

Negotiating the Balance

*Reconciling Individual Privacy and Public Interest When Addressing
At-Risk Individuals, Campus Violence and Ontario Privacy Legislation*

by
Yasmin Nissim, B.A. Hon.

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of

Master of Arts

Department of Law
Carleton University
Ottawa, Ontario
August 22, 2008
© 2008, Yasmin Nissim

Abstract

The recent application of Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) to the university sector has raised new issues between the habitually conflicting perspectives of individual privacy and the public interest. This study attempts to reconcile these opposing sides with the goal of illustrating that, under the new privacy regime, Ontario Universities can achieve a balance between these interests. Using the massacre that took place at Virginia Polytechnic Institute in April of 2007 as a case study and a media analysis of the resulting moral panic that followed, this thesis discusses the negative consequences of allowing privacy legislation to go misunderstood and misapplied when dealing with at-risk students. Ontario Universities have the opportunity to clarify their new privacy landscape and institute a framework that would protect the safety and security of the general public by identifying at-risk students without jeopardizing the individual privacy of those identified.

Acknowledgements

This thesis was written with the help and encouragement of many important people in my life. Sheryl, there isn't enough space here to thank you for your guidance and for lending your expertise and academic passion to this work (and we shouldn't forget Chester either). Mom, Dad and David - the constant love and support you have given me throughout my life has helped me accomplish not only this thesis, but so many other achievements. I must thank my friends for listening attentively whenever I decided to launch into a far too detailed discussion and analysis of the most recent addition to a chapter...especially at parties. Sai and Rasputin, thank you both for reminding me that a game of tag, a good nap and some time in the sun are vital aspects of any large project. Chris, my best friend, soul mate and the love of my life - thank you not only for your attentive eye when editing and your patient ear when listening (and patience in general!), but for all the other little things that kept me going, not the least of which was an unending supply of warm tea and hot chocolate, and many long drives to cool hot feet. And to Grandma and D - thank you for being a loving presence, always.

Table of Contents

1	Chapter I	Private Space/Public Interest: A Clash of Ideals
24	Chapter II	Understanding Social Influence: Media Power, Moral Panics and Policy Change
30	<i>II.I</i>	<i>Concern</i>
31	<i>II.II</i>	<i>Hostility</i>
34	<i>II.III</i>	<i>Consensus</i>
38	<i>II.IV</i>	<i>Disproportionality</i>
42	<i>II.V</i>	<i>Volatility</i>
43	<i>II.VI</i>	<i>Moral Panic: Influence and Impact</i>
56	Chapter III	A New Framework for Ontario Universities: Understanding FIPPA
86	Chapter IV	Structure and Balance: The Knowledge Sharing Framework and its Risks
86	<i>IV.I</i>	<i>Structure: Conceptualizing a Knowledge Sharing Framework</i>
91	<i>IV.II</i>	<i>Balance: Reconciling The Two Faces of Surveillance</i>
108	<i>IV.III</i>	<i>Negotiating the Balance: The Final Weigh-In</i>
113	Works Cited	
122	Appendix A	

CHAPTER I Private Space/Public Interest: A Clash of Ideals

September 2007, an eighteen-year-old student at Delaware State University in Dover, Delaware shoots two students, murdering one. March 2005, a sixteen-year-old boy in Red Lake, Minnesota murders his grandfather and his grandfather's partner at home, then goes to Red Lake High School where he kills five students, a teacher and a security guard before committing suicide. April 2000, a fifteen-year-old student wounds four students and one staff member in a knife attack at Cairine Wilson High School in Orleans, Ontario. April 1999, a fourteen-year-old boy shoots two students, murdering one, at W.R. Myers High School in Taber, Alberta. ("List of Major Incidents...", Kipp) These incidents are a mere glimpse into the acts of harm and self-harm that continue to permeate learning institutions all over North America.

Whenever a tragedy of this nature takes place, questions of why and how inevitably follow from the surrounding community and media. Many motivations have been attributed to the violence that youth and young adults exhibit. Factors blamed in the past include a lack of a solid family structure, absence of social programs, ease of access to guns, aggressive music, violent video games and movies; the list is extensive and ongoing. (Newman 61, 69, 70, 272) It is difficult to understand these occurrences as caused by any one factor, for each instance of violence or harassment can be surrounded by multiple motivations and mitigating circumstances. However, as complicated as the landscape is around explaining violent and harmful behaviour in students, there is yet another dimension to the questions being asked around this issue that has recently come under the spotlight: what role does privacy play in preventing violence in educational institutions?

Seung Hui Cho was the young student who opened fire upon his academic colleagues on April 16, 2007. His actions resulted in the deaths of thirty-two individuals and the wounding of seventeen more, all students or faculty at Virginia Polytechnic Institute and State University. (Report of the Virginia Tech Review Panel 1) “Virginia Tech”, as the tragedy is now referred to, stands in history as the deadliest school shooting to have ever occurred in the U.S. (Shapira and Jackman) Virginia Tech has also catalyzed a strong surge in the discourse around privacy and the sharing of information of at-risk individuals in an educational environment. There are many different accusatory fingers that can be pointed when determining what could have led to the murders at Virginia Tech, but there is one factor that cannot be disputed. A leading cause contributing to the tragedy was misunderstood and misapplied privacy legislation. (Report of the Virginia Tech Review Panel 63)

Three days after the tragedy at Virginia Tech, the governor of Virginia, Timothy M. Kaine, assembled the Virginia Tech Review Panel. The goals of the Panel included conducting a review of the events in the hopes of gaining answers as to how and why something like this occurred, and most importantly how to avoid such a catastrophe in the future. (Report of the Virginia Tech Review Panel vii-viii) Its findings in relation to relevant privacy policy and standards of information sharing were distressing. *The Family Educational Rights and Privacy Act* (FERPA) is the U.S. federal law which protects the privacy of student education records. According to the report produced by the Review Panel, prior to Cho’s attack, Virginia Tech staff and faculty were under the impression that FERPA disallowed any sharing of information about a student, even one

at risk of harming themselves or others. (Report of the Virginia Tech Review Panel 63)
This assumption was incorrect.

Cho presented a large risk that went wholly undiscussed by the staff and faculty at Virginia Tech because of poor understandings of relevant privacy legislation. The Review Panel's Report attempts to address this lack of communication and ignorance of policy, but also points out the fact that because of this widespread blackout of information, Cho did not receive vital help and intervention that could have meant the difference between aiding a troubled young man and cleaning up after a murderer. (63)
The possibility for any potential intervention or required treatment was lost, which likely resulted in the tragic deaths of thirty-two innocent people.

Virginia Tech, as an occurrence, has fuelled responses from the public, media, political leaders and policy makers in both Canada and the U.S., as the events leading up to the shooting and the role that privacy played within them have had significant implications for both countries. Questions have been raised about the point at which the health and safety of the public begins to outweigh individual rights to privacy. (Van Der Werf) This question has had serious implications for universities in the U.S., but also for those in Canada. Ontario is in the interesting position of having just recently broadened the application of the *Freedom of Information and Protection of Privacy Act* (FIPPA) to include universities, making the events at Virginia Tech quite significant to the operation of privacy legislation in this province.

Despite the obvious differences between Virginia and Ontario, there are enough similarities between the relevant legislation and surrounding legal and social reaction (i.e. media coverage, public outcry, policy review etc.) that Ontario universities can benefit

from examining the American tragedy more closely. Virginia Tech provides a clear example of the negative consequences that can come about when an appropriate balance between individual privacy and public interest is not realized. Ontario's FIPPA has great potential to provide protection for both individual privacy rights *and* the public interest, but this requires an interpretive standpoint with room for compromise between both sides.

The friction between public interest and individual privacy has been a source of much contention within contemporary privacy debates. This study will focus on that tension in order to understand the importance of each perspective, as both individual privacy rights and the public interest have equally valid claims to overall priority. However, allowing one to take precedence over the other will not provide an ideal balance that is vital to developing comprehensive and beneficial policy interpretations around privacy.

Through an evaluation of the tragedy at Virginia Tech and an analysis of Ontario privacy legislation, I will present a format for a balanced approach between public interest and individual privacy, specifically in regard to addressing at-risk individuals in a university setting. Finding a balance when understanding privacy appears to be an elusive concept that has never fully come to fruition through any current academic discourse on the issue. Contemporary literature on individual privacy and public interest reveals a deep divide that is also reflected in situations like Virginia Tech. Understanding the polarity in this discourse is fundamental to facilitating a balanced approach.

Contemporary arguments around privacy and public interest have gained much of their current momentum from the terrorist attacks of 9/11. This event has sparked a heavy response from many intellectuals, breathing new life into old arguments and reasserting established academic divisions. This is quite obvious when reviewing the relevant literature around this topic as 9/11 presents a poignant foundation upon which recent arguments for both public interest and individual privacy rights have been based. Although Virginia Tech was not understood as a terrorist act, the significance of this event in a post 9/11 society carries more weight and certainly more implications for the roles of privacy and public interest. Therefore, recognizing how 9/11 has shaped the current field of discourse is important when understanding the social and political environment within which the tragedy at Virginia Tech exists.

Kevin Haggerty and Richard Ericson (2006) understand the tensions that have arisen within privacy discourse and succinctly identify the two main opposing camps currently involved in the privacy debate. On the one hand are those intellectuals such as Paul Fairfield and William Staples, who believe privacy has been “dangerously eroded” due to increased surveillance. (Haggerty and Ericson 11) Advances in technology, mounting pressure by the state to allow surveillance and changing social perceptions about what we consider to be acceptable levels of monitoring are affecting the security of individual privacy.

In contrast to this argument however are those scholars such as Dennis Bailey (2004) and Amitai Etzioni (1999) who view privacy as something that can be manipulated to serve destructive purposes and therefore should not be so plainly guaranteed. (Bailey 33) Individual notions of privacy from this perspective should not

impede upon institutional policy endeavours. (Haggerty and Ericson 11) From this standpoint, upholding the safety and security of the public should be a primary concern over individual claims to privacy. As one can see, privacy is an intricate concept, not simply a quiet corner away from the public.

Our conceptions of what constitute public and private are complicated by the many other expectations we associate with each. When contemplating what it means to have privacy, all the interests we are seeking to protect when retreating into this space must be considered as well. Privacy is not a singular concept. It can “be defined as places, spaces and matters upon or into which others may not normally intrude without the consent of the person or organization to whom they are designated as belonging.” (Reiss 20) When we seek to have privacy, we look for a place where we can reveal our vulnerabilities yet be secure from others. We are seeking a place in which we are free from scrutiny, judgement and embarrassment. We are also looking for a place where we have not only freedom *from* others, but the freedom *to* express ourselves and engage in activities of our choice.

To threaten privacy is to threaten not one aspect of existence, but several. Christine Sypnowich (2000) and Judith Jarvis Thomson (1975) both understand the private domain as one laden with many expectations around our liberty, property, and security of the person. Therefore, when it is deemed necessary to encroach upon this private space for a seemingly legitimate public interest, the resulting consequences can have many different implications. For some academics and policy makers, these consequences do not constitute a dilemma of any magnitude and simply fall away behind the importance of upholding safety and security for all. Increasingly, many authorities

and institutions are involving themselves in public surveillance, as well as encroaching upon what was once considered to be the private realm under the pretences of risk management and protecting the collective. (Staples 2000 117, Fairfield 1)

Fairfield, along with several contemporary intellectuals in this field such as William Staples (2000, 1997), and Colin Bennett and Charles Raab (2006), suggest that privacy is indeed eroding. They have observed a substantial increase in surveillance of the general population by the state and private institutions, signalling the gradual shift of private spaces becoming public. Fairfield notes with concern that in some instances all that is needed to justify these encroachments upon individual privacy is a claim towards protection of the majority. (Fairfield 1) Raab and Bennett echo this point, stating that privacy has been interpreted by some as a value that “cannot be allowed to get in the way of the satisfaction of public-order objectives that include, principally, the security of the state and the personal security and safety of its citizens.” (50)

Staples offers many examples in his work which support the arguments of Fairfield, Raab and Bennett. Additionally, he also heavily underscores the increasing tendency for risk assessment and control that has allowed many private and public institutions to invade upon the personal space of individuals. (2000 117) In many instances this risk management trend goes hand in hand with the above claims to protection of security and safety. Jacqueline Klosek (2007) gives practical shape to the claims put forth by not only Fairfield, Raab and Bennett around public interest, but also concerning risk management as analyzed by Staples. Like so many contemporary works on privacy, Klosek looks to the events of 9/11 and their effects on Canadian policy to illustrate the current trends in this area.

In Klosek's analysis, protecting Canadian citizens from terrorist attacks and managing the risk associated with certain groups has justified the creation and application of the *Anti-Terrorism Act* in Canada. (Klosek 123) This legislation has dramatically increased the state's freedom to use surveillance while requiring much less justification for invasion of privacy, all with the express purpose of protecting the Canadian people. (Klosek 124-125) Although Klosek outlines the benefits that have come out of surveillance, she also points out that the data collected through the *Anti-Terrorism Act* can be used by the government for ancillary reasons not associated with stopping terrorism, but rather for other forms of social control. (126) This reinterpretation of a law justified for one purpose but applied in a fashion exceeding its original mandate is known as "function creep". (Haggerty and Ericson 18) Function creep can be a dangerous practice as it can mean the further erosion of private space, as Klosek cautioned. Through her analysis, Klosek supports the idea that privacy has and continues to erode. This, however, is not a new concern.

Alan Westin (1967), writing forty years before Klosek, discusses the same problem of the state and various private institutions engaging in surveillance to protect the "security of the nation". (206) He illustrates how this surveillance could grow to encompass other areas of perceived risk that were not originally intended, thereby threatening individual liberties. (207, 233) The consequences of this deterioration of private space are argued to have negative implications for democracy, liberty, autonomy, and the division between state and citizen. (Fairfield 6; Staples 1997 11; Raab and Bennett 4) The proponents of this argument are pointing an accusatory finger at the motivations behind chipping away at individual privacy and the use of public security as

a justification for surveillance. However, as Haggerty and Ericson stated, there is another side in this debate.

The alternate discourse around privacy does not view claims towards protecting the public interest as a subversive method for achieving social control. Rather, it suggests that protecting public interests should be placed before any one individual and their claims to privacy. On this side of the issue, notions of public interest can take many forms. One expression of public interest draws upon a feminist perspective which sees ideas of privacy tied to unjust power relations. Carol Pateman (1988) sees the private domain as one filled with injustice which remains unnoticed because it exists out of the public eye. Because women have been associated with the private sphere, any injustice or inequality that occurs in this space is “natural” and does not detract from the universal equality of the public world. (Pateman 19, 117) In this interpretation, the private sphere can be used to hide harmful action. This perspective argues that completely separating the private from the public allows women to remain outside the scope of justice.

The idea of the private sphere being a veil behind which one can hide malicious behaviour is echoed in another manifestation of the public interest: security and safety. Bailey, like Klosek, draws on the events of 9/11 to illustrate this point. In his study, he outlines the negative consequences of attempting to uphold strict individual privacy rights when dealing with public safety and risk management. Bailey blames the destruction and lives lost during 9/11 on misplaced priorities, specifically individual privacy over public security and safety. (6-7) While claiming to understand the importance of protecting individual privacy, Bailey states that the hyper-prioritization of privacy rights in Western democracies is ultimately a weakness rather than a strength. (5)

It was this weakness that allowed the individuals involved in 9/11 to execute their plans with veritable anonymity. (Bailey 5) Bailey views the freedom of anonymity found in Western democracies as an exploitable commodity for those who wish to infiltrate these public spaces with mal-intent. (Bailey 5)

Bailey is not alone in his interpretation. Amitai Etzioni also focuses on problematizing the idea of individual privacy and draws attention to the “degree to which privacy can inhibit the development of desirable social policies.” (Haggerty and Ericsson 11) Synnowich and Thomson as mentioned earlier, articulate privacy as a multifaceted notion inherently tying concepts of democratic freedom to the protection of individual privacy. Etzioni argues that this current construction of privacy rights is a relatively new idea that began to take shape between 1890 and 1960. (Etzioni 83) He argues further that following the 1960s, “the realms of rights, private choice, self-interest, and entitlement were expanded and extended, but corollary social responsibilities and commitments to the common good were neglected with negative consequences such as the deterioration of public safety and public health”. (87)

Etzioni feels the common good is something that has fallen into neglect due to the rising force of individualism and its relationship to the protection of privacy rights. (87) Bailey also argues that by upholding everyone’s right to privacy and freedom, undemocratic outcomes are created which do more to limit people’s freedoms than enhance them. If authorities have limited information about real threats, they are forced to treat everyone as suspects, thereby limiting everyone’s freedom. (Bailey 7) By having more openness, it will be easier to identify those who should be the true targets of state scrutiny. “The best way to curtail the need for governmental control and intrusion is to

have somewhat less privacy.” (Etzioni 99) Like in feminist theory, allowing an overlap between public interest and private spaces ensures that a greater sense of safety and security is upheld.

