REVIEW OF UBC'S PROCESSING OF FREEDOM OF INFORMATION REQUESTS

Report to the University Counsel

David Loukidelis QC

March 2016

INTRODUCTION

This report flows from my review of the policies and practices of the University of British Columbia in responding to requests for access to records under the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The University Counsel, who oversees FIPPA compliance, initiated the review in February 2016. He did so in the wake of UBC's inadvertent disclosure, in January 2016, of personal and other protected information. The disclosure occurred when UBC posted on its website electronically-redacted records in response to several access requests. It turned out that the records contained hidden attachments which could be accessed through links embedded in the records, disclosing third-party personal information that should have remained confidential. A material amount of this personal information has been published in various media reports.

It became readily apparent during my review that all UBC employees involved in the processing of access requests take their jobs seriously and are conscientious about their work. This is not the first time a public body in British Columbia has inadvertently disclosed protected information, including third-party personal information or third-party business information. These incidents illustrate the risks involved in processing requests that involve third-party personal information and other protected information.

These incidents all underscore the need to ensure that requests are handled in a manner that mitigates as far as reasonably practicable the risks of inadvertent disclosure. As regards personal information, the mitigation of risks is a facet of the duty of public bodies under FIPPA to implement reasonable security measures to guard against unauthorized access to or disclosure of personal information. There is no such duty in FIPPA in relation to third-party business information, but confidential business information that third parties have entrusted to public bodies surely merits protection against unauthorized disclosure. There are also important public interest considerations in protecting information that has properly been withheld from accidental disclosure.

It is, of course, not possible to eliminate all risk. But it is important for all public bodies to ensure that their access request response processes meet evolving risks. Continual review is necessary, as the UBC incident illustrates. New technologies for handling of access requests hold great promise for public bodies that struggle to keep ahead of increasing demands for information and more complex situations. This incident should not deter UBC or others from embracing these technologies. It does show, however, that UBC and others have to ensure that their policies and practices in using technology identify risks in using them and meet the risks.

One goal of my review has been to identify what happened, but a key goal is to make recommendations that reduce the risk of inadvertent disclosures down the road.

Another objective of my review has been to make any recommendations that I consider desirable to further enhance the efficiency and timeliness of UBC's processing of access requests. Periodic review of access request processes is necessary as a matter of good administration and this incident has given UBC the opportunity to examine the efficiency of its processes through this review.

All UBC staff co-operated fully with my review and their co-operation is greatly appreciated.

SUMMARY OF QUALIFICATIONS

British Columbia's Information and Privacy Commissioner from 1999 to 2010; British Columbia's Deputy Attorney General and Deputy Minister of Justice from 2010 to 2012; Registrar of Lobbyists for British Columbia from 2003 to 2010.

Currently Privacy Commissioner, Ad Hoc, for the Office of the Privacy Commissioner of Canada; Information Commissioner, Ad Hoc, for the Office of the Information Commissioner of Canada; and Chair of the Law Enforcement Review Board of Alberta.

Taught privacy and freedom of information law in the Faculty of Law at the University of Victoria; the Faculty of Law at Thompson Rivers University; and the Faculty of Law at the University of Alberta (prospective: autumn 2015 term).

Principal of David Loukidelis QC Consulting & Legal Services, providing advice in these areas: freedom of information law; privacy law; open government and open data; lobbyists registration law; government ethics law; technology law; administrative law; public policy and legislation; tribunal operations and administration; justice system administration and reform; and public administration.

BCL from the University of Oxford; LLB from Osgoode Hall Law School (York University); MA in English Language and Literature (Medieval Studies) from the University of Edinburgh.

Clerked for a Justice of the Supreme Court of Canada before becoming a lawyer in British Columbia in 1985. Appointed Queen's Counsel in British Columbia in 2010.

REVIEW PROCESS

The review involved assessment of UBC's documented procedures and practices for processing access requests under FIPPA. To this end, UBC provided copies of all relevant policies and procedures and these were reviewed for completeness and currency.

In addition, on-site interviews were conducted at UBC. This included an interview of UBC's Legal Counsel, Information and Privacy, the Freedom of Information Specialist and the Freedom of Information Assistant. These interviews enhanced understanding of the processes followed, and the issues encountered, in handling typical access requests.

In addition, practices of other public bodies in British Columbia in publicly disclosing information already disclosed to individual access applicants were considered, as were UBC's other pro-active transparency initiatives.

