Canadian Association of University Business Officers

Emergency Preparedness Workshop, March 27, 2008

"A Legal Perspective On Managing the Threat of On-Campus Violence"

Dan Michaluk, Hicks Morley Hamilton Stewart Storie LLP

The following was drafted informally as my speaking notes. It also only contains general information on issues that are very complex, is not legal advice and should not be relied on as a legal opinion. Readers who need advice or assistance with a matter should contact a lawyer directly.

SLIDE 1 - ROADMAP

Good morning. [Thank you.] Hicks Morley is counsel to many universities in the Ontario system, and I am a lawyer at Hicks who specializes in information and privacy law. This has allowed me the pleasure of working on some very challenging issues in university administration, including the issue that I'll address today – the legal perspective on managing the threat of on-campus violence.

Shortly after the Virginia Tech shootings last April, my colleague Catherine Peters and I wrote a short article called, "Maintaining Balance." It's the one in your materials. This was

our response to some of the early comments on the shooting. Some commentators were saying that privacy and human rights regulation actually **stopped** the University from preventing the attack.

We wanted to tell our clients that this is certainly **not** the case in Ontario. And we wanted them to feel empowered to act.

***

Now I have to say right up front that managing a student body at a university has to be one of the hardest jobs around. Think of the ambiguities.

- Students aren't children, but they're also not adults
- Parents fund their children's education but don't have parental rights
- Campuses are neither fully private nor fully public spaces

This makes our task more complex but it also makes balancing the various legal duties difficult – those duties (which I'll discuss today) are primarily based in human rights, privacy, health and safety and negligence law.

Does the complexity mean that we should do nothing in the face of a real risk?

No!

We can act and, in fact have a duty to act. That's what I'm here to talk to you about today. Here's our roadmap.

daniel-michaluk@hicksmorley.com

- I'll start with a relatively detailed description of what happened at Virginia Tech

The Virginia Tech shooting is a case study that outlines the need for institutions to share information as a prerequisite to making good decisions in managing students at risk. You'll see that at Virginia Tech information that might have triggered some form of management and accommodation process was known by parts of the University but wasn't transferred to the decision-making body charged with responsibility for managing students at risk.

***

Then I'll spend the rest of my time presenting a model of information flows in three parts.

- risk assessment
- medical monitoring
- threat advisories

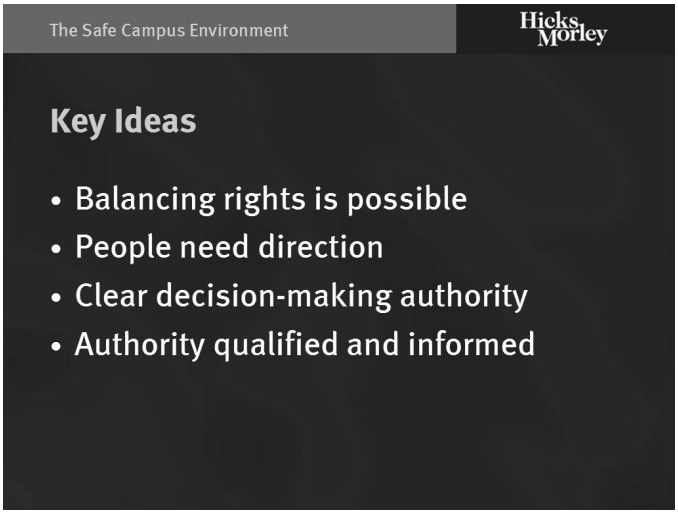
I hope that at the end of this presentation you will have an understanding the types of policy options that are available to you to manage the threat of violence while **fully-respecting** your privacy and human rights related duties.

A few housekeeping notes. First, I'm going to refer to Ontario law because I'm most familiar with the nuances of Ontario privacy legislation. I do believe that the concepts I'll discuss will be relevant to those of you from the other provinces. Second, I don't have many slides to speak to – maybe about 45 minutes worth – and then would be happy to open the floor to questions. Finally, [note materials on blog].

daniel-michaluk@hicksmorley.com

Let's move on.

SLIDE 2 – KEY IDEAS



Now I've talked about my empowerment goal, another theme in this presentation is that this problem **must** be solved by policy.

Not to exclude employees, but let's think about who it is in our campus community who knows students best. Think of the front-liners – especially the teaching staff. If it's hard for you, as an expert, to understand what you can and cannot do about violence because of privacy and human rights regulation, how are the laypeople in your community to know?

Here's what the panel that looked into the Virginia Tech shootings said about how people are inclined to act when they learn that a student has a problem:

> The widespread perception is that information privacy laws make it difficult to respond effectively to troubled students. This perception is only partly correct. Privacy laws can block some attempts to share information, but even more often may cause holders of such information to **default to the nondisclosure option**—even when laws permit the option to disclose. Sometimes this is done out of ignorance of the law, and sometimes intentionally because it serves the purposes of the individual or organization

daniel-michaluk@hicksmorley.com

> to **hide behind the privacy law**. A narrow interpretation of the law is the least risky course, notwithstanding the harm that may be done to others if information is not shared.

Yesterday Dr. Klassen and Dr. Wood both raised the natural discomfort people have in stepping into someone else's affairs. Though reports of concerning behaviour are made every week (and maybe every day), there are also students who are going unmanaged because people either choose to ignore the obvious signs that they are at risk or are mistaken about their ability to do something about it.

You may have heard about the proposed amendments to the United States FERPA regulations proposed on Monday by the United States Department of Education. These have been promoted as "clarifications" of rights that were already there but not clearly spelled-out. As far as I can tell, what they do is clarify that parents are "appropriate" persons to disclose to under the FERPA health and safety exemption and also clarify that the regulator will defer to an institution's disclosure decision under the provision where there is a "rational basis for the determination" that the exemption applies.