The line in this debate is heavily drawn, with those attempting to hold back the encroaching arm of surveillance in our everyday activities on one side, and those pushing for more transparency and openness on the other. The strong divide this debate has created has also resulted in an interesting paradox when trying to attach a defining character to our society. The idiom of privacy has created cultural markers that are completely at odds with each other. Consider the popular terms “culture of privacy”, “culture of surveillance”, “transparent society”, “society of control”, and “open society”. They all illustrate the inherent tensions around the privacy discourse. There is no clear balance within the privacy debate. Open or closed, private or surveyed, the polarizing language of this dialogue is highly problematic.

By having such a polarized field of argument, the language used by either side of the debate tends to reflect and reproduce certain presuppositions. Not all areas of the discourse around privacy may exude these assumptions through their analysis, however they do underlie enough of the literature to warrant acknowledgement. The first noticeable presumption that can be noticed when evaluating this debate is the notion that one cannot have real privacy with any kind of institutionalized monitoring. The second assumption is that there can be no effective social protections or regulation when prioritizing individual privacy over public interest.

When unpacking these assumptions even farther, it is possible to see the extent to which the discourse from a particular side may influence the characterization of other

social actors. For example, the assumptions around the role of the individual, the state, and even technology can be very different depending on the standpoint of the argument. Staples for example consistently articulates the individual as being surveyed and “systematically manipulated” by the state and forms of private authority through use of the media and communications technology. (Staples 2000 157) Here we can see the individual interpreted as a victim of the overbearing state, and media and forms of communications technology as tools of the authority. This echoes the underlying assumption that institutional monitoring is detrimental to individual privacy and autonomy. However, when delving into the presuppositions within the work of someone like Bailey, the individual, the state and technology take on very different roles.

Bailey cautions that the individual may be someone who will use the freedom of privacy and anonymity as a tool for subversion. He describes communications technologies as giving more flexibility to ill-intentioned individuals to coordinate and carry out malicious plans. The state, in respecting their privacy and autonomy, has no power to act until negative consequences have already become apparent. (Bailey 5) This side of the discourse characterizes the individual as a target of suspicion, with technology providing various means of concealment and covert communication. The state however is characterized as a blind institution burdened with notions of protecting individual autonomy and privacy to the point at which defence of these values becomes a fault and disables the capacity of the state to efficiently protect its citizens and their interests. The assumption that there can be no effective social protections or regulation when prioritizing individual privacy over public interest emerges clearly.

It is vital to understand how these assumptions affect the landscape of the privacy discourse as they have led to such a noticeable division. By creating a heavy divide in the discourse it is sometimes difficult to see that some of the assumptions of each perspective carry commonalities. Both view technology as an autonomous tool that can work in the favour of those who wield it, but it is not inherently good or bad on its own. Also, the state is a target of harsh criticism from both perspectives, either as being too lenient or too dictatorial. The most important similarity however is with respect to the goals of each viewpoint: freedom, privacy, and security for all individuals are the end results being sought after in both instances. Striking a balance between the two is a difficult endeavour that neither side of the debate has successfully achieved. I believe this is because neither side is able to fully accept a *balanced approach* to privacy, despite sharing some common ground.

As illustrated with the examples from Bailey and Klosek, it is clear that emphasis is always placed upon the ultimate validity of the side being argued, but to the point where the motives and opinions of the opposing side are undermined. So although it may seem at first that some consideration is being given to the opposing argument, in the end, there is still *more* weight placed on either public interest or individual privacy, rather than a true attempt to balance these concerns. A complete consideration of each side's anxieties and opinions provides for a much clearer and informed argument without reducing the importance of the opposition. What I am proposing is a stance that is sensitive to both sides of this discourse, one that appreciates the tension without becoming part of it.

The proponents of this debate have cut two distinct paths in order to reach the same ultimate goal of a society which contains autonomous individuals, who are both free to act and are secure in their surroundings. I have considered each path and in this thesis I am exploring a third route. By evaluating both sides with some neutrality, it is possible to understand the flaws and strengths from each camp and propose a balanced alternative to this ideological conflict. An alternative within this debate is strongly needed as privacy concerns have only continued to multiply, while frequently conflicting with the public interest, as seen with Virginia Tech. By creating an operational framework that both understands the necessity of individual privacy, but appreciates the need for public security, it is possible to facilitate an effort that does not entirely quash the validity of either standpoint. This framework will be constructed within the context of Ontario universities, at-risk individuals, privacy regulations and campus safety initiatives.

As illustrated at the beginning of this chapter, both Canada and the United States have experienced the horror of school-based violence, which sadly reflects what appears to be a trend in North American education institutions. Virginia Tech is a tragic landmark in school violence that has reverberated heavily in Canada due to the surrounding controversy of privacy laws that very much parallel Ontario's privacy legislation under FIPPA. By ensuring a comprehensive understanding of FIPPA in relation to dealing with information sharing for at-risk individuals, Ontario universities will be better able to facilitate a balanced approach between public interest and individual privacy. Creating a network of knowledge around students at risk of violent behaviour in

order to better protect the public is necessary, but so is appreciating the need to still uphold the privacy of at-risk individuals. This is a balance that can be attained.

A lack of knowledge around students who have the potential to commit violent acts is not a new concern, nor is it one limited to universities as demonstrated with the examples at the beginning of this chapter. Katherine Newman directly criticizes the segregated nature of information around at-risk students. She has evaluated several school shootings (ranging between elementary and high schools) and found in many of these instances that “there was sufficient evidence that they [the shooters] needed more help and guidance, but because no individual had the whole picture...no one recognized the depth or seriousness of their problems.” (Newman 109) Information sharing must be recognized as a vital tool in addressing at-risk individuals.

William Staples would most likely look at this information sharing with a critical eye and characterize it as a form of surveillance. This surveillance would allow for surreptitious institutional controls to be injected into the private sphere resulting in systematic manipulation. (Staples 2000 157) Surveillance is a form of risk management characteristic of a neoliberal society which Zygmunt Bauman (2000) and Nikolas Rose (2000) both suggest we currently inhabit. (Rose 327) Neoliberal strategies when dealing with crime and possible threats involve the calculation and management of potential undesirable future events in order to reduce risk. (Rose 332) This strategy makes the avoidance of these events the central object of decision-making processes (Rose 332), which does satisfy Staples’ criticisms of the function of surveillance as a tool of risk management and social control. (2000 10)

It does appear on the surface that the suggestion for information sharing is merely an attempt to survey and manage targeted individuals, which Staples argues is the main function of surveillance. (2000 10) And it is true that to encourage the sharing of information about an at-risk individual is to control for, and hopefully avoid, a violent situation. However, while this idea of risk management is correct, there are beneficial possibilities that arise with information sharing that do not completely fit the narrow, neoliberal approach of risk management. David Garland (2001) states that we are in a hybrid state that seeks to manage at-risk individuals, but one which also attempts to treat and rehabilitate. (27) Garland differs from Bauman and Rose in that he feels there is still an element of welfarism that permeates crime prevention initiatives. While neither welfarism nor neoliberalism is an absolute “right”, each perspective offers useful tools that when considered together offers a more balanced framework within which to place a strategy to address at-risk individuals.

Garland describes this hybrid model as one that tries to “address statistical distributions and patterns of crime” in order to measure and control for them, but also attempts to “understand the individual criminal”. (43) By assessing the ways in which social patterns and the surrounding environment impact an at-risk individual or already existing criminal, it is possible to understand causality and provide intervention or treatment as necessary. (Garland 42, 43) Garland refers to this as the *penal-welfare* model. This theoretical model serves as an appropriate framework for constructing a balanced approach between individual privacy rights and public interest, as the penal-welfare model possesses a balance of its own. It is essentially an equilibrium between neoliberal risk-management strategy and welfare state ideas of reform and rehabilitation.

The penal-welfare model relies on informal social controls such as families and communities along with disciplinary structures like schools to work effectively. (Garland 49) The broad nature of this framework is a feature of penal-welfare institutions which focus upon “deep underlying causes, unconscious conflicts, distant childhood experiences and psychological trauma” in order to determine causality. (42) This in turn allows for the managing of risk and at-risk individuals, but also reveals possibilities for treatment and intervention which should be a goal that Ontario universities look to, while being aware of the possibility of a “function creep” into the inappropriate monitoring that Staples would caution against.

Although this theoretical framework is one traditionally employed within criminal justice regimes for existing criminals, there are obvious qualities within the theory that would translate well into a university setting when addressing at-risk individuals. By attempting to interpret legislation like FIPPA in a way that appreciates both sides of the privacy debate, while extending the penal-welfare model to the university context, an alternative viewpoint can be discovered that has great potential for achieving balance. Finding the equilibrium between risk management and intervention, and individual privacy rights and public security is a feasible goal. However, before attempting to construct this framework within an Ontario university setting, it is important to take what lessons can be learned from Virginia Tech.

The methodology utilized for this study comprises several levels of analysis and discussion, with the overall approach being framed within Garland’s penal-welfare model as described above. There were many influences that surrounded the fallout from Virginia Tech that Ontario universities need to take heed of in order to avoid unhealthy

interpretations and applications of FIPPA. One of these influences is referred to by theorist Stanley Cohen (2004), as a moral panic. This consequence has sent reverberations across the U.S. and Ontario. The media is a central instigator during a moral panic, as news media tends to label deviant behaviour, which works to enhance stereotypes and enforce the existence of a deviant aspect within society. (Jones 7, 8) This works to fuel society's fears that there is a new trend attacking the moral fabric of society. I conducted an analysis of print news one week following the tragedy at Virginia Tech in order to illustrate the shape of a moral panic with regard to school violence and to understand the effect it had on policy-making.

The week following the shootings was chosen as this is the point at which this event would dominate the media, making it easier to pick out journalistic tendencies that would encourage a moral panic. The *New York Times* was the main news source relied upon for this one week period as it is a respected and largely read national and international broadsheet newspaper. There are several other articles from various news sources that fall outside of the one week time frame that will also be included within the analysis. They are necessary to illustrate the lasting impact of certain elements of a moral panic. Additionally, a counter-discourse from policy makers in Canada and the U.S. that tries to dissuade the moral panic and heated social reaction following Virginia Tech can be found in these extra articles.

From the articles collected several characteristics were looked for. Attempts to group in Virginia Tech, and specifically Cho, with previous school shootings to build the notion of a "trend" was an important quality to note. Also, evidence of media and social reaction regarding youth and violent media consumption were pinpointed in order to

determine how Cho's deviant behaviour was categorized. Lastly, demands for policy change and government intervention were noted as this is highly characteristic of a moral panic and central to the focus of this thesis. The influence of calls for policy revision fuelled by a moral panic can be found within the institutional reactions that followed in the wake of the massacre, which the Report of the Review Panel demonstrates.

The Report of the Review Panel is heavily relied upon within the moral panic analysis. This two-hundred and sixty page report was completed in August of 2007, four months after the shooting. The Review Panel consisted of the governor of Virginia, Timothy M. Kaine, and eight other individuals specializing in areas such as law enforcement, security, governmental management, mental health, emergency care, victims' services, the Virginia court system, and higher education. (Report of the Virginia Tech Review Panel viii) Their report illustrates the impacts the surrounding moral panic had on policy interpretation and the characterization of Cho. Specifically noted are links between the decisions and commentary from the Review Panel with the characterizations of Cho and surrounding social and media reaction when evaluating calls for policy revision found in the media analysis.

The next level of analysis carried out as part of the overall methodology was an evaluation of the terms of Ontario's privacy legislation. This is a vital step to take, as should a difficult situation arise it may force unnecessary policy change, a factor tied to moral panic that will be explained further in the following chapter. In order to avoid having negative policy interpretations for the sake of placating an angry community's call for action, Ontario's universities need to understand the capabilities of FIPPA with regard to facilitating information sharing about at-risk individuals. By understanding what the

legislation already contains, it is possible to identify areas that may require clarification from the province and avoid unnecessary changes should a moral panic ever occur concerning FIPPA.

Specific sections of the legislation have been highlighted as they expressly address how and when information can be shared should an individual be a danger to themselves or others. A brief discussion of the similarities between sections of FIPPA and FERPA will be presented in order to reinforce the importance of knowing the capabilities of a piece of legislation *before* a shocking event strikes that may remove the possibility of uninfluenced interpretation. In addition to gaining clarity of FIPPA itself, a brief discussion of Ontario's *Personal Health Information Protection Act* (PHIPA) is necessary. The U.S. had several conflicts with FERPA and their version of Ontario's PHIPA, titled the *Health Insurance Portability and Accountability Act* (HIPAA). Many universities have health and counselling services on campus and as a result there are questions around overlap that will be outlined, as there is currently very little information concerning standards on how these two pieces of legislation should interact in a university setting.

The final point of discussion and analysis undertaken within this thesis is to present a hypothetical model of a knowledge sharing framework based upon Carleton University's current administrative structure. This is then followed by an analysis of how surveillance can negatively impact a campus community if it is improperly insulated from aggressive institutional monitoring and "function creep". The harmful social implications of function creep will be discussed in detail so as to illustrate the caveats around this issue and how best to avoid falling into a potentially destructive pattern of

surveillance. Following from this discussion about protecting the individual, sections of FIPPA will be outlined that present the ability to shield any information collected and compiled about at-risk individuals. Attention needs to be given to protecting the information being gathered, as release could result in public stigmatization and targeting of identified at-risk individuals. Maintaining a balance between sharing information about at-risk individuals and the protection of their information is the ultimate goal of this discussion. Following this analysis, suggestions for “best practices” with regard to the collection and compilation of information on at-risk individuals will be provided.

It is necessary to mention that much of the knowledge and information collected around the legislation itself has come about due to my current employment position with Carleton University. I have held the position of FIPPA Implementation Assistant since April of 2007, which has placed me in close contact with many resources and tools for interpreting the legislation. This position has given me an inside look into how Ontario universities are handling their procedures, as well as allowed me to have access to the resources and directives of the Ontario Privacy Commissioner. I have had the opportunity to attend several conferences and to take part in weekly meetings regarding the operation and implementation of FIPPA on university campuses across the province. This position and the knowledge benefits that have arisen as result have been an invaluable resource to this thesis.

The following chapter will begin with the analysis of the Virginia Tech moral panic. A quick overview of the theoretical components of a moral panic will be presented first to provide the basis for the review of news media which is the major component for this section. The evaluation of the impact the resulting moral panic had

upon the Review Panel's actions and policy decisions is the next major section. The overall purpose of this chapter is to illustrate the lessons from Virginia Tech that Ontario universities can look to should a similar situation ever arise within their sphere.

Chapter three will move into the analysis of FIPPA. This section will address the relevant sections of the legislation when sharing the information of at-risk individuals. The comparative discussion regarding FERPA will also be included in this chapter, along with the brief discussion of Ontario's PHIPA and the caveats that arise with this piece of legislation in a university context. The final portion of this chapter will discuss how the *penal-welfare* model can contribute to the conceptualization of a sound knowledge sharing framework.

The fourth and final chapter will provide a more in depth analysis of how an information sharing network could operate, using Carleton's administrative structure as an example. It will also address the section of analysis concerning surveillance, function creep, the potential influence of regulated health professionals in decision making processes and the privacy interests of at-risk individuals. Additional discussion around disclosure provisions within FIPPA appears in this section but the reasoning is geared towards ensuring the privacy and protection of at-risk individuals should a university deem it necessary to disclose their information to select individuals.

The goal of this work is to find balance: balance between individual well-being and public safety, balance between privacy and public interest, and balance between help and punishment. Ontario universities have an opportunity to find this symmetry. The conclusion of this thesis will endeavour to illustrate an alternative interpretation which

satisfies the common goal of this divisive privacy debate: freedom, privacy, and security for all individuals.

Chapter II Understanding Social Influence: Media Power, Moral Panics, and Policy Change

By the late 1990s, school shootings had moved into the realm of being a familiar spectacle, often described by the media as a “trend”. By categorizing an individual shooting as part of a wider tendency towards violence, the event is both removed from its specific context and structured to intensify people’s fears about the safety of their children and youth in schools. (Killingbeck 186) The end result of this homogenization can be misdirected public policy generated to safeguard schools, even though the real problem may lie elsewhere. (Killingbeck 186) A study conducted in 1999 on news coverage of school shootings in Canada and the U.S. noted the media’s ability to distract politicians, police, teachers, and parents from “more pressing and realistic issues”. (Greenberg and Wilson 95) This consequence of encouraging misguided and hasty policy initiatives is part of a series of factors tied to the recognized media effect known as a “moral panic”.

Whenever a tragedy strikes with the magnitude of an event like Virginia Tech, attempting to understand and uncover the relevant issues to prevent such loss in the future is necessary. Yet in retrospect, there are other opportunities for consideration affecting policy creation and legislative interpretation that have emerged from this sadness apart from suggestions of how to carry out sound risk management on a university campus. It is important to understand the role and power of public reaction and media presence on policy interpretation and action. The actions of administrators and policy makers following this tragedy did not exist within a social vacuum.

