Using Microsoft products may be unethical for universities

May 7 2014, by Adam Fish

Microsoft has been at the forefront of allegations regarding the NSA. Credit: rhonogle, CC BY

Universities and researchers all over the world have a problem with Microsoft. It's not just that the company forces expensive and dated software on customers. Using products like Microsoft's email service Outlook is potentially in breach of the ethical contracts researchers sign

when they promise to safeguard the privacy of their subjects.

The revelations about spying by the US National Security Agency and the UK's GCHQ have led people everywhere to ask whether their data is secure. But unlike many others, researchers face serious ethical implications if the answer is "no".

When a researcher wants to carry out a study, they have to run it past an ethics review committee. This committee does its best to ensure that scholarly practices protect the privacy and safety of research subjects.

Medical researchers gather sensitive information about our fragile bodies, psychologists about our minds, law scholars about our crimes, sociologists about our private lives.

In my research on media activists, I routinely write emails about hacking, counter-surveillance, revolution, and political protests. These emails contain suspicious keywords that could easily set off NSA computers. And even those that don't work in the same area can no longer be sure they are not being watched.

That Google, Apple, AOL, PayPal, Facebook and more handed information over to spy agencies was alarming but no company has allegedly done more to ensure that the NSA and GCHQ has access to private information than Microsoft – the company many universities including my own, hire for its document processing and email services.

Under the Prism programme, Microsoft is said to provide the NSA with "direct access" to personal metadata. Microsoft even helped the NSA circumvent encryption on Outlook and helped the FBI to "understand" how individuals remain anonymous on Outlook.

Microsoft also owns Skype and tripled the number of calls collected

when it linked up with the NSA under Prism.

I'm using Microsoft Word on my university computer to write this article and when it's finished, I will send it for editing using Microsoft Outlook. I use both these programs to write about and discuss private issues regarding my research subject's political convictions.

I have responsibilities towards them but can no longer guarantee that the content of my communications with them or about them is confidential.

If they are serious about ethical research, universities should consider abandoning the Microsoft suite of programs. They should instead use not-for-profit, transparent and highly encrypted software platforms that do not hand data and metadata over to governments.

This ethical dilemma goes beyond ditching the Microsoft Office suite. It should cause us to completely reconsider the way information technology is set up in universities. That includes the programs used to construct arguments to the networked systems used to distribute research findings to the for-profit cloud services used for data retention.

Knowing how committed universities are to Microsoft, I appreciate that this is a Swiftian modest proposal. The software represents years of investment in training, skill development, and licensing deals. Many of my colleagues struggle with Microsoft software as it is so any new software would almost undoubtedly cause rigor mortis in the university.

But practical or not, the NSA leaks should force universities to do something to ensure that we are not compromising private information.

Silicon Valley is currently in a state of remorse about its complicity in this global scandal but it is too little, too late. Scholars need to follow India's government in attempting to cease the use of Microsoft's hotmail

and Google's gmail for official communications.

Life after Outlook

Thankfully, network activists are developing encrypted, not-for-profit, transparent and technologically robust information systems.

The idea is already catching on. At Goldsmiths University in London, more than 250 people signed a petition earlier this year opposing what they saw as forced migration to Microsoft's cloud and email service. And IT professor Andrew Clement organised a teach-in at the University of Toronto, challenging his own institution to use encrypted alternatives to Microsoft.

Universities should leverage their trend-setting capacity to instigate a wholesale transition from compromised private systems to encrypted not-for-profit services.

This would have reverberations over the long term. Students would get used to these systems during their studies and continue to use them in their subsequent professional lives. As a lecturer who teaches about the potentials and pitfalls of our networked lives, I would welcome such an approach.

And if the ethical argument doesn't appeal, our university leaders might warm to the idea of dumping Microsoft by making a cost-benefit analysis.

Never mind the money saved on software and support, can you imagine the free publicity a university would get from the media if it led the charge? I can see the headlines now: "University drops commercial software platforms until government surveillance stops". Free press like that might just help us meet our enrollment quotas.

It's time to end our addiction to surveillance software.