Here in Ontario, neither our privacy legislation nor our human rights legislation clearly spells out what you can do to with information to manage students at risk. So to provide a truly safe campus you really **must** provide clear guidance and direction. I call this a "command and control problem": there is very little time to make a decision and the threat of harm is acute. Directive policy is key to risk minimization. Think of McMaster's orange folder and Waterloo's QPR – Question, Persuade, Refer – campaign. These types of initiatives are what's required.

daniel-michaluk@hicksmorley.com

Which leads to another theme in this presentation – good decision-making structures. One of the challenges with universities is that they're large decentralized institutions with multiple departments and an arguable bias towards collegial decision-making. You've got student affairs, security, facilities, academic departments and divisions (schools) and maybe some other areas with jurisdiction over this challenge. Not only do the **right** people have to have the **right** information, the relationship between these people must be structured so they can make **rapid** decisions.

SLIDE 3 – LEGAL DUTIES

Let's quickly go through the four legal duties that govern the ways in which you can manage the risk of violence.

- Duty to provide a safe campus environment

First, you have a duty to provide a safe campus environment. For **employees** on campus, this is derived in part by occupational health and safety legislation. In Ontario, employers have a duty to take every precaution reasonable in the circumstances for the protection of a worker. For **students**, the duty is derived from the student contract or the common-law of negligence.

Now there are some debates about the scope of the common-law duty – you may have heard about the *MIT v. Shin* case, and there has also been some excellent academic work done by Robert Bickel and Peter Lake in their book, "The Rights and Responsibilities of the

daniel-michaluk@hicksmorley.com

Modern University." While there may be some fine points in your policy-making that demand a close look at the duty of care issue and lots of issues fit for litigation, for the most part university policy making ought to be driven by an assumption that you have a very broad duty to protect students and employees from all reasonably foreseeable harm. That, after all, is why we are here today.

- Duty to provide a harassment free campus environment

Second, you have a duty to provide a harassment free campus environment. If you're typical of most universities in Ontario you probably have a safe campus policy and a harassment policy. The focus of my comments are on controlling the threat of violence, which is typically addressed by your safe campus policies. But it is very important to acknowledge the obvious link between violence, students at risk and the problem of harassment. In fact, as you'll hear, at Virginia Tech the shooter was first identified as a student at risk because one of his professors thought she was a victim of his bullying. You'll also hear that in the same semester the shooter was reported for several incidents of e-mail harassment.

So there lies the link. It seems strange to say, but harassment events are opportunities for identifying and assuming control over potential threats. You can generally respond to a harassment complaint three ways: (1) you can conflict manage it (usually when there are weaknesses in the complaint); (2) you can respond with discipline (usually for culpable behaviour) or (3) you can respond with non disciplinary management. If there are weaknesses in the complaint or other reasons for not proceeding with discipline we still

daniel-michaluk@hicksmorley.com

should be sensitive to the separate potential need for non-disciplinary management of potential threats.

- Duty to protect personal privacy

Third, you have a duty to protect personal privacy. The primary source of this duty at Ontario universities the *Freedom of Information and Protection of Privacy Act*. There is also the *Personal Health Information Protection Act*, which essentially applies to information generated in the course of a health care relationship.

These statutes regulate the collection, use and disclosure of student personal information. They are extremely technical statutes and are often misunderstood, but what you'll get a sense of today is that FIPPA and PHIPA do **not** prevent universities from doing what they need to do – and necessity is always the basic test – to manage students who are at risk of perpetrating acts of violence.

- Duty to provide reasonable accommodation

Fourth, you have a duty to provide reasonable accommodation – which is often part of the analysis because students at risk often suffer from mental disabilities. I'd like to make two empowering comments about the duty to accommodate.

First, human rights law does not prevent us from taking steps to control students at risk. You must, however, respond in a manner that is compassionate and consistent with the mandate of human rights legislation. Conceptually, you are offering individuals at risk with a package that allows them to participate in the educational experience (or work) on

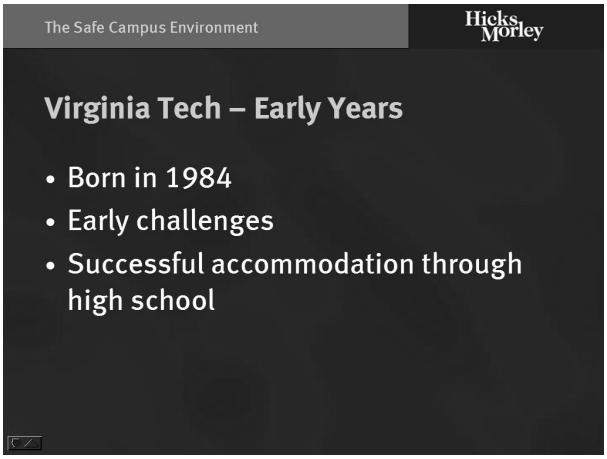
daniel-michaluk@hicksmorley.com

conditions that you deem to be reasonable. Security-related considerations should not be sacrificed – I completely concur with Dr. Klassen on this point – but we must be a problem-solvers when managing people with mental disabilities… be helpers… We must not embrace the management task with a heavy hand … and we must try our very best to avoid reacting to the uncooperative front the individuals we are managing often take. And when we actually **do** embrace the spirit of accommodation and the individual we are **trying to help** doesn't accept the help or simply wants more we can eventually say **NO** and be quite justified in doing so.