Analyzing how the path of public policy was shaped by these symbolic and cultural factors during the weeks and months following Virginia Tech will provide

insight into how media and social consensus can sometimes damage constructive legislative objectives. This is vital to examine if Ontario universities wish to work towards achieving and maintaining a balance between individual privacy rights and the public interest. This chapter will demonstrate that it can be difficult to construct an effective policy response if the response itself is constrained and enabled in a certain fashion due to external influences like a moral panic, as occurred with Virginia Tech. The third chapter will set out the points within Ontario privacy law that require understanding and clarification in the event that should a tragedy ever strike, the affected university can rely on a strong foundation of knowledge established beforehand, free of any peripheral discourse.

The proliferation of media coverage following Cho's actions alerted the public to what had occurred at Virginia Tech campus, but also fuelled a moral panic. The media are a powerful agent with the ability to both convey knowledge and construct and influence audiences. (Attallah 91) Following Virginia Tech, the fears of the public were augmented through the media by placing the event within greater themes of recognized problems around violence and crime. This is not uncommon during a moral panic, as many powerful political and public interest groups will use an event like this to push forward their agenda. (Greenberg and Wilson 97)

The inclusion of this consensus building within the Virginia Tech moral panic worked to generate the targets for society's anger and calls to action. It drew focus away from other fundamental issues, as mentioned earlier, but in this case the misdirection was also accompanied by misinformation directly relating to the functions and provisions of privacy legislation in the U.S. The effects of this moral panic and the fallout that

occurred as a result illustrate how the moral panic-induced discursive consensus negatively impacted the balance between public interest and private rights in the relevant legislation.

As mentioned in the first chapter, I conducted a study of one week of North American print media coverage from April 17th to April 23rd 2007 in order to determine whether a moral panic had indeed occurred with regard to Virginia Tech, and if so, what its effects were. An electronic search of all articles in the *New York Times* following the April 16th massacre revealed sixty-six articles in which Virginia Tech was mentioned. Of these sixty-six articles, fifty-one were devoted entirely to coverage of the event, illustrating local, national, and even some international perspectives and criticisms around the tragedy. These articles form the primary corpus of the study.

Stanley Cohen (2002) is widely known for his theoretical development and study of “moral panics”. Cohen defines a moral panic as the point at which

a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people; socially accredited experts pronounce their diagnoses and solutions; ways of coping are evolved or (more often) resorted to; the condition then disappears, submerges or deteriorates and becomes more visible. ... Sometimes the panic ... has more serious and long-lasting repercussions and might produce such changes as those in legal and social policy or even in the way the society conceives itself. (Cohen 1)

Moral panics have five elements: concern, hostility, consensus, disproportionality, and volatility. *Concern* (as opposed to fear) is public anxiety directed towards the potential or imagined threat. *Hostility* is recognized as moral outrage targeting the actors and sometimes certain agencies (e.g. politicians) that are seen to be ‘ultimately responsible’ for the problem. They are defined by Cohen as “folk devils”. *Consensus* is the

widespread agreement that the threat is real and serious enough to warrant action. *Disproportionality* is an exaggeration of the number or strength of the cases, in terms of damage caused, moral offensiveness, and the potential risk if ignored. *Volatility* is recognized as the quick eruption of panic and sudden dissipation that occurs without warning. (Cohen xxii) The media serve as both instigator and broadcaster of these five elements, giving them form and substance within a public context.

The ability of the media to have this influence and power by way of a moral panic can be understood through the work of Stuart Hall (1978). Hall understands the news media as “presenting information about events which occur outside the direct experience of the majority of society”, often making them the only, primary source for the public to gather information about important events and topics. (56) Thus, the content of the news through its coverage of “new” and “unexpected” events, works to make comprehensible what society would normally consider a “problematic reality”. (Hall 56) These “realities” are events that threaten society’s expectations of consensus, order and routine. (Hall 57) A school massacre can be interpreted as an example of a “problematic reality” that the media attempt to break down into comprehensible pieces. Following the deconstruction of an event, the interpretations that follow are based upon prefabricated categories of understanding that emerged from similar past events. This has a direct impact upon the function of a moral panic within the public sphere.

When the media creates this framework for understanding, it is carrying out two other functions that relate directly to the power of influence Cohen understands a moral panic to have. Hall defines these two functions as follows: “The media define for the majority of the population *what* significant events are taking place, but also, they offer

powerful interpretations of *how* to understand these events.” (57) These interpretations implicitly provide society with certain orientations towards the events and the people or groups involved in them. (Hall 57) This coincides with Cohen’s understanding of a moral panic as framing an event in a “stylized and stereotypical fashion”, as the media is basing their interpretations on generalizations and assumptions from past events. (1) Therefore, through Hall it is possible to understand both the authority of the media in identifying events of importance, and their capacity to direct consensus and action.

Cohen’s original framework was published in 1971. In his study, Cohen addresses the much publicized confrontations between the British sub-culture groups of “Mods” and “Rockers” during the sixties. Since then, moral panic theory has been applied to many other groups and social situations in which the media had deemed the moral fabric of society to be under siege (for example, Goode and Ben-Yahuda, Hall, McRobbie, Schissel). This link between moral panic and identifying a “problematic reality” relates back to the understanding of the media as defining mechanisms for significant events within society. Over the last thirty years, Cohen has identified moral panics within media around drugs, HIV/AIDS, child abuse, paedophiles, computer games, and comic books to name a few. (Cohen xiii-xxvi) School massacres in particular have also been highlighted by Cohen as generating moral panics. Thus, to draw upon Hall once again, the identification of a “problematic reality” occurs which inevitably invites the interpretative frameworks provided by the media that guide social consensus.

Moral panics can draw attention away from a more careful, complex consideration of the mitigating circumstances of an event, attributing it instead to

peripheral factors. “News coverage of youth crime tends to follow a moral panic narrative in which events such as school shootings provide a tipping point for articulating collective anxieties about broader changes in the social structure.” (Greenberg and Wilson 108) As stated earlier, this function of building upon pre-existing anxieties only works to categorize a specific occurrence among other similar events, encouraging the idea of an alarming trend. The theme of youth violence is an often used moral panic discourse linked to an overall perception that there is a growing tendency towards violence among young people. (McRobbie 198, Greenberg and Wilson 108) Donna Killingbeck noted several years prior to Virginia Tech, that school violence was consistently being framed as a moral panic with youth violence at its core. (186) This framework looks to influences such as violent entertainment media and family structure to rationalize, and thereby categorize, violent behaviour, drawing attention away from other relevant mitigating factors within each event. (Saunders 138-139)

The media coverage by the *New York Times* in the week following the Virginia Tech tragedy illustrates the trend identified by Killingbeck as well as the characteristics of an overall moral panic and the power of the media to guide public consensus. Out of the fifty-two relevant articles found, I will present examples which stand out as the most poignant illustrations of Cohen’s five elements of a moral panic. As well as the articles from the *Times*, there is additional coverage from other media sources outside of the one week time frame which warrant mention as they illustrate the effect a moral panic can have on oversimplifying the issues. The final discussion will focus upon privacy legislation and the actions of the Virginia Tech Review Panel taken in the context of the

moral panic. This analysis will suggest how the surrounding moral panic could have influenced their work and their ultimate policy position.

II.I Concern

Over the course of the media analysis, *concern* was found to have been exhibited around potential (or imagined) threats to the safety of students. This manifested in two specific areas in the immediate wake of the events: killers with all too easy access to guns and school shootings that regularly place innocent, young lives in danger. (“Eight years after...”, Roy Apr. 17, Stanley Apr. 17) The day after the shooting on April 17th, the idea of angry malcontents able to arm themselves with ease was an immediately established fear that drew upon pre-existing anxieties from other school massacres like Columbine High in 1999. As one article pointed out while referencing both Columbine and Virginia Tech, “the gravest dangers Americans face come from killers at home armed with guns that are frighteningly easy to obtain.” (“Eight years after...”)

The ability of violent individuals to access guns was a growing point of concern throughout the remainder of the week, highlighting the potential threats that such unrestricted access presented. (Broder Apr. 17, Kulish Apr. 22, “The silence of...”) Evidence was provided and claims made that murders were more easily carried out “by the fact that guns of all sorts are readily available to Americans of all shades of morality and mentality.” (Herbert Apr. 19) As pointed out earlier, politicians and public interest groups often take advantage of sensational events in order to politicize certain issues and give relevance to their claims. The issue of access to guns and gun violence was a rallying point for many groups of this kind. Some right wing factions were demanding that students be allowed to arm themselves to reduce their reliance on the state to protect

them, whereas more left leaning groups were calling for stricter gun laws. (Steinberg Apr. 20, Broder Apr. 17) Debates of this nature only contributed to drawing attention away from other relevant issues stemming from Cho's particular situation.

School shootings as an event were also articulated as an element of concern. These tragedies were established as a frightening but common horror, generating an additional level of apprehension to the unexpected risks created through easy gun availability. Virginia Tech was labelled as a familiar tragedy among many others of its kind, effectively removing Cho's actions and possible mitigating factors from their individual context. (Stanley Apr. 17, Herbert Apr. 19, Whitcomb Apr. 20, Kulish Apr. 22,) The event was held up to Columbine repeatedly over the course of the week, and placed perfunctorily among a list of school shootings that have occurred in the U.S. dating back to 1927. (Dewan Apr. 17) As noted earlier, by distracting the public with this re-contextualization, important issues can be both oversimplified and ignored. By broadly categorizing Virginia Tech as "just another school massacre", a general idea around what are deemed to be the relevant problems is created and thus concern is generated according to those themes.

II.II Hostility

The second element of a moral panic as outlined by Cohen is *hostility*. This aspect represents the performance of moral outrage felt towards the involved parties, which often produces the "folk devil". The folk devil provides society with constant "visible reminders of what we should *not* be." (Cohen 2) This is a form of "social typing", focusing on how "society labels rule-breakers as belonging to certain deviant

groups and how, once the person is thus typecast, his [or her] acts are interpreted in terms of the status to which he [or she] has been assigned.” (Cohen 3)

Discussions of past school shooters set the tone at the beginning of the week, reminding society of what these individuals were supposed to be like, thus providing details that would aid in pigeonholing Cho's behaviour. On April 17th, one day after the shooting, comparisons began between the individuals responsible for the 1999 Columbine high school massacre in Littleton, Colorado and Cho. The Columbine shooting involved two students described as “alienated” and “disaffected”, who identified as Goth, a dark subculture known for its sinister clothing and music. (“Eight years after...”, Broder Apr. 17, Scott Apr. 23) Cho was described numerous times in similar terms as a loner, troubled, disturbed, and alienated. (Carey Apr. 22, “The silence of...”, Scott Apr. 23)

Despite the fact that reports discussed him being diagnosed as mentally ill long before the shooting actually occurred, this did little to cushion the disturbing image created of Cho over the week. (Kleinfield Apr. 22) One article even went so far as to say that we should not always rely upon the explanations provided by medicine and science to excuse the rash actions of people; an element of individual choice and moral responsibility should remain. (Brooks Apr. 19) The state of Cho's mental health was being minimized, and his actions viewed as an individual choice towards violence. A student who was in one of the classes attacked by Cho was quoted as describing him as “just disgusting; he just had no facial expression, showed no signs of emotion or anything”. (Hernandez Apr. 18) Another article described Cho as “indifferent to every small act of human kindness, any effort to connect.” (Carey Apr. 22) He was effectively

characterized as a recognizable folk devil, “a generic malcontent” who “does not shatter the mould for mass murderers.” (Carey Apr. 22)

Within every moral panic there is an element of risk theory concerning society’s perception and acceptance of risk. (Cohen xxvi) This is “intimately tied to the question of who is perceived to be responsible for causing the hazard or damage to whom. This allocation of blame is intrinsic to moral panics.” (Cohen xxvi) At the end of the week, Cho was the easily recognized folk devil for this event and the primary point of blame for the deaths at Virginia Tech. He was typecast as a psychopathic killer within the now familiar framework of the “school shooter”, the “rampage killer”, a well known folk devil persona in contemporary media. As one article states, “The amazing thing is how familiar campus shootings have become. For viewers, initial disbelief is quickly folded into a methodological ritual of breaking bad news.” (Stanley Apr. 17)

Cho is by simple definition a “school shooter”, but this term invokes certain characteristics that do not necessarily correspond with his actual actions. As discussed earlier, Hall understands the media as offering powerful interpretations of *how* to understand certain social events and that those interpretations contain orientations towards the events and the people or groups involved in them. (57) The news coverage presented within the *Times* was orienting its readers towards identifying Cho as fitting the same mould as past school shooters. Because society is so well acquainted with this issue, by understanding Cho within the context of past school massacres, it becomes easier to analyze his behaviour as it can fit into a pre-existing framework, like that of Columbine. Therefore, peripheral factors such as clothing and taste in music, which were widely analyzed following Columbine, were given importance as opposed to other more

relevant issues such as the actions of university administration leading up the shooting and the lack of communication between key bodies on campus holding information on Cho. (Hernandez Apr. 18, Klienfield Apr. 22) In an attempt to make sense of the lapse in acceptable behaviour that has occurred, “people talk less about the event itself and more about the implications of it”. (Cohen 35) The implications in this respect work to reinforce the anxieties of society around school shootings and the attributes of those who commit these acts.

II.III Consensus

After establishing the targets for *hostility* and creating a recognizable folk devil, the next stage of a moral panic is *consensus*. This is the production of widespread agreement that a threat exists and that something has to be done about it. (Cohen xxii) After identifying a clear risk, a discourse of policy change will emerge, bolstered by society's demand for action against the perceived threat. There were several areas where consensus emerged in this instance: access to guns and gun control legislation, campus safety and preparedness, university policy concerning students with mental health issues, restrictive privacy law, and violent entertainment media and youth violence in general. (“Eight years after...”, Roy Apr. 17, Lewin Apr. 18, Oakley Apr. 19, Dewan and Santora Apr. 19, Scott Apr. 23) It is necessary to touch on all of these in order to evaluate if and how they had an impact upon the response from both the Virginia Tech Review Panel and society in general.

Access to guns and gun control was the first problem identified that called for a policy response. Articles that touched on this issue ranged over the entire week, but its early flagging preceded many of the other concerns listed above. On the first page of the

Times a mere day after the shooting, unease was reported from public interest groups and the media in general on this point. (Broder Apr. 17) Josh Horwitz, the executive director of the *Coalition to Stop Gun Violence* was quoted in a front page article on April 17th stating that “Virginia’s gun laws are some of the weakest state laws in the country, and where there have been attempts to make some changes, a backdoor always opens to get around the changes, like the easy access at gun shows.” (Broder Apr. 17) This theme continued throughout the week, with the “laissez-faire weapons marts of Virginia” touted as a point of distress for the American public. (“The silence of...”) By the end of the week calls for changes to gun laws had been proposed regarding access and availability. (Sullivan Apr.23)

Anxious questions also arose as to how well university faculty are prepared for this sort of tragedy. One editorial featured ended with the stinging question: “Can administrators and deans really continue to leave professors and other college personnel to deal with deeply disturbed students on their own, with only pencils in their defense?” (Oakley Apr. 19) Consensus emerged throughout the week around the need to address the lack of knowledge and expertise on the part of the universities when having to deal with mentally troubled students. (Lewin Apr. 19) This issue was of particular interest as Cho had a long history of mental health issues to which some argued Virginia Tech administration did not give appropriate attention. (Lewin Apr.19, Santora and Hauser Apr. 20) Lucinda Roy, one of Cho’s English professors, told the *Times* that she had sent examples of Cho’s writing, which had disturbed many other faculty members as well, to the campus police, campus counselling service and other officials as far back as 2005. According to Roy, the university held the position that little could be done despite the

obvious discomfort many students and faculty had around Cho. (Dewan and Broder Apr. 18)

The response time of Virginia Tech's campus police department to the shootings was also placed under heavy scrutiny. Although Virginia Tech officials had opportunities to defend their handling of the shootings (Urbina and Fernandez Apr. 20, Broder Apr. 17) the media found many parents, students, and faculty were still concerned with the fact that two hours had occurred between Cho's initial killing of two individuals and the subsequent shootings that occurred at Norris Hall. (Broder Apr. 17, Dewan Apr. 17) An email sent by a member of the university's engineering faculty illustrating strong anger at the school was quoted as saying: "I am outraged at what happened today on the Virginia Tech campus. Countless lives could have been saved if they had informed the student body of the first shooting. What was the security department thinking?!" (Dewan Apr. 17) One parent of a Virginia Tech student also outwardly expressed frustration to the media: "As a parent, I am totally outraged. I would like to know why the university did not immediately shut down." (Broder Apr. 17) By presenting the direct sentiments of parents and faculty, the media were able to strengthen the image of an overarching public consensus around the weaknesses in Virginia Tech's emergency response system and actions, thereby reinforcing the need for policy change in this area. This point was not lost on the Virginia Tech Review Panel, as will be noted in the final analysis of this chapter.

Violent entertainment media and youth violence were hastily linked as an element of consensus as this made it easy to categorize Cho among other school shooters as discussed in the section on folk devils. (Scott Apr. 23) As was discussed, by attempting

to understand Cho through the lens of past shootings, importance can be placed by the media and the public upon factors that do not have any true bearing on the event. The example of Columbine worked to illustrate an overall link between Virginia Tech and school massacres, acting as a point of consensus around dark and violent media targeted to youth. However, it was a very vague connection presented by the media in which the Review Panel ultimately found no merit and so could make no recommendations for policy change on the issue. The stretch to label Cho as a violent-movie watching, jaded youth will be revisited again when discussing the element of *disproportionality*, as exaggeration of the strength of this claim becomes quite apparent within the news coverage.