HOW REQUESTS ARE PROCESSED

UBC's approach to processing access requests is consistent with the practices of other public bodies. There are five main phases to a response: receiving the request (or, intake); searching for records; preparing records for review; review of the records and severing of protected information; and disclosing the records to the applicant.

The following summary breaks these phases down into the typical constituent steps. Other steps may be involved in addition to the above. They may happen at different times, which is why they are not included as part of the following chronologically-typical response process. For example, UBC staff regularly communicate pro-actively with the applicant where the request is very wide or vague. They may do so at the outset, upon receipt of the request, or they may do so later, if it is not clear at first what volume of records may be responsive. They do this to see if the applicant's needs can be met by narrowing the request's scope, or clarifying the applicant's goals. This is a commendable practice, which can yield better and more timely responses and save processing resources.

Receiving the request (intake)

1. UBC staff determine whether the request is a request for access that falls within FIPPA's scope.
2. If staff determine that the applicant is seeking access to third-party personal information, they look for a consent validly signed by the third party. Consent will reduce the processing effort needed.
3. If staff determine that the applicant is seeking access to her or his own personal information, they require proof of identity.
4. Staff assess whether, as FIPPA requires, the applicant has given enough detail to enable UBC to, with a reasonable effort, identify the records sought.
5. The details of the request itself are entered into UBC's case management system, FOI Tracker (a Microsoft Access database).
6. The request itself is stored in a UBC server.
7. An acknowledgement of the request is sent to the applicant.

Searching for records

1. Based on their knowledge of UBC's administration, administrative structure and information holdings, staff email relevant UBC departments or units asking that they conduct a search

for records. The email sets out the terms of the request (but not the applicant's identity). UBC staff maintain a list of contacts in each UBC department or unit.
2. At this time, UBC staff assess whether fees should be charged for the request. If so, a fee estimate is given to the applicant.
3. Staff follow up on search requests in order to ensure the maximum possible timeliness.
4. Records are received from the target departments or units and receipt is confirmed for them, again by email.

Preparing the records for processing

1. Records that are received in paper format are scanned and the electronic versions are saved in UBC's server.
2. These electronic copies are converted to Adobe Acrobat PDF format and saved in the server. Records received in electronic form are also converted to Adobe Acrobat PDF format and saved in the server.
3. Each record is renamed and saved by date in a separate folder under each request.
4. Responsive records may come from disparate UBC sources. These are generally combined in chronological order and saved as a package. (Some kinds of records are kept separate, such as payroll records or timesheets, as these cannot sensibly be separated and then combined with other records.)
5. Records are cleansed of all embedded links and metadata.

Reviewing records for release

1. Any third-party is identified and, where necessary in accordance with FIPPA, formal third-party consultations are conducted in accordance with FIPPA.
2. Also at this stage, staff consider whether, due to the volume of records or other relevant factors, it is necessary to extend the response time. If it is, the extension is taken.
3. Line-by-line review is undertaken and information that must or may be withheld is identified and marked for severing.
4. Each page of the responsive records is numbered.
5. Staff ensure that each box within which information has been severed is marked with the appropriate FIPPA exception number.
6. The marked-up, severed document is saved as the release record, again in a UBC server.

Disclosing the records

1. The response letter to the applicant is drafted, then signed.
2. Where appropriate, advance notice of disclosure of information in response to the request is given by email to select UBC officials.
3. The release copy of records is secured against alteration by others.
4. The release copy is encrypted with a robust password if the release is to be emailed and it contains personal information.
5. The response letter and release copy are sent to the applicant, often by email.
6. Copies of the access request and the released records are uploaded to a dedicated internal UBC Microsoft SharePoint site.

HOW THE INCIDENT OCCURRED

This section outlines how the incident happened.

UBC converts all records into PDF documents in order to use its redaction software, which is an add-on to Adobe Acrobat. The conversion process does not remove any embedded information in PDF documents (*e.g.*, metadata, email addresses, hidden attachments). To remove this hidden information, it is necessary to 'sanitize' the document using a special feature of the redaction software. This step is, of course, separate from the severing of protected information, also known as redacting.

Unfortunately, because it is not always obvious that a file contains embedded information, it is possible to overlook the sanitizing step. This is what happened in this case. Because the document had not been sanitized, individuals were able to click on links within the documents and open hidden attachments, some of which contained sensitive information.