This leads me to my second empowering point – individuals who claim accommodation have a competing duty to cooperate, and this includes a duty to provide information that's "reasonably necessary" to the provision of accommodation. I'll come back to this when we talk about medical monitoring later.

daniel-michaluk@hicksmorley.com

SLIDE 4 – VIRGINIA TECH (EARLY YEARS)



Let's move on to Virginia Tech as a case study. I don't take any particular pleasure out of putting the Virginia Tech administration under a microscope, but it is a good case study. The reality is that this could happen to any of us and we're lucky to have an opportunity to learn from what did and didn't happen there. This is all taken from Chapter 4 of the Virginia State report on the incident. You can find it by Googling "Tim Kaine," the governor of Virginia, or you can link through my blog, which you'll find by Googling my name.

Here are some details about Cho's childhood. Why are these important?

Well, part of my message is that student human rights and campus security don't conflict. And I always have said this, but until I read Chapter 4 I had never **felt** this point so strongly.

Now we know that Cho did a terrible, terrible thing. He's a killer and this must not be forgotten.

But the story of Virginia Tech starts with Cho as an infant with a medical problem – and he's as innocent as any infant can be. I have a ten month old of my own and I thought many times when I read Chapter 4, "This could be my child."

***

daniel-michaluk@hicksmorley.com

At nine months Cho was hospitalized for a problem with his heart. This problem was eventually solved with surgery at around age two, but ever since that point he was frail, withdrawn an introverted. And when he moved to the United States at age 9, he was soon after diagnosed as having a severe social anxiety disorder.

And then we go to high school. And what's remarkable about Cho's time in high school is how well he's doing. He had an incident when he was around 13 where he wrote that he wanted to "repeat Columbine." At that point he is medicated and starts a program of regular counselling. All the while, his high school educational program is modified and he's got his parents and his sister providing close support. Cho graduates without significant incident and with good marks, and despite his parents' urging to live closer to home, chooses to go to Virginia Tech.

So we've got this picture of successful accommodation of mental disability at high school.

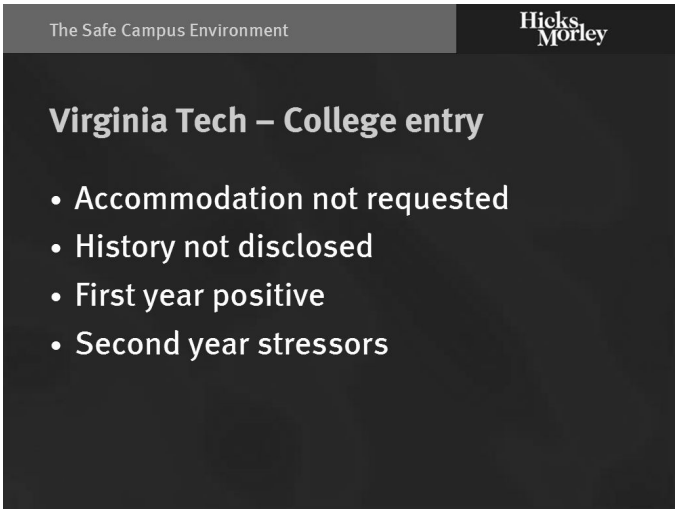
SLIDE 5 – VIRGINIA TECH (PAUSE FOR THOUGHT)

After hearing Mr. Fillion's inspirational speech on the response to the Dawson College shooting yesterday, I decided to put this picture of my son on this slide, not just because I'm a proud father, but because its an effective reminder of the approach we need to get this right. I'll stress again that the hardest thing about managing individuals at risk is that its easy to lose perspective and slip into an adversarial dynamic. If you can

daniel-michaluk@hicksmorley.com

maintain a compassionate perspective – think of a Cho as that young child – you'll make decisions that are **firm** on security and **fair** on the person. I may be the only lawyer ever to tell you that its okay to make decisions with your heart, but I think we can also draw upon Mr. Fillion's idea in tackling the prevention of violence.

SLIDE 6 – VIRGINIA TECH (COLLEGE ENTRY)

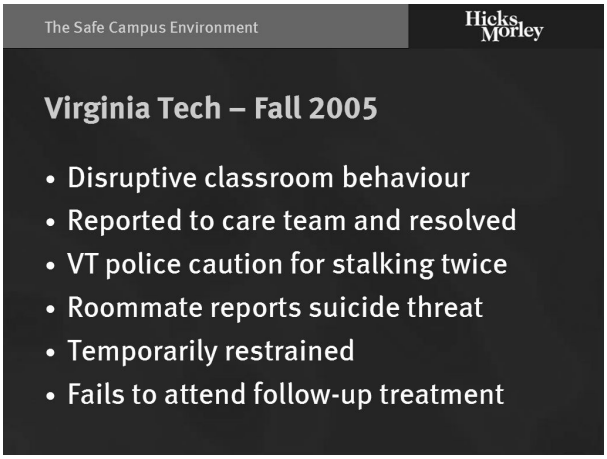


We see in the Virginia Tech case study the healthy accommodation of Cho came to an end when he went to university – a very large **institution**. All the supports that were there to help Cho through high school were gone. The records of his individual education plan at his high school are not transferred to the University, nor is the University made aware through its registration process that Cho has any special needs at all. He's moved away from his parents and sister and of course he experiences all the typical stressors that first-year students experience.

Notwithstanding this, in his first year Cho exhibits no particular behaviour that would cause him to be identified by the Virginia Tech administration.

daniel-michaluk@hicksmorley.com

SLIDE 7 – VIRGINIA TECH (FALL 2005)



It's fall 2005 when Cho is first brought to the University's attention.

And the very first incident was the only incident that was reported and dealt with by the University's multidisciplinary care team. This was an incident in which one of his professors asked for Cho to be removed from class for his disruptive behaviour:

- he refused to take of his glasses and kept his hat pulled down over his face
- he read aloud a paper that had a general threat to the members of his class ("I hope you all burn in hell…")
- he took pictures of other students with his cell phone
- and his professor felt she was being bullied.