The last area of consensus with specific importance to this study is the disquiet around privacy legislation. Despite the fact that officials at Virginia Tech knew of Cho's psychiatric problems and potential for violence, Cho's professors in English (his major) and the associate dean of students are reported to have had no record of problems with Cho. (Dewan and Santora Apr. 19) At several points throughout the week, quotes from administrative faculty and staff from Virginia Tech illustrate a common assumption that little to nothing could be done about the threatening demeanour and behaviour that Cho displayed. (Dewan and Broder Apr. 18, Lewin Apr. 19) One article in particular titled "Laws Limit Colleges Options When a Student Is Mentally Ill" stated outright that "universities cannot tell parents about their children's problems without the student's consent. They cannot release any information in a student's medical record without consent." (Lewin Apr. 19) Calls for change to relevant privacy provisions grew quickly out of these criticisms. The *Family Educational Rights and Privacy Act* (FERPA), along

with the *Health Insurance and Portability Act* (HIPAA) were the main pieces of U.S. privacy legislation criticized as being too restrictive with regard to student and medical records respectively. (Lewin Apr. 19)

It is important to note that long after the initial moral panic had subsided, this sentiment continued to be reproduced in the media. About a month after the shootings an article appeared in *The Chronicle of Higher Education* reporting that Kay K. Heidbreder, Virginia Tech's chief legal counsel, had told Virginia Tech's Review Panel that "state and federal laws are so restrictive that the campus's police department and university administrator's could not share Mr. Cho's academic, medical, or disciplinary records". Further evidence of this pervasive element of consensus appeared again *five months* after the massacre. *The Washington Post* printed an article titled "When Privacy Laws Do More Harm Than Good" which echoed the criticisms around obstructive privacy laws when it comes to information sharing about at-risk students. The overall tone of this article was to condemn privacy laws as being too restrictive, separating individuals from their "human obligations" for care and concern. (Fisher Sept. 2) The resulting influence of this particular area of consensus was quite persistent, as will be seen when addressing the impact of this moral panic upon the Review Panel's deliberations.

II.IV Disproportionality

The fourth element to be addressed within a moral panic is *disproportionality*. This aspect is intended to address the exaggeration of various details around an event that occurs during a panic. The coverage of Virginia Tech displayed three main techniques of exaggeration. These techniques were identified by analyzing the following: descriptive

language used by the media when discussing the event, over-generalizations made about safety risks, and the implied significance of various popular culture elements.

Language was the initial and most obvious element of disproportionality to be found during the media analysis, with the shooting described in exaggerated and, at times, overly emotional terms. The more dramatic approaches used vivid descriptions to play out scenes of the massacre in embellished detail, “They [the gunshots] went on, for what seemed like 10 or 15 or 20 minutes, an eternity with punctuation. Bang. Bang.” (Dewan Apr. 17) “Room 207 was a scene of utter terror and panic, with students trying to escape out windows or cowering under desks”, “we look on aghast, as if the devil himself had appeared from out of nowhere.” (Hernandez Apr. 18, Herbert Apr. 19) Several articles rhetorically asked “how did we end up here, yet again” amidst an “eruption of murderous violence”. (Whitcomb Apr. 20, Herbert Apr. 19) The tragedy itself was described as “senseless death-as-usual”, a situation for which “everybody knows the drill”. (Stanley Apr. 17)

It is true that school shootings have been on the rise since the early 1990s, a quick glance at the *Times* reveals as much in a timeline produced early in the week. (Dewan Apr. 17) Yet the language used to frame school shootings expressed a sense of panic reflected in the exaggerated response from surrounding academic communities. The day after the shooting, universities in Oklahoma, Tennessee and Texas cancelled classes and a Louisiana public school district locked down its middle and high school. (Lewin Apr. 18) Security officials were said to have been on edge and worried about copycat incidents. At the University of Oklahoma the police ended up responding to reports of a “suspicious person with a weapon”, the “weapon” turning out to be an umbrella. (Lewin Apr. 18)

This frenzy of fear, encouraged and reinforced by the excessive language of the media, worked to fuel the anxieties of surrounding communities.

The second type of disproportionality I found was in the claimed number of psychopathic killers waiting to act out upon society. The numbers alluded to over the course of the week concerning individuals capable of a massacre were grossly exaggerated at several points. One editorial stated bluntly that “it’s a simple fact that, for every deranged murderer like Mr. Cho there are thousands more oddballs just below the breaking point.” (Oakley Apr. 19) These claims are offered without proof and are framed as so obvious they do not require data to be credible. Another article, published on the day following Cho’s attack, claimed that “none of us is safe as long as there are angry young men who yearn to blast a hole in the world.” (Roy Apr. 17) Concerns around potential threats from violent individuals were raised in very ambiguous terms that allowed for a reader’s imagination to fill in any number of hidden murderers lurking below the social radar ready to shake the moral foundations of decent, law-abiding communities.

The third area of exaggeration noted during the analysis concerned the influence of violent media and popular culture upon Cho’s actions. Much media attention was paid to the clothing, music and movie tastes of Cho, trying to find some tie between his violent actions and possible pop-culture influence, as had been done with past school shooters like those at Columbine. This is a pre-existing media frame developed during past moral panics that is being utilized again to help break down the event into comprehensive pieces, a tactic discussed earlier in this chapter. Cho was described on the day of the shooting as “dressed in a black leather jacket and wearing a maroon baseball cap”.

(Hernandez Apr. 18) A suitemate of Cho's told the *Times* that he would "repeatedly play "Shine", a song of spiritual longing from the Georgia alternative rock band Collective Soul." (Kleinfield Apr. 22) None of these details however pointed to a specific area of personal interest the media could rationalize Cho's actions through, as had been done with Columbine for example and the criticisms of Goth culture that emerged from that tragedy.

It was towards the end of the week that experts and opinionated editorialists began to try and fill in the gaps with their own assumptions that had been created when attempting to fit Cho into the existing character mould for school shooters. (Steinberg Apr. 20, Dewan and Santora Apr. 19) Weak ties to violent movies based on Cho's race, nationality and photos seen of him prior to the attack gave some basis for conjecture among several journalists. A single photograph of Cho wielding a hammer drew intense scrutiny and comparisons to the violent 2004 South Korean film "Oldboy". (Dewan and Santora Apr. 19) A *Washington Post* article, which was also quoted in the *Times*, explains that the main character of this film exacts a rampage of bloody revenge, largely with the use of a hammer and that the visual and racial ties to Cho "must feature prominently in the discussion, even if no one has yet confirmed that Cho saw it". (Hunter Apr. 20)

A completely hypothetical analysis around the influence of this film was created despite the fact that no evidence has surfaced that Cho ever saw this film or was even aware of it. (Steinberg Apr. 20) A journalist with the *Washington Post* suggested that "on the surface, it [the movie] seems a natural fit, at least in the way it can be presumed that Cho's hyper-fervid brain worked. It's a Korean story -- he would have passed on the

subtitles and listened to it in his native language -- of unjust persecution and bloody revenge. A narcissist with a persecution complex would identify with its plot". (Hunter Apr. 20) Further ties to the films of another movie director, John Woo, were also made due to the director's reputation as a violent filmmaker and because he is also Asian. (Steinberg Apr. 20) However, there is also no evidence that Cho saw the films of John Woo either. (Steinberg Apr. 20) The effect of this disproportionality was the fabrication of influences to which Cho's actions were attributed. Drawing upon Hall, the media have attempted to break down this event into manageable pieces based on past knowledge, yet their misleading interpretations have provided society with an erroneous justification of the events. These false interpretations also managed to influence the work of the Review Panel, as will be discussed shortly.

II.V Volatility

The final element of a moral panic according to Cohen is *volatility*. This is essentially the eruption of a public panic followed by its quick, unexpected dissipation. When looking at the distribution of articles over the week of analysis, the volatility of the issue is quite apparent. The majority of the articles for the week appeared within the first four days following the shootings. Of the fifty-two consulted for this media analysis, thirty-nine of them appeared between the 17th and the 20th, equivalent to seventy-five percent of the articles for the week. April 19th, three days after the shooting, had the most reporting with thirteen articles devoted to discussing Virginia Tech. This single day produced twenty-five percent of the week's total coverage. The last three days of the week had thirteen articles total, the same quantity produced in one day of coverage on the

19th. The clear drop in coverage following the first four days illustrates the rapid dispersal of interest by the media and the fading out of the initial panic.

By the end of the week, within the coverage offered by the *New York Times* all five elements of a moral panic had emerged, ending with a rapid drop-off of attention. What followed in the wake of this moral panic will be the focal point for the remainder of this chapter. To refer back to Cohen's words, "Sometimes the panic ... has more serious and long-lasting repercussions and might produce such changes as those in legal and social policy". (1) My concern is with the ramifications this moral panic had upon influencing the actions and policy recommendations of the Review Panel, specifically relating to privacy and information sharing. However, the creation of the Review Panel itself also warrants consideration as the speed of its inception appears to reflect some influence from the moral panic.

II.VI Moral Panic: Influence and Impact

The Virginia Tech incident occurred on April 16th. Three days later on the 19th, Timothy M. Kaine, Governor of Virginia, announced the formation of the Virginia Tech Review Panel. It was the task of this panel to undertake an independent review of the situation and the efforts of the Commonwealth of Virginia in responding to the tragedy. (Report of the Virginia Tech Review Panel vii) This quick response and assembly of individuals happened to coincide with the height of the moral panic for the week on April 19th. This panel was created in the midst of the public and political uproar demonstrated by the media. This is not to say that direct correlations can be made between the construction of the Panel and the moral panic, but there are strong consistencies between the two that should be highlighted.

Governor Kaine called upon eight individuals to serve upon this panel. They are listed as follows along with their credentials as they appeared in the Report:

- > Panel Chair Col. Gerald Massengill, a retired Virginia State Police Superintendent who led the Commonwealth's law enforcement response to the September 11, 2001, attack on the Pentagon and the sniper attacks that affected the Commonwealth in 2002.
- > Panel Vice Chair Dr. Marcus L. Martin, Professor of Emergency Medicine, Assistant Dean of the School of Medicine and Associate Vice President for Diversity and Equity at the University of Virginia.
- > Gordon Davies, former Director of the State Council of Higher Education for Virginia (1977–1997) and President of the Kentucky Council on Postsecondary Education (1998–2002).
- > Dr. Roger L. Depue, a 20-year veteran of the FBI and the founder, past president and CEO of The Academy Group, Inc., a forensic behavioral sciences services company providing consultation, research, and investigation of aberrant and violent behavioral problems.
- > Carroll Ann Ellis, MS, Director of the Fairfax County Police Department's Victim Services Division, a faculty member at the National Victim Academy, and a member of the American Society of Victimology.
- > The Honorable Tom Ridge, former Governor of Pennsylvania (1995–2001) and Member of the U.S. House of Representatives (1983–1995) who was also the first U.S. Secretary of Homeland Security (2003–2005).
- > Dr. Aradhana A. "Bela" Sood, Professor of Psychiatry and Pediatrics, Chair of Child and Adolescent Psychiatry and Medical Director of the Virginia Treatment Center for Children at VCU Medical Center.
- > The Honorable Diane Strickland, former judge of the 23rd Judicial Circuit Court in Roanoke County (1989–2003) and co-chair of the Boyd-Graves Conference on issues surrounding involuntary mental commitment.

(Report of the Virginia Tech Review Panel vii)

Each representative on the panel has expertise that touches upon an area of consensus that was constructed and emphasized by the media during the panic. Knowledge and experience with safety and preparedness, mental health issues among students, and violent youth behaviour are all reflected in the credentials of the Review Panel.

Along with the consistencies between the expertise of the panel members and consensus formed during the panic, there are also correlations that can be found within the research conducted by the Panel and the direction of administrative action taken. The following is an examination of how the media discourse during the week after the shootings mirrors the general path of discussion and response taken by the Review Panel. The Report consisted of eleven chapters, many of which reflect the myriad of issues and criticisms that were raised over the course of the week-long media analysis. Gun control, privacy laws, university safety and emergency response, student mental health and violent media effects are major areas of consideration and evidence that were examined by the Review Panel. These topics correspond directly with the elements of the moral panic presented in the first portion of this chapter. Like the striking of the Review Panel, direct causal links may be hypothetical, but the discursive parameters of the moral panic and that of the Report are so similar it is difficult not to give some credence to a possible relationship.

Discussion of access to guns and gun control were heavily apparent during the moral panic. Arguments were put forth stating that easy access to guns was the major problem that triggered this event, while more extreme opinions claimed that if students had been able to arm themselves and freely carry guns on campus they would have been able to ensure their own safety without having to rely on others, like university security. ("Eight years after...", Steinberg Apr. 20) The Review Panel addressed this issue directly in chapter six of the Report, admitting outright that they recognized the deep divisions in American society concerning readily available firearms. (Report of the Virginia Tech Review Panel 71) The Panel found that Cho's gun purchases were

considered illegal under federal law due to his mental health record. (Report of the Virginia Tech Review Panel 71) However, Virginia's state law was not as clear as to whether an individual with a mental history like that of Cho should be able to legally purchase firearms. (Report of the Virginia Tech Review Panel 71-73) Nevertheless, the overall issue was found by the Panel to be outside the scope of the university's control, thereby shifting the ability to act upon gun legislation to the state.

The Report also appeared to respond to claims raised in the media of whether students should be arming themselves. The Review Panel pointed out that students had, at one point, been able to carry weapons on campus, but a total gun ban policy had been instituted a few years prior to the massacre. (Report of the Virginia Tech Review Panel 74) The Report went further to address the claims regarding a student's need to protect him or herself, concluding that if students had in fact possessed their own weapons during the massacre, the situation may not have been much better. Accidental shootings could have occurred and police outside would have shot anyone emerging with a gun from the building where the massacre took place. (Report of the Virginia Tech Review Panel 75)

The Report illustrates further parallels between the moral panic and criticisms levelled towards the university's security. The Virginia Tech Police Department was under heavy fire within the media. As demonstrated earlier in this chapter, both parents and faculty were called upon to present their criticisms in relation to the ability of the university to properly respond to an emergency of this nature. These criticisms appeared to carry significant weight as the Report devoted an entire chapter to respond to these criticisms, which for the most part were acknowledged by the Review Panel as justified.

(Report of the Virginia Tech Review Panel 17) During the moral panic, consensus was expressed that more had to be done about the university's ability to notify students of an emergency. The findings of this report were produced four months after the shooting, by which time Virginia Tech had made several modifications to their safety procedures. The university had updated their Emergency Response Plan, moved forward with updates to emergency notification systems (such as campus sirens and cell phone text messaging), and began implementing a new Unified Campus Alerting System which "would allow university officials to send an emergency message that would flow in parallel to computers, cell phones, PDAs, and telephones." (Report of the Virginia Tech Review Panel 15)

A final consistency that illustrates the similarities between the moral panic discourse and the efforts of the Panel can be found within the disproportional reaction to violent media and its perceived role in Cho's motivations. As discussed earlier in the chapter when analyzing the element of disproportionality, there were attempts to link Cho's behaviour with dark and violent entertainment media as had been in done in the past with events like Columbine. Chapter four of the Report gives a very thorough background to the mental history of Cho, which follows the same path of reasoning found within the media. The Panel's research involved discussions with his parents and sister, and examinations of his pre-university education, health, mental and emotional care. The Report addressed the issue of possible violent media influences but found that Cho had never engaged with media of this nature; his family supported this point. Video games like Sonic the Hedgehog were apparently his preference. (Report of the Virginia Tech Review Panel 32) None of the video games he played were war games or had violent

themes, and his favourite movie was apparently X-Men, nothing along the lines of “Oldboy” or John Woo films. (Report of the Virginia Tech Review Panel 32)

There is a clear homology between the moral panic and the discussions and research of the Panel, even though *The New York Times* is never once quoted or referred to within the Report. It is interesting to note the almost responsive quality the Review Panel adopted when setting the parameters of their research. Changes to campus safety procedure and policy were implemented following calls for action on this point from the public. Despite the fact that Virginia Tech has no power over gun legislation, the Panel still devoted time and resources to examining and discussing this issue. These two examples do illustrate a parallel between public interest and administrative action; however, the power of a moral panic is best seen when discussing violent entertainment media as a possible influence. Cho never showed any signs of having interests of this nature, yet the Report still examined the possibility. The Panel drew upon the pre-existing structures of understanding from past school massacres to try to categorize and thereby comprehend Cho’s behaviour, even though there were no reasonable links to be made on this point. The power and ability of the media to influence the work of decision makers can be seen here.

The remainder of this chapter will address the significant areas within the Report of the Review Panel that demonstrate where elements of the moral panic specifically impacted policy recommendations and procedural changes for privacy and information sharing. A very large misconception created during the moral panic was that federal privacy laws in the U.S. disallowed the sharing of vital information concerning the danger Cho posed to himself and others, as well as information regarding his mental

stability, psychiatric confinement and treatment, and disciplinary record. Virginia Tech was in the difficult position of having to operate under several different pieces of legislation, each with its own standard of information sharing and privacy.