UBC's system for sanitizing documents before release is reasonable. The incident occurred because of a simple mistake. If the sanitizing step had not been missed in this case, with the added factor of publication on the internet, there would have been no disclosure of third-party personal information.

Honest mistakes happen, and the next section makes forward-looking recommendations to prevent further such incidents.

OBSERVATIONS & RECOMMENDATIONS

Request processing: observations and recommendations

The review disclosed that UBC's processes for responding to access requests meet FIPPA's processing-related requirements and sound practice. No specific changes to UBC's processes are necessary at this time, although UBC should, of course, periodically review its processes to keep pace with legislative change and changes in request patterns and technology.

As a matter of overall context, the review disclosed that UBC receives a large number of access requests each year compared to other universities or similar institutions, whether comparing against budgets or full-time employees. Related to this, UBC's access to information staff process a large number of access requests each year, substantially more than staff in other universities or the provincial government on a comparative basis, per staff person. Accordingly, UBC should consider whether the level of funding that it has committed to its access to information function is commensurate with the demand. This is also discussed below.

Although it is outside the scope of the review, it should be noted here that UBC's web-published guidance on access requests is commendable. The UBC website offers good guidance for access applicants, notably in relation to specialized requests it routinely receives, such as students' requests for their academic record or requests from employees for their own employment records. It is nonetheless recommended that UBC periodically review this guidance to ensure that it is up to date, complete and clear.

Another matter that UBC could review is the nature and scope of its pro-active publication of information. At present, UBC routinely publishes a wide range of information on its website. To give only a few examples, it publishes financial reports, board of governors meeting minutes and agenda packages, information technology reports, strategic planning materials, and summaries of student discipline decisions. It also publishes quarterly lists of access requests it has received. This is all commendable, but, as with request processing practices, UBC should periodically review its routine disclosure practices to ensure that it is being as open and transparent as possible.

One area in which UBC should take care, however, is publication on the web of the contents of disclosure packages. This review was prompted by the public posting of a disclosure package, leading to inadvertent disclosure of personal and other information. This incident illustrates that extra care is needed to vet disclosure packages, to ensure that third-party personal or protected business information, or other information, is not accidentally disclosed to the world

at large. Accidental disclosure to a single requester is a concern, but in such cases it is more likely UBC would be able to retrieve the information safely. This is not the case with web-posted information, of course.

The risk is not merely technological, as was the case here. The well-recognized 'mosaic effect' might be a concern in some cases. It might be possible for a member of the public to piece together personal information, for example, from a properly severed disclosure package, using other information that is available to that person or to the world at large. These cases are not likely to come along very often, but they cannot entirely be discounted.

Another consideration is the extra demand on UBC's access to information resources that would flow from routine publication of all disclosure packages. Rather than consider doing this, it is recommended that UBC continue to publish disclosure packages only where it concludes that the public interest warrants it (as was done here). In these cases, UBC should ensure that a disclosure package is not disclosed unless it has been vetted at least twice to ensure that no third-party or other protected information will be exposed.

Electronic severing of records: observations and recommendations

After this incident, UBC made changes to reduce the risk of further processing errors. It is now the practice that records are sanitized at the start of the process, as soon as they are received. The sanitization therefore happens before information is severed. UBC has had the new process tested by a Montreal-based computer forensics company, which has not been able to recover any sanitized information. Unfortunately, UBC staff advise, this new method is more time-consuming than the previous method, for technical reasons.

UBC has also anticipated a recommendation that would have been made here, which is to implement a step-by-step checklist, to ensure that all steps are followed in each case. This checklist should continue to be used.

Another change is that UBC now requires a second staff member to check record packages containing sensitive information, to ensure that protected information has properly been sanitized. This should continue, acknowledging that this change is time-consuming, and will put significant further strains on existing staff resources. On the question of resources, it is recommended that UBC assess whether, given the high volume of requests processed by the two staff members, further staff resources are needed.

Last, UBC should monitor relevant technical developments on an ongoing basis, to help ensure that its approach to electronic severing is not compromised by technological changes.

CONCLUSION

UBC's accidental release of personal information and other information by publishing a disclosure package online illustrates the challenges in being open and transparent while protecting third-party interests. As this report underscores, the disclosure was an accidental result of UBC's good-faith attempt to be open and transparent. UBC has already taken steps to prevent this from happening again, and this report makes several recommendations intended to help ensure there is no future occurrence.