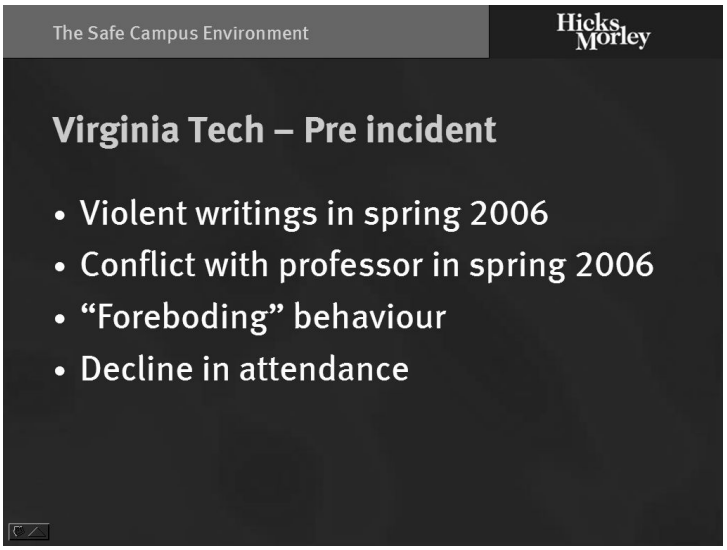
This looks like it was approached as an interpersonal conflict rather than campus safety, because the solution was to remove Cho from the professor's class and provide individualized education.

It also does not appear to have been approached as an issue of accommodation. Even though his writing was shared with a counsellor who recommended that he enter a program of counselling, Cho was not put under any continuing program of accommodation or care.

daniel-michaluk@hicksmorley.com

Later on that fall it gets worse. Cho is cautioned for stalking two individuals by campus security. Only days after the second caution his roommate reports that Cho has made a suicide threat and he's temporarily restrained overnight. He is released by a judge who orders him to attend counselling at the University's health clinic. Cho attends the clinic as ordered and is triaged but there was never any follow-up treatment. Importantly, no information about Cho's hospitalization or the court order is transferred to University's care team by the court or campus police (who initiated the detention).

SLIDE 8 – VIRGINIA TECH (PRE-INCIDENT)



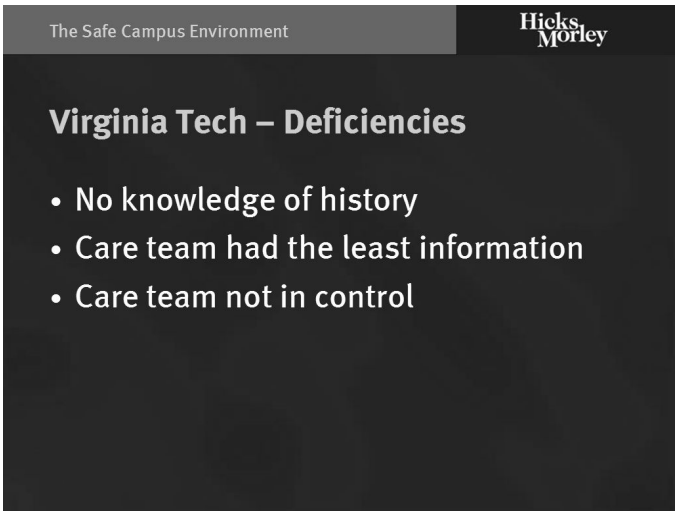
Now that really rough period of time was in the fall semester of Cho's second year (in fall 2005). We know that the shooting happened in April 2007, **over a year and a half later**.

During that year and a half Cho is not on a treatment program and not being formally monitored. We do know that he was working closest members of the University's English department. In the follow-up to the shooting they reported strange foreboding behaviour and very violent writings, none of which led to any formal response. One writing that has now surfaced was about a student who was struggling with whether or not to kill every person in his school. The student meets a female compatriot and the story ends with the line, "You and me. We can fight to claim our deserving throne." And then, in

daniel-michaluk@hicksmorley.com

the weeks leading up to April 2007, the English department would have been in custody of information showing a decline in Cho's attendance.

SLIDE 9 – VIRGINIA TECH (DEFICIENCIES)



And then we all know what happened.

Now there are a number of lessons that come out of Virginia Tech. Some relate to emergency management, some relate to the need for better mental health services on campus and some relate to privacy and security.

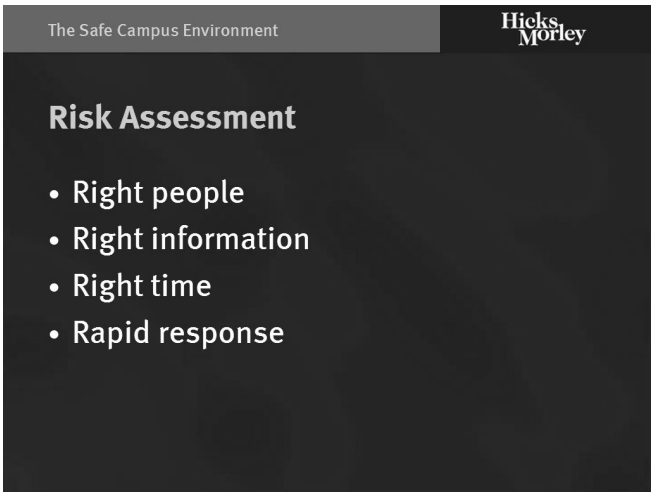
As for information and privacy, what you see is a picture of an institution that had information about a student who really needed help. He needed help for his own sake but also for the sake of campus safety. Just compare the successful management of Cho's condition through high school years and his very slow downward spiral once he got to university. What might have been the outcome if he was actively managed over that period? And the remarkable conclusion of the various reports into the Virginia Tech shooting was that people didn't report information because they were afraid that doing so they would breach privacy law.