The *Family Educational Rights and Privacy Act* (FERPA) and the *Health Insurance Portability and Accountability Act* (HIPAA) are the two pieces of legislation that created the most confusion in the press and for university administration. FERPA sets out the privacy standards required for student education records held by an institution. HIPAA deals specifically with personal health records and the privacy standards required for this type of data. In addition to these two pieces of legislation, there was also some conflict between HIPAA and *Virginia Code 32.1-127.1:03 Health Records Privacy* (VaHRP), but this conflict was not the main focus of the Report's analysis of information privacy laws, nor was it particularly apparent within the media. (Report of the Virginia Tech Review Panel 57, 63)

Within the articles analyzed, the *Times*' "Laws Limit Colleges' Options When a Student is Mentally Ill" and the *Washington Post*'s "When Privacy Laws Do More Harm Than Good" display a distinct lack of knowledge of the actual provisions within FERPA and HIPAA. The general consensus was that privacy laws were a direct bar to sharing information about Cho's behaviour and mental state, contributing to the overall lack of knowledge that ultimately led to the tragedy. Ontario's own Privacy Commissioner, Ann Cavoukian, responded to these claims with an article in the *Washington Post* titled "The Laws Didn't Fail". She claimed in her response that both HIPAA and FERPA "permit the sharing of information in situations involving imminent threats to health or safety." (Cavoukian A14) Cavoukian also stated that "to infer that privacy protections were

responsible for the events at Virginia Tech is to completely misunderstand the role that privacy plays in preserving liberty.” (A14) According to the findings within the Report of the Review Panel, Cavoukian is entirely correct.

After reviewing FERPA and HIPAA, the Panel found that “much of the frustration about privacy laws stems from lack of understanding”, yet even within the pages of the report there still appears to be some confusion. (Report of the Virginia Tech Review Panel 63) The Panel claims in one instance that the laws were poorly designed to accomplish a balance between protecting privacy and allowing necessary information sharing. However, they also state that “when seen clearly, the privacy laws contain many provisions that allow for information sharing where necessary.” (Report of the Virginia Tech Review Panel 63) The contradictions displayed in the Panel’s understanding do not reflect a sense of clarity needed to maintain a proper balance between public interest and private rights. “During Cho’s junior year at Virginia Tech, numerous incidents occurred that were clear warnings of mental instability. Although various individuals and departments within the university knew about each of these incidents, the university did not intervene effectively. No one knew all the information and no one connected all the dots.” (Report of the Virginia Tech Review Panel 2)

It is clear from the findings of the Panel that a greater understanding was needed on the part of Virginia Tech officials involved in safety and administration as to how FERPA and HIPAA operate independently, as well as in conjunction with each other. Yet, despite the fact that understanding of these laws is lacking and provisions allowing sharing are already included, the Panel still made recommendations for changes to the legislation. Suggesting changes to a body of law that is not entirely clear to those who

use it illustrates a motivation for action that may be driven by social pressure rather than informed decision making. The moral panic that surrounded the tragedy was fuelled by misinformation, but the calls for changes to privacy policy were still loud and clear. If the Review Panel had not made any policy recommendations, they may have been perceived by the wider public as ignoring what the surrounding community and media had defined as a problem desperately requiring change. Pressure to act on what were viewed as harmful privacy laws existed before the Review Panel convened. This could have placed undue pressure upon the Panel to make recommendations and to be seen to be making recommendations when the time finally came.

Some of the suggestions made by the Panel, arguably, do not reflect changes that are necessary or helpful to the establishment of sound university policy and the building of a proficient legislative knowledge base around FERPA. Seven recommendations were put forth, with two focusing on revisions and interpretations needed for active privacy legislation. The initial item lies with the Panel's recommendation that privacy laws be revised to include a "safe harbour" provision so as to "insulate a person or organization from liability (or loss of funding) for making a disclosure with a good faith belief that the disclosure was necessary to protect the health, safety, or welfare of the person involved or members of the general public." (Report of the Virginia Tech Review Panel 68)

During the moral panic issues were raised in the *Times* around liability and how universities could be placed in a double bind. They "may be liable if they fail to prevent a suicide or murder", but could also be "held liable if they do take action to remove a potentially suicidal student". These are scenarios that have both already occurred with American universities. (Lewin Apr. 19) Yet, if privacy legislation already allows for an

institution to share information during specific instances involving the safety of an individual or group, a section like this should not be necessary. Furthermore, by including something of this nature, the balance between individual privacy and public interest may be disturbed. If a person or organization is not given reason to pause when deciding whether to share information, rash decisions could be made. The assured knowledge of protection under the law should anything go wrong may minimize the consideration of negative consequences that could result from a poor choice.

The second change to privacy legislation recommended by the Review Panel was for the Department of Education to “allow more flexibility in FERPA’s ‘emergency’ exception.” (Report of the Virginia Tech Review Panel 69) Currently, the way the legislation is written “allows for the release of records during an emergency when the disclosure is necessary to protect the health or safety of either the student or other people” (Report of the Virginia Tech Review Panel 69) The issue is that this exception is strictly construed by the Department of Education. The Panel feels this is “unnecessary and unhelpful”, and only “feeds the perception that nondisclosure is always the safer choice” (Report of the Virginia Tech Review Panel 69)

During the moral panic around Virginia Tech, a *Times* article did raise the problem of confusion around what constituted an “emergency”, but I would argue that widening the definition of an “emergency” is problematic. (Lewin Apr. 19) By opening up the classification of this term, a wide scope of ambiguity and conjecture as to its meaning is created which can be just as damaging as a “strict construction” definition. If there is a lack of consensus on the level of risk posed by a student, a general interpretation will not provide administrators with a concrete example with which to

assess the situation. Clarifying with the U.S. Department of Education what is meant by an “emergency” under the strict construction rule would give American universities a concrete definition to apply. Without this, general interpretation would give more weight to the subjective views of various administrators rather than providing them a framework with which to develop their assessments.

The overall purpose of this chapter was to illustrate the moral panic surrounding Virginia Tech and to examine how it may have both structured the Panel’s discussion, as well as set interpretive frames into which any subsequent policy considerations would be placed. The terms of analysis available to this decision-making body were very likely constrained by the existing moral panic discourse. Looking at the policy recommendations of the Panel, it appears that the fine balance between individual privacy and public interest has been tipped towards the public interest as a result of the public consensus that arose during the panic. As was demonstrated, Cho’s identity as a folk devil outweighed any consideration from the public as to other issues around the university’s lack of policy knowledge and information sharing which contributed to his deficient mental health treatment. The Panel responded with a negative interpretation of privacy law, reflecting the sentiment expressed during the panic, which ultimately treated the legislation as a block to public safety.

Their recommendations seek to free institutions from liability when releasing information and give administrative bodies greater power in making subjective decisions as to what constitutes an emergency. The latter recommendation would allow a university to override any personal information protections available under the law should administration arbitrarily decide that there is an emergency. There is no

appreciation for upholding the standards of individual protection available in the law. Because there was an initial lack of clarity surrounding the relevant legislation from the start, there was no foundation of understanding or reason upon which to build a response to the negative reactions held towards these pieces of legislation. Had there been clarity from the beginning as to what these laws allowed in terms of information sharing, the recommendations for change made by the Panel may not have favoured the public interest so heavily, but then Cho may not have fallen through the cracks either.

Examination by the Panel as to why clarification was never sought by Virginia Tech administrators, or why their legal counsel was uninformed as to the scope of either FERPA or HIPAA is never provided within the pages of the Report. These individuals were responsible for understanding the necessary policy provisions in order to maintain a wider scope of information when dealing with at-risk individuals, yet their gap in knowledge goes widely unaccounted for except to say that the legislation was confusing. (Report of the Virginia Tech Review Panel 63) This lapse in administrative knowledge will be further examined in the following chapter in order to understand precisely how this uninformed state affected the university's ability to effectively balance both public interest and individual privacy rights.

The examples from this tragedy illustrate the importance of a proper understanding of privacy legislation when dealing with at-risk individuals; this clarity of understanding should happen *before* a tragedy with the magnitude of Virginia Tech occurs. Once a moral panic has happened, it is very difficult to engage in objective decision making, especially when the institution has received criticisms regarding inaction. It is also important for an institution to clarify what its position is when

multiple pieces of privacy legislation may apply, such as FERPA and HIPAA in the American context. Should overlap occur the importance of comprehending how two or more sets of laws interact can greatly influence procedure during an emergency situation. For Ontario universities this is of particular importance as the *Freedom of Information and Protection of Privacy Act* applies to personal information, but the *Personal Health Information Protection Act* applies to personal health information. Some universities have various facilities on campus in which this type of data falls under both. The following chapter examines Ontario's situation.

Chapter III A New Framework for Ontario Universities: Understanding FIPPA

As Chapter Two discussed, the major impediments offices of Virginia Tech faced to sharing information on Cho and his behaviour were due in part to a fatal lack of knowledge of the provisions within that institution's privacy legislation. The Virginia Tech Review Panel found that the *Family Educational Rights and Privacy Act* (FERPA) contains provisions which would allow for the sharing of information during emergency circumstances. (Report of the Virginia Tech Review Panel 63) However, the realization of this fact after experiencing an immeasurable loss of life is a painful demonstration of the consequences that can occur when there is a lack of institutional knowledge of relevant policy. During difficult situations an institution can benefit from a thorough comprehension of the black letter provisions within applicable legislation. As was demonstrated in the previous chapter, without this foundation of knowledge it is difficult to ensure sound policy decisions that balance public interest and private rights when faced with persistent social pressure demanding action.

A university should have a strong foundation of policy knowledge and be able to illustrate internal practices that adhere to that policy, or they risk being coerced by public sentiment in the wake of disaster. Administrators at Virginia Tech lacked the necessary understanding of relevant privacy policy and so were placed in a difficult position as they could not respond to the public from a knowledgeable standpoint. The university became subject to the direction and pressures of the moral panic rather than their own principled understanding. As mentioned, the only reason given by Virginia Tech to justify their knowledge gap in policy was that the legislation was confusing. (Report of the Virginia Tech Review Panel 63) Despite this uncertainty, clarification was looked for only *after*

tragedy had taken place. Currently, Ontario universities are in a position where they may examine and clarify privacy legislation independently of social pressures and preconstructed knowledge frameworks of a crisis, like those of moral panics. Understanding the provisions, ambiguities and limitations of the province's legislation can help universities identify necessary points of clarification, and thereby work to circumvent critical inconsistencies in communication like those suffered by Virginia Tech.

The *Freedom of Information and Protection of Privacy Act* (FIPPA) is a relatively new piece of legislation for Ontario universities, although the Act itself has been in force for twenty years within the province. (Information and Privacy Commissioner of Ontario "Access and Privacy Excellence...") The political climate at the time of its introduction and assent in the mid-1980's was dominated by the increasing unpopularity of the Conservative government under the Premier Davis. The introduction of FIPPA in 1985 was seen as a positive change for Canadian society which had "lived so long with the secrecy of the Conservatives". ("Information on Order") Initial application of FIPPA was intended to regulate the privacy practices of public government institutions, as the government had been marred by vocal criticisms of closed dealings and secrecy, particularly around the controversial Meech Lake Accord. (Geddes 16, 17)

Ian Scott, former Attorney General for Ontario, was the force behind this legislation. Through FIPPA, Scott sought to institute more transparency for government held information in the province, and to allow members of the public to have more access and control over their personal information. He was a strong advocate of these values, and made no effort to cushion the intentions of the legislation when introducing it to the

legislature. Scott stated on the day he first introduced the bill to Ontario's Legislative Assembly on July 12th, 1985:

Let there be no doubt that, notwithstanding the difficulties the concepts of freedom of information and the protection of individual privacy may pose, they are fundamental principles for this government...We do not now and never will accept the proposition that the business of the public is none of the public's business...The goal of the privacy aspect of the legislation is to strengthen protections for the personal information in government files and data banks and to give individuals access to personal information relating to them...I recognize and have no doubt that at some point in the future information could be made public under this new bill that could embarrass or harm the fortunes of the government of the day. We recognize that possibility; however it is a fact of life and a natural consequence of an open, consultative government. It will achieve the greater good of parliamentary democracy, open administration and thus the good of society as a whole. That potential risk, that potential cost, can and must be borne in the interest of freedom. (Scott)

On January 1st, 1988, nine months after the Meech Lake Accord had been signed in secret, FIPPA became the first active freedom of information legislation in the province of Ontario. Prior to this there had been efforts by other politicians to raise the profile of government transparency and individual privacy issues, but it was through Scott that FIPPA was first introduced to Ontario and these matters were able to gain legislative force. ("Information on Order")

Almost twenty years after its inception, FIPPA was extended to govern the privacy practices of universities. In keeping with Scott's theme of institutional transparency and accountability, as well as public access to personal information, universities were brought under FIPPA in 2005. Bill 197, also known as the *Budget Measures Act, 2005*, contained the amendments to FIPPA that have since altered the privacy framework for Ontario post-secondary institutions. The specific section of Bill 197 concerning the addition of universities under FIPPA reads:

The Freedom of Information and Protection of Privacy Act is amended in order to accommodate the inclusion of universities as institutions under the Act. A definition of “educational institution” is added to subsection 2(1) of the Act. (Schedule F, Bill 197)

Bill 197 received royal assent on December 12th, 2005, taking effect for universities on June 10th, 2006.

The office of Ontario’s Information and Privacy Commissioner (IPC) is the independent body responsible for ensuring compliance with all provincially legislated privacy law, including FIPPA. The IPC works to oversee the application and enforcement of the laws, and handles all appeals and formal privacy complaints that occur within the province. The interpretations and precedents that flow from this body are regarded as authoritative on privacy issues in Ontario. It was pressure by the IPC that ultimately led to universities becoming subject to this legislation. As part of their operating budget, universities regularly receive large transfer payments from the government. Prior to FIPPA, the records of these transactions were not subject to public review. This was a problem in the eyes of the IPC. As stated in the 2004 Annual Report, “One of the foundations underlying freedom of information is the principle that organizations that exist by virtue of public funding should be subject to public scrutiny through FOI laws”. (7) Universities were interpreted by the IPC as having this quality and so urged the Ontario government to extend FIPPA to them.

Unfortunately, despite two decades of application in the public sector, understanding of this legislation within an academic institutional context did not begin until FIPPA’s scope was widened in 2006. Thus, it has been a steep learning curve for Ontario’s universities. There is little precedent that applies to the specific setting of a university, especially in relation to information sharing when dealing with an at-risk

individual. At a conference in January of 2008, a panel speaker from the office of the IPC attempted to shed some light on this very issue. The IPC representative noted that the Privacy Commissioner “does not take the view that privacy laws must be read in a way that is obstructive in resolving serious emergencies or that personal information or personal health information may not be disclosed to prevent harm”. (O’Donoghue) However, despite the support of the IPC in maintaining balance between public interest and private rights, there are no practical examples of incidents that have challenged this balance, as none have yet emerged. As a result, Universities need to create their own understandings and interpretations of FIPPA relevant to their environment and the unique safety issues they face.

The following discussion will address the provisions of FIPPA that govern the disclosure of information when a safety risk arises, as well as potential issues of overlap with other pieces of legislation. The purpose of this is to provide a basis of understanding for both the legislation and the considerations involved with maintaining a balanced approach to potential safety risks within a student population. Because there are no practical examples upon which to base such an approach, having at least a thorough comprehension of the relevant legislation may aid in directing a response during a difficult situation that is sensitive to both perspectives. The discussion will also address how FIPPA compares to FERPA in its provisions, demonstrating that FIPPA may in some respects be easier to apply and interpret. A hypothetical information sharing structure and the cautions needed to ensure it does not move into the realm of intrusive surveillance will be examined in Chapter Four, as this issue warrants a thorough analysis of its own.

The overall analysis provided in this chapter is intended to illustrate that the basic tools for ensuring balance between the public interest and individual privacy rights are already present within Ontario's black letter law. The value of realizing these legislative capabilities is directly related to the difficulties posed by a moral panic. Public demands for change in the wake of disaster are difficult to manage when an institution has no understanding upon which to base a response. This is why it is favourable to identify potentially useful provisions before tragedy strikes so as to avoid being subject to the emotionally driven demands of a wounded community.

When evaluating the U.S.'s FERPA, section 1232g. (b)(1)(I) allows the release of a student's "education records" during an emergency in order to protect the health or safety of a student or other persons. However, when the Review Panel examined the definition of an "education record" they discovered that this term did not necessarily extend to *all* information about a student existing within an institution. (Report of the Review Panel 66) For example, "personal observations and conversations with a student fall outside of FERPA." (Report of the Review Panel 66) This inconsistency relates directly to data collected about Cho by his professors and residence staff. Their data consisted of observations and discussions about his troubled state, his disturbing behaviour in class and in residence, violent content in his submitted work, and his conduct when approached individually – all of which is not considered to be an "education record" under FERPA.

