MEMORANDUM

From:
Dominique Clément, dclement@uvic.ca, 250-686-6604, Assistant Professor and Postdoctoral Fellow, University of Victoria.

To:
Colin Bennett (chairpol@uvic.ca)
Richard Keeler (avpr@uvic.ca)
Andrew Rippin (arippin@uvic.ca)
Eric Sager (ewsager@uvic.ca)
Tom Saunders (histchr@uvic.ca)
Mary Anne Waldron (avpla@uvic.ca)

Date: 27 September 2007

Re.: BC Archives Audit of UVic Office

The British Columbia Archives recently contacted me about conducting an audit of my office at the University of Victoria and my home. The audit is to confirm my compliance with the Access to Personal Information for Research or Statistical Purposes agreement ('Agreement'). I have had several meetings with the staff at the Archives and I can now provide a more complete picture of the audit. I am sending out this memo to everyone who has been contacted thus far about this issue.

I apologize in advance for the long memo, but I thought it would help to start at the beginning to avoid any confusion. To summarize: At this stage I am confidant that the process set out by the archives is non-invasive and will not violate the integrity of my work/office. However, this new initiative does still raise serious concerns for the future, particularly for vulnerable researchers, and our community should be aware and alert to possible abuses.

Research Agreement

Individuals who wish to conduct research at the BC Archives using materials that contain personal information found in records covered by the Freedom of Information and Protection of Privacy Act, and the Youth Criminal Justice Act, are required to sign an Agreement. The Agreement stipulates how the material will be stored (e.g., locked filing cabinets, never left unattended, etc…) and commits the researcher to destroy the material within two (2) years unless an extension is approved in writing by the Archives. Section 7 stipulates the following: "I will permit BC Archives staff to carry out any measures deemed necessary to verify compliance with the terms and conditions set out in this agreement. Such measures may include, but are not limited to the following: On-site inspection of premises or computer databases to confirm that stated security precautions are in effect."

Background

Several months ago, an individual who had conducted research at the BC Archives was robbed. Their home computer, which contained research notes from materials covered by an Agreement, was taken. As a result, the British Columbia Information and Privacy Commissioner directed the BC Archives to implement two new policies. First, an addendum to the Agreement (Schedule A) now sets out specific requirements for storing and encrypting electronic data. Second, Mac Culham (Manager; Corporate Information, Privacy, and Records; Royal British Columbia Museum Corporation) was directed to conduct random audits every year to ensure researchers' compliance with the Agreement.

Audits

At this stage the process for conducting an audit remains largely informal. Mac Culham will conduct two audits each year, one in Victoria and one in Vancouver. The requirements for electronic and physical storage are partially explained in the Agreement. I have met with Mac Culham and spoken with his technical expert (both of whom will conduct the audit). Mac Culham will visit the University of Victoria and enter my office to confirm that the office has a locked door and that the physical records are kept secure (e.g., locked filing cabinet). He may ask me to show him some of the files, but he will not be looking through the cabinet himself. His technical assistant, Brant Brady, will then ask me to show him how I store and secure electronic data. Schedule A has recently been amended to require that all research data be kept on an encrypted flash drive or memory stick; no material can be kept on a computer. However, the audit will include a review of my computer to ensure it has anti-virus and spyware software. Brent Brady will not interface directly with the computer. He will ask me to demonstrate how I create files, add them to the memory stick, destroy the files on the computer, and clean the drive using security software. No individual files will be opened.

Sanctions

An individual who refuses to provide the auditors with access to their home/office, or is in violation of the Agreement, will have their research privileges at the BC Archives revoked. At one meeting it was suggested that all UVic employees would have their privileges revoked if the university did not ensure compliance with the FOI Act. However, this was pure speculation; it is ultimately the responsibility of the Information and Privacy Commissioner to determine sanctions. Still, I include this detail to stress two points: First, this process is still very new and it is unclear to everyone, including the auditors, how it will evolve. Second, such aggressive statements could easily intimidate some researchers, notably graduate students and new scholars, and force them to comply with potentially abusive practices.

Privacy Concerns and Intellectual Freedom

The process outlined above appears, at this stage, to adequately balance the government's need to ensure compliance with the Freedom of Information and Protection of Privacy

Act and the rights of the researcher. However, a great deal of this process is informal, and the University should keep a close eye on future audits.

First, the audit will only take place in my UVic office because I do not keep records at home. However, many independent researchers, graduate students, and faculty who do not have an office keep their research materials at home. Should we be concerned about government bureaucrats entering our private homes to conduct inspections?

Second, the audits will include people whose Agreements have expired to ensure that the material has been destroyed. This provision is extremely vague and it is not clear at this stage how it will be enforced. Moreover, individuals at UVic who signed agreements several years ago may not be aware that they are in violation of the Agreement if they never destroyed their private notes. At the very least, the UVic community should be warned about possible audits.

Third, Schedule A requires that all BC Archives material be kept on a memory stick. However, the auditors will insist that they review the individuals' computers to make sure that the computers contain the proper security software to protect against viruses and hackers. Once again, this provision is vague. Any personal or campus computer that comes into contact with the memory stick is subject to the audit at the whim of the auditor.

Fourth, the audits will likely be limited to researchers in Victoria and Vancouver. Is this a fair and legitimate formula for randomly selecting candidates for audits? Should a fair process not include anyone who signs an Agreement, or at least the entire province?

Fifth, I have an informal understanding that the audit will not involve inspecting my personal notes (written or electronic). However, the Agreement does stipulate how notes should be taken (e.g., not replicating any case file numbers or identifiers found in the records). It is possible that future audits will include a detailed review of private notes. At the very least, our community should be cautioned against what they write in their files and be aware that an outside source will review their notes. Unfortunately, this means that scholars may have to self-censor their personal notes if they wish to keep them private.

Recommendations

I would suggest the University take at least two actions at this stage:

First, a clear set of guidelines (brief, non-technical and accessible) should be produced by the University of Victoria. The guidelines should explain to staff, students and faculty how to remain in compliance with the Agreement (e.g., recommend specific anti-virus and spyware software, list contacts for technical support on campus, and remember to destroy notes) and clearly explain a person's rights during an audit. For instance, the guidelines could encourage scholars at UVic to keep their records on campus to avoid home audits. The guidelines could also warn scholars to be aware of potential abuses.

These guidelines should be linked to the UVic main website, as well as on Faculty (Social Sciences, Humanities) and individual Department websites. New scholars to UVic should be encouraged to review the guidelines.

Second, the University should consider writing a formal letter to the Freedom of Information and Privacy Commissioner asking the Commissioner to develop written guidelines on the audit process to supplement the current Agreement. It should be clear how individuals are selected for an audit and what will take place during the audit. The Archives should explain, in writing, how to obtain an encrypted memory stick and proper security software. For instance, researchers should be aware that the auditors may reject open-source software if it is undependable. Moreover, I am concerned about the implications of home audits. Graduate students, in particular, could easily be compelled to allow officials to search their homes. Perhaps the Commissioner would be satisfied with allowing researchers the option of bringing their home computer and memory stick to the Archives for inspection, and signing an additional contract that clearly states that any physical files at home are kept in a locked cabinet.