This is what I'll address for the remainder of my presentation. My key message is that privacy and human rights laws do demand prudence, but in my view the law does not

daniel-michaluk@hicksmorley.com

prevent reporting of information and the use and disclosure of that information so long as all actions are taken in order to manage a **reasonably-determined** threat.

SLIDE 10 – RISK ASSESSMENT



Here's where we move into the various information flows that are necessary in managing the risk of violence. I've broken them into three categories:

- risk assessment;
- medical monitoring; and
- threat alerts.

If you think about the problem in terms of these three categories you'll really start to see a model for managing the risk of violence and also the makings of a policy document.

This slide is really about the objective of risk assessment: getting the right information, to the right people at the right time. This in turn supports an assessment that properly balances all rights and allows for the **rapid** development a **defensible** plan of action.

A multi-disciplinary decision is the ideal because you are really in double (or even multiple) jeopardy in making these decisions.

If you have a **security expert alone** make case management decisions, you may be able to defend them as they relate to your duty to provide a safe campus environment, but will be

daniel-michaluk@hicksmorley.com

vulnerable to claims that you've breached the duty to accommodate or the duty to respect individual privacy. On the other hand, if you use a **mental health exper**t alone to make case management decisions, you may respect students' medical needs and meet the duty to accommodate, but how can you be sure that decisions are defensible from a security standpoint? The **academic perspective** is also needed because any behavioural contract or accommodation proposal must be tailored to ensure the student's academic needs are met.

Now to go back to Virginia Tech. It's clear that we had neither type of expert involved. From the various reports we get a picture of an **English department** that was managing Cho over the year and a half period preceding the shooting. They might have felt some measure of comfort living with Cho despite his disturbing behaviour, in which case they made a poor assessment that ought to have been made by a risk assessment expert. Or, they felt there was a threat but they didn't report because they didn't know they could.

The answer: you have to get the information out of the English department to a group of expert decision-makers.

Normally the team will include someone from senior administration, someone from security and a mental health expert who is either employed or on retainer. You all heard Dr. Klassen yesterday. If you get the information to an expert in risk assessment like him and let the expert make a risk assessment your next step will almost always be defensible from a privacy and human rights perspective. It may be a preliminary decision to request a formal assessment based on a report from the community or an accommodation and management proposal, but if you're going to impose something that imposes any form of restriction on a student or employee, you want your decision to be based on an expert's backing.

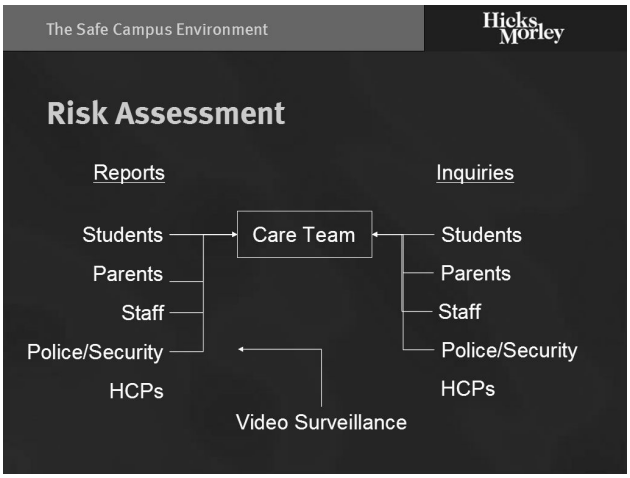
daniel-michaluk@hicksmorley.com

Now you're all looking at me like I'm being unrealistic. I noticed the feverish note taking yesterday when M. Fillion described the financial costs of managing his emergency and his remedial program. I also know that finding experts qualified in risk assessment is not easy, especially if you're not located in a major centre.

The intact care team is an ideal, and I know many of you currently make decisions without full multidisciplinary support. Exigency is one reason to go forward without full support and. Fiscal considerations will also guide the type of team you have in place. You can also bootstrap by training laypeople to assess risk. The simplistic legal answer is the structure you choose must be "reasonable in the circumstances," but there articulation of that standard right now. But the better your access to expert support, the lower your legal risk will be. Having ready access to expert help won't guarantee you never have violent incidents and harm, but it will maximize your protection from safety-related legal claims as well as privacy and human rights claims. No question.

daniel-michaluk@hicksmorley.com

SLIDE 11 – RISK ASSESSMENT



So here's a diagram depicting the various information flows that are part of risk assessment.

You'll see that it's broken down into two parts: reports (which involve information that is reported in from the community at large) and inquiries (information that is collected from the community at large after an initial report). These concepts are drawn from a United States Department of Education and United States Secret Service jointly-sponsored report published in 2002 in response to the Columbine incident. You'll see a citation for it in the materials Dr. Wood has provided (the last page of his September 4, 2007 memorandum). I'll link to it when I post these materials on my blog.

For reports, let's distinguish between reports from three different groups.

First there are reports from regular academic and non-academic staff, including security. For this group, the rules under Ontario's privacy legislation are fairly permissive; essentially universities can share information internally on a "need to know" basis. I support the view that we've heard consistently at this conference - universities can and should promote the internal sharing of information about potential threats.

At the same time as encouraging sharing, universities should provide guidance to faculty and staff on the actual objective criteria for identifying threats that may exist. We've seen

the McMaster orange folder – which is basically what I'm talking about. We're not asking front-liners to do an assessment, but we're advising them of the behaviours they should be aware of. Specification of objective criteria not only addresses a university's security-related duty, but also ensures a respect for individual privacy because it helps limit the information that's reported to valid information. A measure of false positives should be viewed as healthy, but universities will better respect individual privacy rights by encouraging **valid** reporting.