The implications of this were that these observations could have been shared with "school officials, law enforcement, parents, or any other person or organization" without even having to rely on the emergency disclosure exemptions under FERPA. (Report of

the Review Panel 66) This could have potentially provided a clearer insight into Cho's fragile mental state when combined with other pieces of information university administration held. This added to the confusion around disclosure at Virginia Tech as professors and residence staff holding pertinent information concerning Cho's potential for violent behaviour were unaware of the status of this information or of their ability to share it with others.

Ontario's FIPPA does not differentiate specifically between education records and personal information, as they are considered to be one and the same. In some respects this could be seen as a benefit as there is no second guessing as to whether certain types of information would fall under FIPPA. The definition under s.2(1) of FIPPA for personal information is quite inclusive, comprising:

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except where they relate to another individual,
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- (g) the views or opinions of another individual about the individual, and
- (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

FIPPA also includes a condition under section 38(1) that renders information not recorded but otherwise defined as “personal information” as still falling under this category. This could potentially make it easier to determine the provisions for disclosure applicable to that information as most data will fall under one common heading.

FIPPA also differs from FERPA in the language used regarding health or safety risks on campus. Section (b)(1)(I) of FERPA expressly states that an “emergency” situation can warrant a disclosure of a student’s education information. FIPPA uses the terms “compelling circumstances” and “grave hazard” to define situations where disclosure of personal information can be made without prior consent. These terms both require disclosure during pressing circumstances, yet FIPPA’s standard is clearly lower. This is significant. The strict construction of FERPA’s “emergency situation” standard was a point of contention for the Review Panel as discussed in the previous chapter. (Report of the Virginia Tech Review Panel 69) However, neither of the terms contained in FIPPA explicitly require an “emergency” to allow unauthorized disclosure, which may provide administrators with a greater interpretive scope when determining the nature of a difficult situation.

These sections in FIPPA are written in plain terms, with clear standards as to what circumstances would allow an unauthorized disclosure. Yet, the circumstances surrounding a difficult situation can make a clear interpretation of an otherwise straightforward legislation provision problematic. This is another obstacle to which Ontario universities should give some consideration. It is necessary to ask what a university actually considers to be a “compelling circumstance” or a “grave hazard”. These terms, or those similar to them, may already be defined within a university’s safety

policy, such as in Carleton University's case where they have defined a "hazard" within their *Hazard Reporting Policy*. However, in certain circumstances, it is only when faced with a difficult situation that these expressions can come to life. For this reason, knowing what a piece of legislation contains is vital, but so is developing institutional standards with which to apply that legislation and the language within it.

Apart from the language, the actual disclosure provisions of each piece of legislation differ substantially in quantity. FERPA contains only *one* section specifically geared to this issue, although this single section was still found to provide adequate allowances with regards to sharing Cho's personal information. FIPPA is much more extensive in its provisions with a total of *four* sections that directly address the sharing of information when dealing with a potential safety risk. As such, FIPPA provides more points of reference, direction and legislative support for universities when dealing with at-risk individuals.

The first section to address disclosures during a situation posing a health or safety risk is within the "Access to Records" portion of the legislation. Section 11(1) of FIPPA contains a broad provision on disclosure of this nature:

11(1) Despite any other provision of this Act, a head shall, as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard to the public.

This section is much more powerful than anything in FERPA as it requires a *mandatory* release of information when the health or safety of the public is at risk. A representative from the IPC during a conference in early 2008 also noted the importance of this section and the required element of disclosure. (O'Donoghue) According to the IPC, should

there be reasonable and probable grounds that a threat exists towards the public interest an institution's head is *obligated* to disclose information that could aid in managing this risk. (O'Donoghue)

Section 20(2)(b) of FIPPA under "Exemptions" provides additional support to the provisions in section 11(1), reinforcing the idea of considering the public interest when faced with personal information that could promote public health and safety if disclosed.

This section states that:

20(2) A head, in determining, whether a disclosure of personal information constitutes an unjustified invasion of personal privacy, shall consider all the relevant circumstances, including whether,

(b) access to the personal information may promote public health and safety;

Regarding the consideration of the public interest, FIPPA is quite unambiguous, stating that individual rights to privacy should never outweigh the health and safety of the public. A large portion of the exemptions against disclosure provided in FIPPA are balanced by section 23 which states when a "compelling public interest in the disclosure of the record clearly outweighs the purpose of the exemption" the exemption will not apply. The inclusion of sections like those outlined above illustrates that FIPPA was not created with the intent of trivializing the public interest when pitted against individual rights to privacy. Rather, these sections are intended to encourage an institution to negotiate both public and private interests when faced with a potentially dangerous situation.

The two remaining sections in FIPPA, along with those outlined above, that address the sharing of information specifically during compelling circumstances are almost identical in their scope and wording:

21(1) A head shall refuse to disclose personal information to any person other than the individual to whom the information relates except,

- (b) in compelling circumstances affecting the health or safety of an individual, if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

42(1) An institution shall not disclose personal information in its custody or under its control except,

- (h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

Sections 21(1)(b) and 42(1)(h) under “Exemptions” and “Use and Disclosure of Personal Information” respectively, have a more individual focus and do not mention an overall public interest within the text. However, they still have the capacity to be interpreted as such. An unauthorized disclosure under these sections, according to the IPC, is permitted provided that it is based upon a reasonable belief that the release would eliminate or significantly reduce the risk of serious harm to a person or group of persons. (O’Donoghue)

As a result of FIPPA, there are more provisions for an Ontario university to rely upon than a U.S. university relying on FERPA when faced with a difficult situation that may require unauthorized disclosure. Yet, despite how clear the provisions of FIPPA may be, there are still obstacles concerning legislative interaction and overlap that require some attention. While Cho did interact with health services and authorities other than those on campus, a significant function of this chapter is to highlight the wealth of internal information and warning signs Virginia Tech itself had at its immediate disposal which went largely overlooked due to confusion around legislative jurisdiction. Administrators at Virginia Tech faced a difficult situation due to their lack of knowledge

of FERPA, but this difficulty was compounded by a misunderstanding of how FERPA interacted and overlapped with other pieces of privacy legislation and other administrative and law enforcement bodies on campus.

The Review Panel concluded that there was ample information about Cho held by other administrative and authoritative bodies at Virginia Tech, that when taken together, should have raised substantial warning signals as to the safety risk Cho posed to those around him. (Report of the Virginia Tech Review Panel 53) There were several instances of note involving Cho and the Virginia Tech Police Department (VTPD), who act as the campus authorities for that institution. The VTPD had been called several times regarding Cho's behaviour, once for suicidal threats and twice for separate instances involving stalking female students. The Review Panel found that the records concerning the instances of stalking existed outside of FERPA and could therefore have been disclosed by the VTPD. (Report of the Virginia Tech Review Panel 66)

The records created by the VTPD about the stalking were for the purposes of law enforcement and investigating a potential crime; these are not covered by FERPA. However, the Review Panel also found that if the VTPD had shared the information with the university, the record that was shared would have become subject to FERPA and thus the release provisions provided within it. (Report of the Virginia Tech Review Panel 66) As it stood, only the second incident of stalking resulted in a larger group exchanging knowledge, yet this was still only limited to residence administrators and Judicial Affairs for Virginia Tech. (Report of the Virginia Tech Review Panel 45)

In Ontario, campus police units are currently governed by FIPPA as they are part of the overall institution. But, in some instances universities have safety officers with the

designation of “Peace Officer”, also known as a “Special Constable”. This provides the designated individual with a recognized law enforcement role. Law enforcement, under FIPPA, can invoke section 42(1)(g) which allows for the collection of any information relating to an investigation in a law enforcement proceeding or relating to an investigation that may lead to a proceeding. This could be perceived as helpful as campus police with special constable status will have wide access to any information regarding a situation they deem to be a law enforcement investigation. However, this could also be seen as problematic should relevant information be part of a *current* investigation.

Special constables due to their recognized law enforcement status may be limited in what they can share under section 14(1) of FIPPA depending on the nature of the incident, whether it is ongoing, and whether the urban police have become involved. This section does not prevent a campus officer from *acknowledging* an individual has had involvement with campus authorities, but it can limit what specific details are made available to a university concerning an at-risk individual. The head of an institution can withhold information for a number of reasons related to law enforcement, including whether the disclosure could be expected to interfere with an ongoing law enforcement matter. On the other hand, if a university lacks special constable status for its campus police, the use of collection under section 42(1)(g) of FIPPA may not be applicable which could indicate that disciplinary records held by campus security, unless part of a current investigation being carried out by police, may remain accessible to university administration depending on their own policies.

Taking the above factors into account, it is up to each Ontario university to understand not only their individual policies on safety and security involving information collection and disclosure, but also the status of their campus safety officers as this could affect their ability to share relevant details about an at-risk individual. Should the police become involved in an incident, their records are governed by the *Police Services Act* (PSA). The PSA, like FIPPA, does contain provisions allowing for the sharing of information should the public interest be at stake, but it is still in a university's best interest to familiarize itself with its internal privacy policies regarding records created and maintained by their campus police and the status of their authority.

Should a situation arise in which university administration would benefit from knowing whether a student has been involved with campus authorities and for what reasons, understanding what information they have access to internally can be an invaluable resource. This information can enable the appropriate individuals to evaluate the level of risk an individual might pose to themselves and others. Also, by understanding issues of overlap between university security policy and provincial legislation, it is possible to identify potential privacy concerns that may negatively impact the individual considered to be at-risk. In this manner, an administrative body can ensure they are not compromising the rights of the individual in question while remaining informed of pertinent information to the fullest extent allowed by their internal policies and the provincial legislation.

The VTPD along with residence staff and students from Cho's dorm, were well aware of his disturbing behaviour as discussed, yet there were many key groups left out of the knowledge loop as Virginia Tech administrators were unaware of how policy

overlap affected them. Cho's professors in the English department where he majored, were among those unaware of his dealings with the VTPD and the communications from Residence Life concerning his stalking and odd behaviour. (Report of the Virginia Tech Review Panel 52-53) This is an unfortunate lapse in communication as Cho's professors had a wealth of knowledge around Cho's behaviour, that when combined with the records from the VTPD and resident staff and students, paints a very disturbing picture.

Cho's professors had ample observations of disconcerting behaviour displayed in class including photographing students with his cell phone without consent, wearing dark sunglasses, wearing a baseball cap pulled low over his face and refusing to introduce himself or participate. (Report of the Virginia Tech Review Panel 41-50) While on its own this information may not raise serious warning flags, combined with Cho's disturbing behaviour outside of class and his record with campus police, a very different conclusion may be drawn. Yet university administrators did not connect the necessary points despite having access to all of the pertinent information.

Cho's professor's discussed the content of his submitted work with each other which was very violent and full of anger, to the point where many instructors were quite uncomfortable. (Report of the Virginia Tech Review Panel 40-42, 49-50) Some professors also expressed their reservations about Cho, both in the classroom and during one-on-one sessions, to upper levels of administration. (Report of the Virginia Tech Review Panel 41-45) Despite all this, Cho's professors were not aware of any alarming behaviour outside of class, and were only minimally aware of how other students felt about him. (Report of the Virginia Tech Review Panel 42-46) Lapses in structural communications also contributed to Virginia Tech's inability to act appropriately and

effectively. Should an Ontario university choose to implement a knowledge sharing framework, clarification on where certain pieces of information reside must also be part of the considerations given to this initiative. There can be no vital information to share if a university does not know where to find it.

The combined picture of Cho that can be determined from his run-ins with the VTPD, the discomfort expressed by residence staff and students, and the observations of his professors is not one of a mentally healthy university student. Yet, however unsettling Cho's behaviour may have been, one professor noted in her report about a meeting with Cho that only a professional had the ability to understand his conduct. (Report of the Virginia Tech Review Panel 45) Thus we see another piece of the information puzzle that was missing which should have been shared. Despite the multitude of observations made by various university administrators, none of them had qualified backgrounds in mental health. Those individuals who did possess the necessary knowledge to make informed judgements on Cho's condition lacked the opportunity to evaluate all the information pertaining to him. Confusion around the legislative jurisdiction between FERPA and another overlapping piece of privacy law contributed to more pieces of Cho's life falling through the cracks.

Along with FERPA, the U.S. also has several other pieces of privacy legislation that the Review Panel found contradicted each other in terms of information sharing practices. (Report of the Virginia Tech Review Panel 52) Of particular importance is legislation governing personal health information. The federal act in the U.S. known as the *Health Insurance Portability and Accountability Act* (HIPAA) has significant implications for overlap that Ontario universities will find some parallel with. When the

VTPD was called concerning Cho's suicidal threats, he was evaluated at the campus police department by a licensed clinical social worker. The social worker found Cho to be mentally ill and an immediate danger to himself and others, and that he was not willing to be treated voluntarily. (Report of the Virginia Tech Review Panel 47) At this point, Cho was transferred to an off-campus mental facility by the VTPD. The following day, Cho was released from St. Albans Behavioural Health Centre of the Carilion New River Valley Medical Center with ordered outpatient treatment as he was found to present an imminent danger to himself as a result of mental illness. (Report of the Virginia Tech Review Panel 48)

Virginia Tech's Cook Counseling Center had been made aware of Cho's need for outpatient treatment for which an appointment was made. (Report of the Virginia Tech Review Panel 48, 49, 59) Cho attended one follow up meeting with Cook and was triaged, not actually having received any treatment from Cook following his release from St. Albans. The policy of Cook was to allow patients to decide whether to schedule a follow up appointment, which Cho did not. Because Cook had received him as a voluntary patient, no notice was ever given to the university or those involved with his off-campus treatment that Cho had never returned to Cook for treatment. (Report of the Virginia Tech Review Panel 49) The details of these records from the VTPD and Cook were never shared with university administration. (Report of the Virginia Tech Review Panel 52)

Virginia Tech's Review Panel found that there was a lack of clarity around the classification of information on Cho as it appeared to fall under both HIPAA and FERPA, thereby complicating their already muddled understanding of the relevant

privacy law. (Report of the Virginia Tech Review Panel 66) Like many universities, Virginia Tech has its own health and counselling services available on campus. The Cook Counseling Center held records concerning Cho's mental health treatment, but these records are not governed by HIPAA despite their health related content. (Report of the Virginia Tech Review Panel 2, 52, 66) Upon further reading of both FERPA and HIPAA, the Review Panel found special provisions on how each piece of legislation functions when there is overlap between their jurisdictions. It was found that FERPA "has special interactions for medical and law enforcement records" and that HIPAA "makes an exception for all records covered by FERPA". (Report of the Virginia Tech Review Panel 66) What this ultimately means with respect to these laws is that any health records maintained by *campus* health clinics are not covered by HIPAA but rather FERPA, along with any valid state law restrictions. These records could have been shared within the provisions of FERPA. (Report of the Virginia Tech Review Panel 66)

Complications of this nature are not unfamiliar within the context of Ontario universities. Consideration of how FIPPA interacts with provincial privacy laws for health information in a university setting is an issue that requires some attention. The *Personal Health Information Protection Act* (PHIPA) functions in a similar capacity to the U.S.'s HIPAA, with comparable issues of overlap and interaction with Ontario's FIPPA. PHIPA applies to personal health information held by "health information custodians" (HICs) in Ontario. It is the determination of what constitutes a HIC that concerns universities. The relationship that a university has with any health services offered on campus could affect how information on an at-risk individual is categorized and shared.

The IPC understands a HIC to include a wide variety of health care practitioners and health care institutions, many of which can be found on university campuses. Doctors, nurses, pharmacists and psychologists for example all fall under the heading of a health care practitioner and therefore constitute a HIC, yet these individuals are also commonly found operating on university campuses all over Ontario. (Office of the Information and Privacy Commissioner/Ontario) There are currently twenty-one universities operating in Ontario according to the Ministry of Training, Colleges and Universities. Of these twenty-one institutions, all of them offer health and/or counselling services of some kind to their students, the vast majority of which are accredited professionals regulated under PHIPA by nature of their position and function. (Appendix A)

As it is possible for a HIC to exist alongside a non-HIC like a university, overlap between PHIPA and FIPPA institutions is expected. However, as stated earlier in this chapter, it is within the context of a university that understanding of this connection must be clarified. Determining the relationship between a university and any offered health and/or counselling services is vital to understanding how information may or may not be shared. When attempting to gain clarification on this point from the IPC it was found that the possibility of a university having a dual role as both HIC and FIPPA institution is very small due to the definition of a HIC provided in PHIPA. This definition addresses those institutions that *directly* offer services relating to health and counselling; a university is not an explicitly recognized institution under PHIPA. But, it was also noted by the IPC that the fiscal relationships arising out of salary dispensation may have some

effect on this. Clarifications as to whether health practitioners and counsellors are direct employees of a university may affect the status of the university itself.

