that whatever information goes to or through the service may become public. This includes records of activities of those using the service, such as who used the service, what they used it for and when, etc.

2. A company's privacy policy (linked from their web site) should detail what it will do with your information, including to whom they may provide information and to whom they will allow access. What permissions have you granted by accepting their agreement/Terms of Use?

3. If a subpoena, search warrant or other legal instrument is presented to the company to obtain information about you, you shouldn't expect to be informed. While some organizations will try to direct the requester to you/the University first, there is no guarantee that this will happen, and the vendor may even be legally prohibited from disclosing the request.

4. Companies can be acquired, change business models or go out of business. Even if you keep local copies of critical data, what happens to your data if, say, the company that was hosting your data shuts down?

Operational, Legal, and Contractual issues

1. When you sign up to use free/low cost services, you may be agreeing to terms and conditions, terms of service, and acceptable use policies that are different from the University of Scranton's. The company can attempt to hold you to what you agree to, even if it is just a "click-to-accept"-type agreement. Do you have delegated authority to enter into this type of agreement on behalf

of the University of Scranton? If not, you may be in violation of University policy if you "click-to-accept" the terms of use.

2. It is essential to ensure that ownership of University data remains with the University. Whenever you put data on a commercial service, ensure that the terms do not conflict with University policy or governmental contracts and grants in terms of data ownership. The Planning and Information Resources division can help with this.

3. Keep in mind that you may be required by the University to produce records relating to University business, including email, instant messages, files, etc., regardless of whether those records are stored on University or non-University systems or services. Using a cloud app does not relieve you of this obligation but may make it more difficult for you to comply.

4. There is no guarantee that deleted content or accounts will really be deleted. It may take awhile before the content or the account is completely flushed from all of the company's archives. Practices will also vary as to how long accounts may remain idle before the account and associated data are destroyed.

5. If the service is free or "click wrap" you probably have little or no recourse against the vendor if something goes wrong or they do something you don't agree with.

Acknowledgements and Further Reading

Most of this advisory document has been adapted from a document published by Jackie Reynolds, Director, Campus Initiatives, and Kent Wada, Director, Strategic IT and Privacy Policy, UCLA Office of Information Technology.

Resources

Anthony Maszeroski, Information Security Manager, Planning and Information Resources, x4226