The second group is non-employed members of the community, especially students. I should say that there are some technicalities in the Ontario privacy legislation that make the right to gather this information somewhat unclear. Nonetheless, most universities do ask people from the community at large to report threats and we think this is justifiable given the relative legal risks provided (a) such reporting is supported and published in university policy that is incorporated into the student and employment contract (b) the university takes steps to encourage reporting that is based on valid objective criteria.

The final group is healthcare practitioners. We'll talk about medical monitoring next, but the basic rule is that information that is generated in the course of a treatment relationship, even if it's at a university's own medical clinic, can't be shared unless there is a risk of serious and imminent harm. So an information flow from a healthcare practitioner giving treatment to a student at a university should generally **not** be part of routine risk assessment systems.

Then there are risk inquiries.

daniel-michaluk@hicksmorley.com

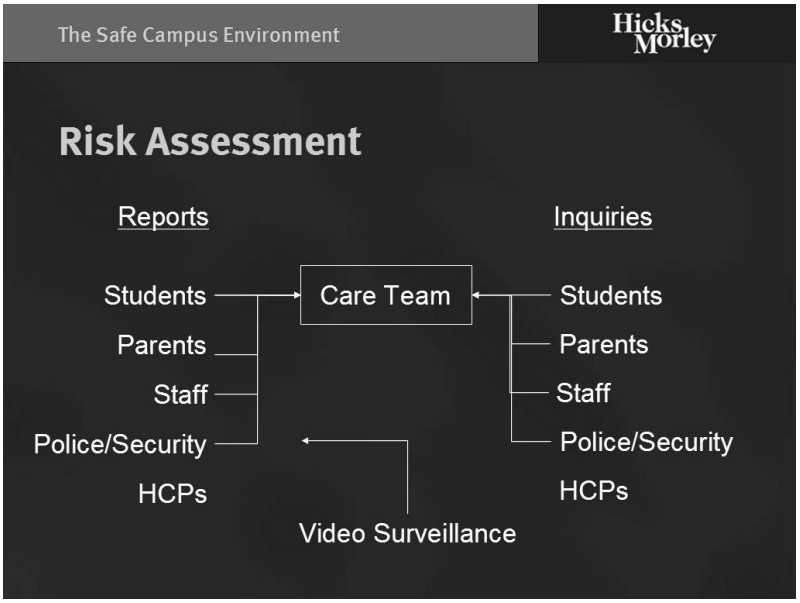
By risk inquiry I mean a process of collecting additional information before making a decision. For example, you get a report and its enough to be concerned. Before you even call your expert to get an opinion on whether its worth requesting a formal assessment, can you speak with the students professors to gather more information? Can you speak with the students friends?

A threat inquiry is a classic "indirect collection" in privacy law terms or a “private investigation” in layperson terms. And there are more restrictions on this type of activity in privacy law.

To articulate some very general rules on an issue that is still somewhat uncertain, it's more permissible to go out and gather information from staff members (teachers and residence administrators, for example) than individuals in the community at large (other students). We do think there is some scope for having special constables (as opposed to non-deputized security staff) conducting “external” investigations when truly necessary, but there is risk associated with this option. Schools wishing to use this management tactic need to acknowledge the risk and control it by policy. What you don’t want is to have your security force conduct a very broad police-like investigation when there’s no reason **not** to contact the student and make a direct inquiry.

daniel-michaluk@hicksmorley.com

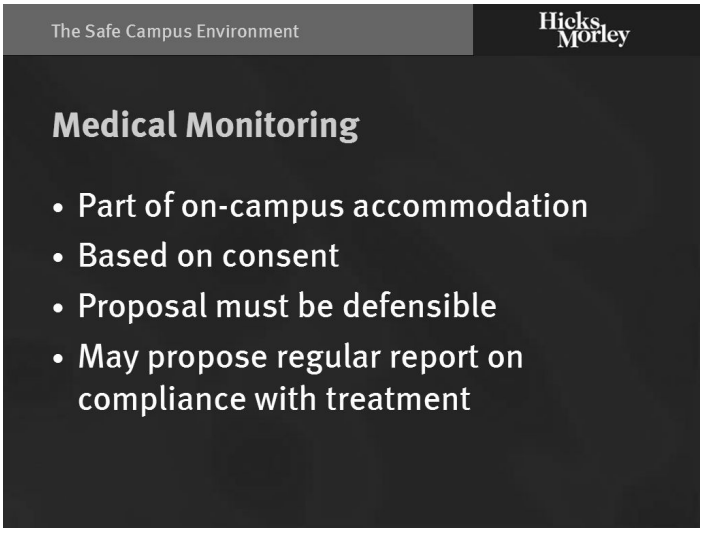
SLIDE 12 – RISK ASSESSMENT



This slide just summarizes what I've talked about. It has a comment on the use of routine surveillance - video surveillance is probably what most of you use. I can't comment in detail on the law of surveillance in this presentation but I will recommend the Ontario IPC's recent investigation report on the TTC's video surveillance system. It's at www.ipc.on.ca. It will provide you with some guidance on how to structure your video surveillance policies and procedures. It also has a novel finding that is important to universities. The IPC held that the TTC's special constables were engaged in "law enforcement," which gives the TTC some additional latitude in its surveillance activities. She stopped short of saying that special constables are always going to be engaged in law enforcement, but the position she took is much different than she has taken in some prior awards dealing with internal security forces and their right to act like police without running afoul of FIPPA. Given that universities are responsible securing the equivalent of a small or even a mid-size municipality, this finding may prove helpful.

daniel-michaluk@hicksmorley.com

SLIDE 13 – MEDICAL MONITORING



Let's move onto the next part of our model.

One of the common tactics available to the care team will be to place a student on a program of medical monitoring. What I mean by this is that schools may impose, as a condition of continued on-campus education, periodic provision of medical assessment information and periodic provision of information about compliance with a treatment program.