Also, a university may find itself in the role of an “agent” to its campus HIC, or conversely, that a HIC is an agent of the university. (Office of the Information and Privacy Commissioner/Ontario) An agent is

a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent’s own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated. (Office of the Information and Privacy Commissioner/Ontario)

For example, a HIC’s agent may be a person who works for the university. A university’s health and counselling services may employ the services of an administrative assistant from the university to aid with their personal health information records management. (Office of the Information and Privacy Commissioner/Ontario) If a university determines that it is an “agent” of their campus HIC (or vice versa), personal health information that passes between these two bodies is considered to be a “use” under PHIPA and not a “disclosure”. Also, it is not considered to be a collection of information by the agent. This can aid in information sharing as “collection” generally requires some prior notice to the individual from whom the information is being collected, and “disclosure” has more specific circumstances regarding its allowance than “use”. Concerning “use”, section 37(1) of PHIPA states that,

37(1) A health information custodian may use personal health information about an individual,

- (a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent

of the individual or under clause 36(1)(b) and the individual expressly instructs otherwise;

- (d) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian;

The contents of section 37(1)(a) could be satisfied if a university's HIC has within its collection notice language addressing the use of an individual's information to ensure their overall health and safety and that of the university population as a whole. The mention of section 36(1)(b) addresses the provision for allowing indirect collection of information if the HIC cannot get reasonably accurate information from the individual themselves, or they cannot collect the information in a timely manner.

As for section 37(1)(d), the IPC does not currently define whether "risk management" in this context may also be interpreted to include health and/or safety risks to an individual or others, but this may be a point of clarification that could provide additional legitimation for any sharing that occurs between a HIC and its agent. With regards to improving or maintaining a quality of care under this section, if the sharing of information between a campus HIC and its university agent could potentially result in an at-risk individual receiving better options for treatment or counselling, then this section may also warrant some consideration for use.

Whatever the scenario, each individual university must ascertain what position its affiliation with a campus HIC might entail. Should a university find that its status is one that has it acting either as a HIC or an agent, there are additional provisions concerning public health and safety within PHIPA similar to those in FIPPA which would allow disclosure. Section 40(1) of PHIPA provides a clear blanket provision to this effect that

takes into consideration wider safety implications affecting someone other than the individual to whom the personal health information belongs:

40(1) A health information custodian may disclose personal health information about an individual if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

The IPC interprets this section to allow the institution to “override an individual’s prior express instructions not to disclose the personal health information” involved in the perceived risk. (O’Donoghue)

In addition to section 40(1), should a university find itself in the position that it is a completely separate entity from their campus HIC, section 49(6) of PHIPA addresses how sharing may occur within such a relationship structure. This section states,

49(6) Where this Act permits or requires a health information custodian to disclose personal health information to an institution within the meaning of the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* that is not a health information custodian, the institution may collect the information from the custodian.

A university, as a recognized FIPPA institution, is authorized through this section to collect information from a HIC where PHIPA permits. As PHIPA permits disclosure under 40(1) when addressing a potential danger to other persons, this section could be understood as providing further legal justification for collection by a university in connection with a reasonably perceived risk.

In hindsight, Virginia Tech found that there should have been more information sharing between its campus bodies with regard to Cho. Too many people with vital knowledge were left with fragmented viewpoints and/or an unrealistic understanding of the pending risk Cho posed. With this in mind, it is important for Ontario universities to

not only clarify their understanding of emergency disclosure provisions in FIPPA, but to also clarify their position with respect to personal health information as this information provides a solid foundation upon which to determine whether an individual is in fact at-risk. The involvement of regulated health professionals lends credibility to a university's assessment of an individual as being at-risk.

Health and counselling services, by their nature, have a more intimate knowledge of an individual's mental and physical status than what is contained within the records of a FIPPA institution. The importance of understanding how to access and interpret this information during an emergency or when a potential risk has been identified should not be ignored by FIPPA institutions. By ensuring clear paths of knowledge sharing between a university and its affiliated HIC, at-risk individuals may be identified faster and understood with greater clarity. As the Review Panel pointed out, it was an overall lack of sharing between academic, administrative, and public safety entities that contributed to the failure to see the big picture. (Report of the Virginia Tech Review Panel 52)

Overall, I suggest that FIPPA provides adequate provisions to consider when faced with a situation wherein a disclosure of personal information could benefit the health and safety of an individual or the public. Yet it is important to note that these provisions are intended to balance the protective aspects of FIPPA for individual privacy, not override them. A thorough consideration of the implications arising from disclosure versus confidentiality should be considered for each individual circumstance, as it is not only a simple knowledge of the legislative sections that will facilitate the operation of a strong, balanced knowledge sharing framework. Each university in Ontario must work to understand what situations will meet the standard of "grave hazard" and "compelling

circumstance”. This can prevent administrators from being placed in a position where they may overreact to a situation and compromise an individual’s right to privacy, or on the other hand, where they may underestimate a potential threat and risk harm to the student body. Universities must also clarify the status of campus authorities regarding disclosure and access, and they must determine their relationship with offered health and counselling services. These issues will have to be addressed with some expediency if Ontario’s universities wish to avoid the same widespread ignorance that contributed to the deadliest school shooting to have ever occurred.

Thus far this chapter has discussed the concept of disclosure and information sharing when dealing with at-risk individuals. It has been illustrated that universities in Ontario have legal provisions within FIPPA and other potentially relevant pieces of legislation to share information if necessary to protect the safety of an individual or the public. The question now remains: with whom should this information be shared?

Despite the major failures in communication that occurred at Virginia Tech, that university actually has an administrative team that is supposed to be the point of convergence for information within the university to review students with problems. (Report of the Virginia Tech Review Panel 52) Known as the Care Team, this committee is comprised of the dean of Student Affairs, the director of Residence Life, the head of Judicial Affairs, Student Health, and legal counsel. Other agencies from the university are occasionally asked to participate, including the Women’s Centre, fraternities and sororities, the Disability Centre, and campus police, although these agencies are not standing members of the Team. (Report of the Virginia Tech Review Panel 43)

Unfortunately, the Care Team was found to have been thoroughly “ineffective in connecting the dots or heeding the red flags that were so apparent with Cho.” (Report of the Virginia Tech Review Panel 52) Although having discussed at one point the disturbing and macabre writings of Cho, the totality of information presented in this chapter from the VTPD, his professors, residence administrators, and counsellors were never brought together in one sitting by the Care Team, thus reducing the significance of what they knew from Cho’s professors. This failure in necessary communication is never fully accounted for in the pages of the Report. There was a structural failure in communications that occurred between the various campus bodies along with a lack of legislative clarity.

Katherine Newman, in her study of school violence and the importance of information sharing, pointed out that despite the fact there was ample information available on the students who eventually carried out the school shootings she studied, “because no individual had the whole picture...no one recognized the depth or seriousness of their problems.” (Newman 109) This is the same distressing pattern that was seen at Virginia Tech. It is vital to ensure all knowledge pathways within a university are kept open and responsive to each other if the health and safety of individual students and the university community at large are to be upheld. In this respect, I propose that Ontario universities consider assembling something akin to Virginia Tech’s Care Team but ensure that they are equipped with a full knowledge of information sharing practices and where valuable pieces of information may lie.

The key element to keep in mind when establishing a team of this nature is to understand that the purpose should not only be towards risk management, but also

towards offering assistance and treatment, if possible, to an individual in need. With these functions in mind, David Garland's penal-welfare model mentioned in Chapter One offers significant structural guidelines that could prove to be beneficial to a university considering establishing such an initiative. The "Key Findings" portion of the Review Panel's chapter on information privacy laws acknowledges that "effective intervention often requires participation of parents or other relatives, school officials, medical and mental health professionals, court systems, and law enforcement." (Report of the Virginia Tech Review Panel 68) Garland's model offers an almost identical conceptualization of the importance of informal disciplinary and governance structures when addressing criminality, but also offers some insight into what the goals of a knowledge sharing team could potentially be.

Penal-welfare agencies depend on the "capacity of civil society to control individuals and channel their activities in law-abiding directions." (Garland 49) Civil society includes families, communities, schools, and other institutions that contribute to the norms and sanctions within society that the law attempts to uphold. (Garland 49) The formal bodies of discipline within society are not able to function effectively without intervention from civil society within this model. Although Cho was at an age where he would be considered a legal adult, the IPC recognizes that "students are not minors, but there may be a general duty of care [upon university administrators] where it is clear that a student is at risk, and may place others at risk."¹ (O'Donoghue) Presently, the parameters of this "duty of care" have not been specifically defined for Ontario

¹ The notion of a "duty of care" attaching to university administrators was raised by Mary O'Donoghue, General Counsel and Manager of Legal Services for the IPC, during the January 2008 conference for which she has been cited. As a "duty of care" is found within tort law, critical analysis as to the basis of this claim is needed, along with consideration of whether a model of fiduciary relations is more appropriate in this circumstance.

universities. However, determining who can and should be contacted when a student is at-risk of harming themselves or others may be part of this responsibility, as this duty was linked by the IPC to collection, use and disclosure of information to prevent harm. (O'Donoghue) When reviewing the series of events that occurred at Virginia Tech and how the Review Panel framed the non-disclosure of information to Cho's parents, this type of disclosure gains validity despite a student's adult status.

Throughout the entire ordeal at Virginia Tech, the university never investigated the relationship Cho had with his family or examined the possibility of whether involving them could have had a constructive effect on the troubled student. Cho's parents were never once notified as to their son's conduct from either the VTPD or professors, nor were they made aware of his received medical treatment. (Report of the Virginia Tech Review Panel 68) They were aware of the fact that their son had social difficulties and mental health issues, and had worked closely with his teachers during his youth to ensure Cho's progress and mental stability in school. (Report of the Virginia Tech Review Panel 31-35) Yet once he began university, Cho's parents were removed from his immediate circle of care.

Upon settling in at Virginia Tech, they communicated regularly with Cho over the phone, though he was never very talkative and did not share any of his anxieties or problems with his parents. (Report of the Virginia Tech Review Panel 40) As noted by the Review Panel, had they known of his ordeals, Cho's parents stated that they "would have taken him home and made him miss a semester to get this looked at", but they did not know anything was wrong and so could offer no input or options. (Report of the Virginia Tech Review Panel 68) The Review Panel looked upon this lack of information

sharing with his parents as detrimental to Cho despite his status as a legal adult. They found he had missed out on potential opportunities for intervention that could have come from his family's involvement had the university notified them of his medical and disciplinary problems. (Report of the Virginia Tech Review Panel 49)

The importance of the IPC's stance on the duty of care that may flow between university administration and an at-risk student becomes apparent here. A university has a vested interest in determining the proper course for collection, use, and disclosure of information if the possibility of harm to an individual or the public exists. As mentioned, this may include determining with whom appropriate disclosures can be made, which based upon the opinions of the Review Panel, could reasonably fall within the duty of care of a university. Family, guardians, spouses, and friends all make up aspects of civil society that may be able to offer support to a university when dealing with an at-risk individual. And, as stated by the IPC, sharing information with individuals of this nature can exist notwithstanding the fact that a student may legally be an adult.

Along with relying upon formal and informal structures, Garland also points out that penal-welfarism is marked by its interest with rehabilitation and a rather discretionary character towards correctionalist arrangements which allow decision-makers a fair amount of latitude when determining the treatment of an offender. (Garland 49) Under penal-welfarism, individuals who offend but lack any real "criminal disposition" are seen as "normal" and are generally handled with cautions, fines, or deterrent penalties if the seriousness of the crime warrants it. It is those who display a "pathological" criminality that warrant rehabilitative attention. (Garland 42) There are criticisms of this aspect of the penal-welfare model, such as the lack of correctional

attention paid to “normal” individuals who display no pathological intent in their offences and the uselessness of deterrent punishments void of punitive intent. (Garland 42) However, within the ideal of this structure the understandings of a sound information sharing framework may be found. Although the penal-welfare structure is understood by Garland within the context of offenders and crime control, I would like to extend this concept to at-risk individuals in a university setting.

Understanding the mind of an at-risk individual is imperative in determining how to address their situation and the risks they pose to themselves and others. The determination of whether an individual is psychologically healthy is quite important as this should dictate how a university proceeds to deal with an issue. Is some kind of medical intervention needed, or is the individual in question simply a disciplinary problem? Here, the importance of involving individuals who have the credentials to make these kinds of assessments is apparent. Virginia Tech did include a representative from Student Health in their Care Team, but the Review Panel did not state whether this individual was equipped with the knowledge to make mental health assessments. When attempting to determine whether a student is at-risk, an accredited health care practitioner can aid in establishing a justified need for disclosure and intervention, as university administrators (unless trained in mental health) do not possess the credentials to do so. Additionally, the VTPD was not always present in the meetings carried out by the Care Team, which deprived the group of pertinent information concerning disciplinary action involving Cho.

Depending on what a university sharing network may discover they can decide on how to proceed, who to involve, and what discipline or aid is necessary, keeping with the

discretionary nature of penal-welfarism. In Cho's case, the involvement of his family could have made all the difference to his situation. In this respect, this is where the knowledge sharing framework becomes essential. Virginia Tech's Care Team, had they known they could share what they knew, were still missing vital pieces of information from the VTPD and Cook. In order to gain as full an understanding as possible of an at-risk individual, universities must ensure they have all relevant information at their disposal. The penal-welfare model depends on understanding the elements of causation and circumstance in order to provide treatment. As such, a university cannot hope to help an at-risk individual if they do not have access to the all information available and they lack a functional communication structure into which the information can flow. This requires an intimate understanding of where relevant information is located, who holds it, and how administration can access and share it, if necessary. These issues along with the caveats associated with implementing such a structure will be discussed in the final chapter.

CHAPTER IV Structure and Balance: The Knowledge Sharing Framework and its Risks

To reiterate the overall intention of this thesis, balance must be maintained between individual privacy rights and public interest. The previous chapter has illustrated the provisions within the *Freedom of Information and Protection of Privacy Act* (FIPPA), as well as those within the *Personal Health Information Protection Act* (PHIPA), that demonstrate the validity of a claim for public interest when dealing with the personal information of a potentially dangerous individual. However, as reiterated many times, these sections are *not* intended to override the rights of any one individual. Safeguards that should be implemented in order to maintain this balance will be addressed in this final chapter along with a proposed hypothetical structure of implementation for a knowledge sharing framework. Included in this discussion are suggestions and insights into how Ontario universities could structure the direction of information flow within a knowledge sharing framework, how information is to be collected, how the personal details of an at-risk individual can remain protected under FIPPA and, overall, how to negotiate between the interests of the individual and the public.

IV.I Structure: Conceptualizing a Knowledge Sharing Framework

It is possible to gain a basic understanding of where personal information may reside within a university by reviewing the institution's directory of records and personal information banks. As per FIPPA under section 45, each university must publish an index of all personal information banks (PIBs) including details on which individuals are included in each bank (i.e. students, staff or faculty), what type of information is kept, and where the information is located, among other things. This is a quick and easy way

to determine where important information such as health and medical records, opinions and views concerning an individual and disciplinary files, both academic and otherwise, are kept. By determining this, a university can start to build a team of administrative representatives to take part in a knowledge sharing initiative that is able to consider both the potentially fragile state of an at-risk individual and the safety interests of the campus population. This group can work to ensure that individual ripples of trouble among a large student body do not get overlooked and help for an at-risk student can be offered where needed. As the IPC stated, a university has a duty of care towards not only the student body, but also towards the well-being of the troubled individual.

Where Ontario universities may want to differ from Virginia Tech is regarding the occasional participation of various groups on campus. It is because of this sporadic involvement that important information from the Virginia Tech Police Department (VTPD) was left out of the picture. As the Review Panel noted when evaluating the Care Team, “key agencies that should be regular members of such a team are instead second tier, non-permanent members.” (Report of the Virginia Tech Review Panel 52) Each university must endeavour to discover which units and administrative bodies on campus should participate in a knowledge sharing initiative, but they should also seriously consider how occasional rather than permanent involvement of certain campus groups could limit their overall observations. It was both a lack of structural clarity and privacy law knowledge that affected Virginia Tech’s ability to act effectively. Consideration also needs to be given as to who the supreme authoritative decision maker should be within an information sharing initiative, or if the decisions of such a committee are to be

democratic in nature depending on a majority decision to pursue potential courses of action.

As a hypothetical example, I have composed a rudimentary skeleton of a knowledge sharing framework based upon Carleton University's current administrative structure. This example is intended to illustrate how such a framework could be constructed and to offer suggestions for potential mandates for the group to follow. Carleton, like many universities, has multiple offices and departments which hold student personal information. These varying points of contact between the university and the student result in pieces and details of individual lives being spread across a wide variety of locations. At Carleton, by consulting the institution's PIBs, it is possible to isolate those information banks containing details that would be helpful when attempting to evaluate a potentially at-risk student. For example, some offices and departments at Carleton that could be included in a knowledge sharing framework are: University Safety, Patrol Services, Housing Services, Residence Life Services, Health and Counselling Services, Telecounselling Centre, Equity Services, Learning Support Services, the Paul Menton Centre for Students with Disabilities and the University Secretariat.

These offices and departments contain the personal information of students relating to one or more of the following: behaviour, discipline (academic and otherwise), psychological and emotional status, medical information, special accommodations, personal opinions, etc. By involving them in a single committee, these varying offices and departments have the ability to allow their separate fields of knowledge on student personal information to converge in one area. Additionally, the offices, departments and

individuals not part of the permanent structure of the knowledge sharing framework must be made aware of their ability to bring any concerns and pertinent information they have about a student to the existing group for consideration and evaluation. This will help to encourage others, like professors, to contribute viewpoints and information that may otherwise be overlooked until the last minute as in the case of Cho. An information sharing network should operate, overall, as a central hub into which all existing information on students can converge.