This is obviously a very invasive intervention but may be justified as part of a program of accommodation. What you're saying to a student is, "We have a legitimate basis to believe you pose a risk. But you can fully participate in the educational program provided you agree to this condition, which we think is reasonable in light of the risk."

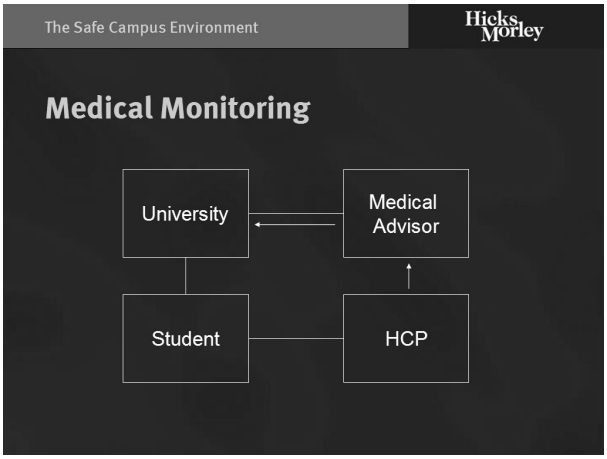
Here we see that human rights, privacy rights and campus security are all in balance, and medical monitoring makes sense as a tool for managing the threat of violence. We have to wonder whether such a tactic was used in the fall of 2005 at Virginia Tech whether it would have made a difference.

Given its invasiveness, however, if you want to impose medical monitoring as a condition of participation in campus life you should be prepared to back the proposal with a good expert

daniel-michaluk@hicksmorley.com

opinion. If the case management decision is made by a properly constituted case management team you should be fine.

SLIDE 14 – MEDICAL MONITORING



You should also have a structure in place that encourages the dissemination of the student's medical restrictions on a need to know basis. Here's what the information flow looks like.

As I've said, the treatment relationship between a student and a healthcare provider is confidential subject only to the risk of serious and imminent harm.

Since we want information from the student's care provider, an exception to the general rule, we **must get express written consent**. That allows for some form of report to flow from the student's health care provider to our own medical expert.

There is some debate about the extent to which an institution's medical advisor should be speaking openly with a health care provider about a patient's condition even with consent. In my view its important that the medical advisor at least be able to discuss **process** with an individual's health care provider.

I know we've all been frustrated seeking quality information directly from health care providers. One of the benefits of retaining an internal expert is that they have a better ability to work with other doctors in seeking medical information (again, consensually). A

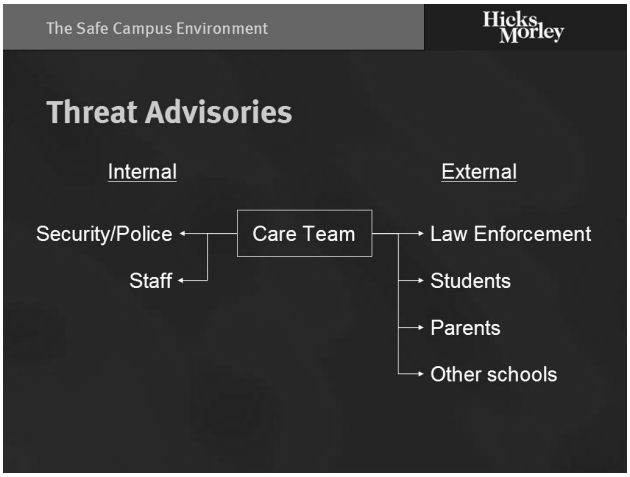
daniel-michaluk@hicksmorley.com

good medical advisor will actually act as an advocate for a university. He or she will remind the healthcare provider that he or she has a professional duty to avoid letting his or her client determine his or her own medical restrictions (think of the employee sick note) and will reinforce the health-related benefits of providing information that allows the university offer the student a proper accommodation program.

***

Once the report is delivered into the care and custody of the university's medical expert, information from that report can then be shared with members of the care team and even members of the broader university community as needed to fulfil the purposes outlined in the medical release. The internal medical expert helps the college comply with its privacy obligations by controlling dissemination. All of this is ideally structured by policy.

SLIDE 15 – THREAT ADVISORIES



Let's move on to the last part of our model, threat advisories. Again, we divide the information flows into two types: internal advisories and external advisories.

By internal advisories we mean advisories to people who are employed by the university. These advisories can be done on a "need to know" basis. For example, if the care team has identified a threat to members of a certain department, members of that department can be advised of the threat and can be told other information they need to

daniel-michaluk@hicksmorley.com

protect themselves. It will often be justifiable, for example, to share information about a threat with the university's constabulary or security staff.

Here are a few different varieties of external reports.

First, reports to police are justifiable under a fairly broad exception in our Ontario privacy legislation – the test is whether the disclosure is made "with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result."

Second, reports to students and other "externals" who may be at risk are justifiable under a "compelling circumstances" exception in FIPPA – the exception allows disclosure "in compelling circumstances affecting the health and safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the disclosure relates." Students may be warned, but of course, you should be aware that you may need to defend the fact of warning and the scope of the warning issued with reference to your risk assessment. We've had a few examples in Ontario in the recent past where schools have warned the entire student body using a picture of a threatening individual.

The decision to warn the community can be a tough one. I know that often institutions take the view that it's best to err on the side of security.

I endorse this view, but also think institutions should have a **risk assessment process** in place that encourages defensible decisions. When a care team is not in place we sometimes get asked as legal counsel to advise on whether a warning is justified. This puts us in a hard position because we are not trained risk assessors. In these circumstances we help clients by articulating the consequences of breaching FIPPA, which they can then

daniel-michaluk@hicksmorley.com

weigh against the undetermined security risk. But if there's a privacy complaint, the real question will be whether the university had time to retain an expert like Dr. Klassen to assess whether the warning was necessary and whether the university should have planned for the situation and retained an expert to be on call. The legal standard in answering these questions will be "reasonableness in the circumstances," and again, there are no clear guidelines yet on what is required.

On the consequences of breaching privacy, I'm of two minds of this. You may know that the IPC has fairly limited powers under FIPPA and that the there's currently no clearly recognized invasion of privacy tort in our law, but there's enough potential liability out there to justify a careful approach. We all know of the *Young v. Bella* decision, where a Canadian university was liable for $1 million in damages for what was essentially a hasty report of potential child abuse. So my view is that we should encourage free-flowing information, but we must also encourage responsible decision-making. That's why expert help is important.

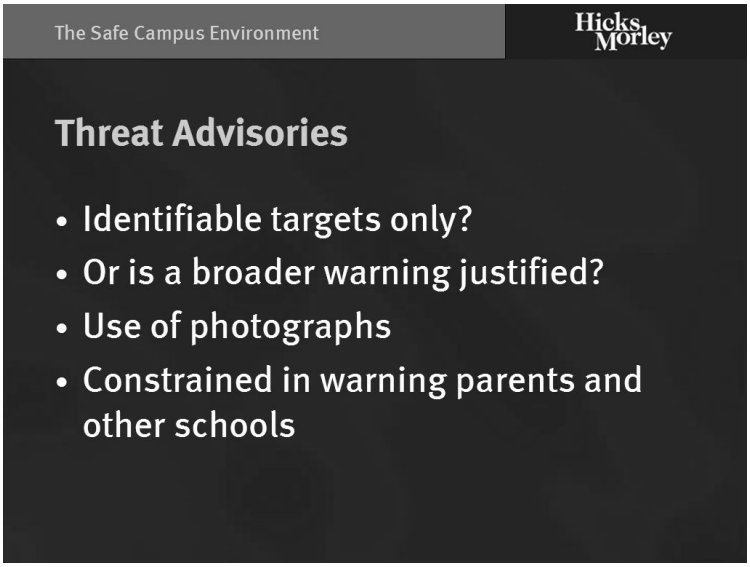
***

One final point is that the transfer of threat related information between universities or other postsecondary institutions is problematic under Ontario privacy legislation. It's not without any uncertainty, but generally speaking one university cannot tell another university or college about a former student that it has identified as a threat to support the registration process. You also can't have direct access to an applicant's secondary school record of accommodation or individual education plan.

daniel-michaluk@hicksmorley.com

This is a problem because most institutions will not perform any sort of background check during the registration process. It's simply not a practical option, yet the potential benefit (especially reflecting on Virginia Tech) is clear. I have had discussions with some administrators about the option of putting a "forced to withdraw" notation on the formal transcript. This would be a flag to the registering institution to address such a notation during the registration process by asking the student for information and, failing the provision of satisfactory information, denying admission. I think this is an option, but there are others that are worth thinking about.

SLIDE 16 – THREAT ADVISORIES

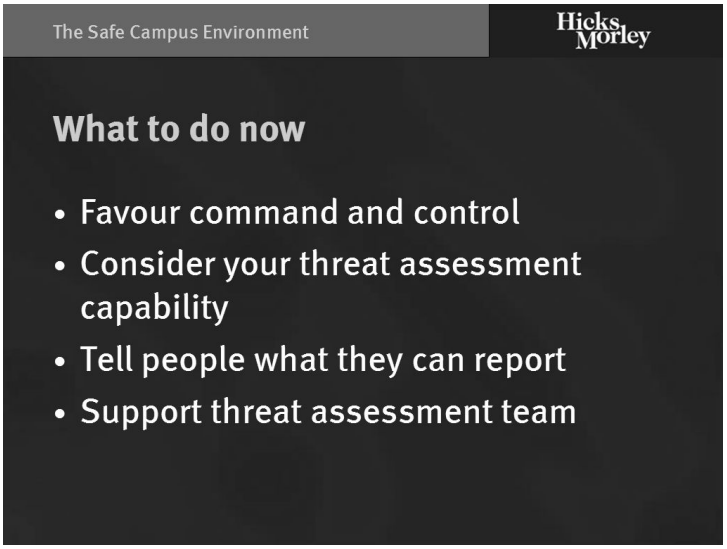


Here is just summary slide of what I just discussed. Warning: disclosing to parents is similarly problematic because once a student becomes 16, under Ontario law, they essentially have privacy rights as against their parents subject to the health and safety (compelling circumstances) exception. It's subject to consent too, and one option in a behavioural contract/accommodation program is to require the student to consent to parental reporting.

I should say that there is a debate about the efficacy of warning parents in every case. The risk management literature generally supports parental reporting as does the United States

Department of Education. As I've explained, the recent proposal to amend the FERPA regulation expressly contemplates (but does not require) disclosures to parents. Personally, I've heard anecdotes from administrators who've told me that reporting to parents have being the best thing they've ever done to help a student and I've heard other administrators are very wary of parental reporting. The proper approach from a legal perspective is to assess the merits of notifying parents on a case-by-case basis with the help of an expert who has all available information.

SLIDE 17



So I hope that gives you a good idea of the legal framework for managing the risk of violence and a view to making policies and procedures that encourage defensible decision making. This is not an subject without challenges and without risks, legal and otherwise. But I was very happy to hear Dr. Klassen's talk yesterday, which I perceived as quite an optimistic message about our ability to prevent violence. I'd like to leave you with the same sense of optimism from the legal perspective. Managing risk in a manner preserves individual privacy and human rights takes more work, but putting all rights in balance is absolutely attainable. Thank you.

daniel-michaluk@hicksmorley.com