Once this structure has been established it is vital to determine specific goals and purposes as well as a final decision-making process. Priorities that a knowledge sharing framework at Carleton could consider include:

- a) seeking advice from the IPC on operating strategies before engaging in knowledge sharing committee activity;
- b) gaining clarification from the IPC on FIPPA and PHIPA interaction when dealing with Health and Counselling Services (the health professionals at Carleton may only be able to act in an advisory capacity if sharing between the FIPPA regulated bodies and PHIPA regulated bodies of the university is prohibited);
- c) ensuring that all notices of collection at the point of student registration include a section on protecting the health and safety of individual students and the student population as a whole so all new registrants are aware that confidential disclosures of some personal information to the knowledge sharing committee for the purposes of addressing potential risks within the student population may be necessary at times;
- d) developing some standards as to what the knowledge sharing committee would consider to be an “at-risk” individual;
- e) ensuring that clearly identified at-risk individuals receive appropriate aid should they pose a potential danger to themselves;
- f) ensuring that the greater student population is protected from at-risk individuals who pose a potential danger to others;

- g) investigating whether the involvement of a third party (i.e. family, spouse, guardian, etc.) would benefit an at-risk individual and, if so, facilitating communication with that third party should they be found to offer a beneficial support system;
- h) facilitating clear communication between the various student administration bodies on campus who are members of the knowledge sharing committee;
- i) facilitating a forum in which those individuals who deal directly with students but who are not part of the knowledge sharing committee can offer information that may help the committee in clearly identifying at-risk individuals. This can include professors, teaching assistants, faculty advisors, etc.
- j) consider implementing an appeal process for those students who have been identified as “at-risk” so they may come before the committee to discuss their situation if they are reasonably able to do so on their own behalf.

These basic directives can form the initial beginnings of a knowledge sharing framework upon which more substantial procedural policy can be built. With regard to the ultimate decision-making power of a knowledge sharing committee, at Carleton this could rest with the University Secretary. The individual holding this position also jointly holds the title of FIPPA Coordinator for the entire university and as such is the authority on FIPPA and related issues at Carleton. Additionally, the Secretary at Carleton possesses some decision making power within other offices of university government, management and control including Equity Services and the Board of Governors. (Office of the University Secretariat) Although this example is specific in scope as it relates to Carleton, the general ideas expressed can be adapted to suit the administrative structure of another Ontario university.

Apart from developing sound knowledge of privacy legislation and establishing various communications guidelines, thought must be given as to how this structure can

operate while maintaining the necessary balance needed between individual privacy rights and the public interest. The importance of maintaining privacy standards that do not intrude upon or alienate the student population is vital to this structure if it is to operate effectively and equitably. The following section of this chapter will seek to address some of the concerns associated with institutional monitoring and information collecting, the purpose of which is to highlight how a constructive concept can transform into a destructive force if not diligently monitored and regulated. Specific points that will be addressed include the concept of function creep, the use of health information in assessing a student's mental health and the involvement of regulated health care professionals in these assessments. Health care professionals are deeply influential individuals during the decision making process when addressing at-risk students and as such should be regarded with care. I will also offer suggestions on how institutions can avoid falling into negative trends when attempting to operate an information sharing network.

IV.II Balance: Reconciling The Two Faces of Surveillance

Virginia Tech has prompted a rethinking of the function of privacy and the responsibility of universities in sharing valuable information on at-risk individuals. This rethinking has arguably followed a limited and partially misguided path due to the surrounding moral panic and lack of privacy policy knowledge the university possessed prior to the tragedy. This context, as I have illustrated, contributed to policy interpretations that upset the existing balance between public interest and individual privacy rights within the U.S.'s *Family Educational Rights and Privacy Act* (FERPA). Rather than maintaining an equal consideration of both perspectives, the public interest

has been given more priority in the wake of Virginia Tech by the media, the public and most notably, the Review Panel charged with providing evaluations of and recommendations for federal privacy legislation.

This trend of diminishing individual privacy in the wake of a horrific event is not a new occurrence by any means. Following 9/11, amidst moral panic and knee-jerk policy reactions, “on a simple calculus, citizens accept[ed] that a loss of privacy [was] the price to be paid for security – as the mass media have reiterated ad nauseum since 9/11”. (Lyon 35) As illustrated in Chapter Two, a similar mindset stemming from public acceptance has been adopted since the Virginia Tech massacre in the U.S., along with the media’s lambasting of individual privacy rights. Despite the erroneous nature of blaming a misunderstood piece of legislation for the shooting, individual privacy rights remain under harsh scrutiny. The recommendations of the Panel reflect a sentiment that would exchange individual privacy rights for a greater sense of perceived security and transparency. Ontario universities must endeavour to move away from attempting to justify the erosion of individual privacy rights in the interest of public safety and security. It is an unnecessary sacrifice. Citizens do not and should not have to forfeit their right to privacy despite alarmist attitudes that claim confidentiality allows dangerous individuals to operate unchecked.

Privacy is a value that we all expect to enjoy as part of a democratic society. Despite Amitai Etzioni’s claims that this association of privacy with notions of democratic freedom is relatively new, the fact of the matter is, this is how we understand our privacy. (Etzioni 83, Sypnowich 96) Should an institution seek to intrude upon our private domain then they do so at the risk of threatening or diminishing our identities as

autonomous individuals. An information sharing network must be cautious in its attempts to engage in the more private domain of student health and wellbeing. Attempting to inject some ability to intervene in this area of an individual's life begins to impede upon a student's control over what they choose to reserve and what they disclose. As Alan Westin notes, "a free society leaves this choice to the individual, for this is the core of the 'right of individual privacy' – the right of the individual to decide for [themselves]...when and on what terms [their] acts should be revealed to the general public." (42) Universities must be aware of the fine line they will walk between a duty of care and the possibility of intrusion when operating an information sharing initiative.

The importance of privacy has also been associated with the power of maintaining control over who has access to us and in what capacity as part of our social relationships.

James Rachels illustrates this concept with the following example:

If someone is our doctor, then it literally is his [or her] business to keep track of our health; if someone is our employer, then it literally is his [or her] business to know what salary we are paid; our financial dealings literally are the business of the people who extend us credit; and so on. In general, a fact about ourselves is someone's business if there is a specific social relationship between us which entitles them to know. We are often free to choose whether or not to enter into such relationships, and those who want to maintain as much privacy as possible will enter them only reluctantly. (331)

Rachels believes that a facet of privacy and why we value it is tied to our ability to regulate what part of our identities we reveal to the public and to other people. "A domain of privacy is a constituent of freedom, a condition for different kinds of social relationships." (Synnowich 97) When attending university, students can expect that their educational career will be the business of the institutions which they are attending. However, with the implementation of a knowledge sharing framework, individual well-

being also becomes a specific area of interest for the university. As a result, the existence of a knowledge sharing group will change the nature of the relationship between the university and its students. If implemented incorrectly, this initiative could damage the relationship between the student and their university, as well as impede upon their general freedoms.

As illustrated in the previous chapter, the *Freedom of Information and Protection of Privacy Act* (FIPPA) allows for the exchange of personal information within an institution under certain pressing circumstances. This sharing can be done without threatening the stability of individual privacy rights, the autonomy of the individual and an individual's ability to direct their social relationships. An information sharing network based upon proper interpretations and understandings of FIPPA is a feasible goal, and one that will not erode these precepts if executed appropriately. However, despite the positive intentions behind the proposed structure, there are caveats associated with institutional monitoring and information collecting. I have proposed that universities engage in this behaviour primarily in order to identify and offer aid when possible to at-risk students, yet the potential for abuse and misuse when implementing such an initiative must be examined in order to identify the negative implications for individual privacy.

A large concern at the forefront of many well-intended initiatives is the concept of "function creep". This term applies to situations when something is used for purposes that were not intended within its original scope. (Monahan 378) This shift can occur with technology, legislation, policy – wherever the possibility exists for the reappropriation of a purpose or role, a risk of function creep can be found. Although

function creep is not necessarily always a negative thing, in certain situations it can produce damaging results. Surveillance for example, as a tool of neoliberal governance, illustrates how unintended consequences affecting the stability of democratic rights can arise from routine practices. (Haggerty and Ericson 6)

Methods of state and institutional surveillance are a focal point when discussing the negative potential of function creep, as this is a primary point at which individual privacy and a perceived public interest can clash. There are many examples of institutional programs implemented with the intent of helping or protecting the public, but under the flag of public interest end up becoming ulterior tools for surveillance, control and coercion. Take London's "Oyster Card" introduced in 2003 for example. This pre-paid, plastic swipe card is used when taking public transit in the UK to make it quicker and easier to get through pay points on the transit lines. Yet, this unassuming little travel card is actually also a "smart card", containing a small computer chip which collects and stores information about the user, including their name and the location and time of each instance of use. (Scullion)

In a news article from 2006, Charles Monheim, a representative from Transport for London (TFL) which provides the Oyster Card, told BBC London that the card allows TFL to "collect journey data so we can provide customer service and answer customer queries." ("Oyster data...") However, the travel information collected through the Oyster Cards by TFL is also provided to police, essentially allowing them to access information said to have been collected for "customer service" reasons. ("Oyster data...") The police claim the card is just an "investigative tool" used to help combat crime, which is of course, in the public interest. Several privacy advocates in the UK are concerned about

this episode of function creep and the implications it has for state surveillance of the public and the privacy rights of the individual. The collection of travel data generated by the public was not originally intended to support police investigations, and those purchasing the card were not aware that their personal information would be handed over to the police without their consent. (Scullion)

Another example displaying the negative potential of function creep can be found within the walls of many U.S. companies. Several American businesses have established “wellness centres” for employee use, intended to keep workers healthy by offering services such as exercise programs, on-site medical personnel, and counselling centres. (Staples 2000 118) These wellness centres have aided in cutting annual employee sick leave and overall medical costs for participating companies, but they have also “crept” into the realm of serving an ulterior purpose. The centres collect a wealth of health and medical information on employees through the services offered and accessed by personnel – unfortunately, this knowledge is not always used to support the wellbeing of the individual seeking help.

There have been several examples of employees filing for medical coverage with their employers only to find that the confidential health information collected through these “wellness programs” had actually been provided to management and used to deny the individual benefits. In one instance involving a large U.S. company, a widow filed for survivor’s benefits with her husband’s employer after he died. He passed away just two weeks after being demoted from a desk job to manual labour, prompting the widow to believe she had a strong case. (Staples 2000 119) However, the company knew from medical records gained through employee health care services, that the woman’s husband

had smoked a pack and a half of cigarettes a day since he was fourteen. This persuaded the administrative trial law judge hearing the case to deny the widow benefits. (Staples 2000 119) The company did not even have to hire a lawyer to defend their stance, relying only on the strength of the medical records they gained through their employee assistance program.

The type of function creep illustrated in these two examples is a dangerous path for any socially based information-sharing initiative to take. When redirecting a once public oriented service into a risk management scheme, the priorities around individual privacy rights can begin to fade. This is especially important to note in a university context as there are dangers to both individual privacy *and* the public interest if the suggested information sharing initiative suffers from function creep driven by a risk management perspective. The whole purpose behind an information sharing network should be to identify at-risk individuals so they can be directed towards appropriate avenues of care, not in order to cull them from the larger population as part of a risk management plan. If at-risk students are being identified and aided appropriately, potential risks of harm to them and to the student body can be reduced as a result of offering beneficial intervention. The reduction of risk and enhancement of campus security is a reasonably expected by-product of a care based approach.

On the other hand, if a university seeks to place institutional security as the primary goal of an information sharing network, then care and privacy for those at-risk will not be at the forefront of any action taken. Monitoring of possible at-risk students will “creep” into the function of being a mere tool for control and coercion, not one of care and positive intervention. Individual consideration is not part of what Nikolas Rose

calls “risk thinking”. Risk thinking “is concerned with bringing possible future undesired events into calculations in the present, making their avoidance the central object of decision-making processes, and administering individuals, institutions, expertise and resources in the services of that ambition.” (Rose 332) Risk thinking has the potential to warp the form and purpose of a care based information sharing group, into an aggressive, intrusive surveillance tool.

Malcolm Feeley and Jonathon Simon (1992), like Rose, have also witnessed that a risk approach is “concerned with techniques to identify, classify, and manage groupings sorted by dangerousness. The task is managerial not transformative...It seeks to *regulate* levels of deviance, not intervene or respond to individual deviant or social malformations.” (452) There is no intent to actually help those who are at risk, nor is there any incentive to consider their privacy rights should those rights clash with the managerial task of controlling dangerousness. Any information sharing initiative that is primarily driven by risk thinking will simply degrade, or “creep”, into institutional monitoring of the public and targeted individuals, quashing privacy rights for the sake of regulating behaviour and removing individual threats. The balance between public interest and privacy rights will be swept aside, and even the public interest will suffer.

As mentioned earlier in this chapter, the autonomy of an individual to choose when and how their actions are revealed is part of privacy and freedom. However, when Westin made this point, he also tempered that freedom with the limitation that it could be set aside “with only extraordinary exceptions in the interests of society”. (42) An information sharing initiative is already impeding somewhat on an individual’s ability to choose when and how their actions are revealed despite whether a public (or individual)

interest can justify this intrusion. To carry out information sharing within the context of risk management posing as public interest is inviting public discontent and the erosion of personal privacy rights, as seen with the Oyster Card and employee benefits examples. William Staples discusses the negative effects of risk management conducted through institutional monitoring in great detail. He describes the small actions involved in government and private based social surveillance as ways to “keep us in line, monitor our performance, gather knowledge or evidence about us, assess deviations, and if necessary, exact penalties”. (2000, 2)

Chapter One briefly presented Staples’ discussion on the drawbacks and pitfalls of public surveillance. He examines this issue with a highly critical eye towards the institutions carrying out such actions. Within his work, Staples has evaluated the landscape of surveillance with regard to several issues, one being health and safety threats and the shape risk management takes when dealing with these issues. His arguments and insights can be paralleled to the issues raised during Virginia Tech surrounding the framing of Cho’s mental health and his right to privacy. These issues are highly relevant when attempting to identify possible areas of function creep and the emergence of risk thinking when implementing a knowledge sharing framework.

When evaluating institutional surveillance of an individual’s health, Staples understands the body as “a contested terrain in the battle over questions of individual and organizational demands, be they schools, hospitals, workplaces, or public health departments.” (Staples 2000 108) The ill-health of one’s body or mind can become a question of how it may threaten institutional security rather than a question of how best to provide individual care. Because an individual’s health can be used as a control

mechanism when operating under risk thinking, those who are able to draw assumptions and conclusions from one's medical history become powerful figures in the decision making process. This resonates within a university environment as there is potential in this area for function creep driven by risk thinking to occur. I stressed in the previous chapter the importance of involving individuals from accredited health and counselling services as an imperative component to any information sharing initiative. This was suggested on the basis that a professional in this area would be able to offer valuable insight and options for care when evaluating an at-risk student due to their specialized knowledge. However, the inclusion of health care practitioners also lends itself to the potential for risk thinking and the ability to transform a care based approach into a device for grouping and controlling elements of risk.

Drawing upon the work of Dorothy Nelkin and Laurence Tancredi (1994), Staples highlights the social implications of profiling individuals based on their health and the power that health care practitioners can have when driven by risk management incentives:

Institutions must operate efficiently, controlling their ... students ... in order to maintain economic viability ... Sanctioned by scientific authority and implemented by medical professionals, biological tests are an effective means of such manipulation, for they imply that institutional decisions are implemented for the good of the individual. They are therefore a powerful tool in defining and shaping individual choices in ways that conform to institutional values. (Nelkin and Tancredi 160-161)

In this fashion, medical professionals can take on a powerful role in decision-making when backed by the rational force of science and the calculating terms of risk management. However, the participation of these members should not equate to a justified mechanism of control over those students who require intervention or aid. This

is “creeping” dangerously close to the realm of risk thinking, which encourages data-mining for harmful elements in an institution, and the use of information for control purposes rather than care ones. As discussed in Chapter Two, Cho’s privacy, mental health and the records documenting his issues were placed in conflict with the security needs of the public. Cho’s destructive mental state and the information pertaining to his issues were framed by the media and the Review Panel at many points as data that should have been available to administration in order to ensure the safety of the university. By adopting and standing by a care based approach, insights from health care practitioners can avoid being distorted into tools for risk management.

This potential for conflicting interests can be seen when addressing the safety of any campus population and the rights of an individual. Universities have a duty to ensure the security of their institution, which may result in the interests of the organization clashing with an individual’s privacy if their current state of mental health is one that could potentially result in the harm of themselves or others. For Ontario universities, there is no guarantee that an information sharing initiative will avoid edging into the realm of institutional monitoring and risk thinking, but there are protections and standards that can be put in place to discourage function creep of this nature. University administrators must be willing to understand and clarify the provisions of FIPPA that allow the sharing of vital information, as confusion or lack of knowledge in this area can contribute to negative interpretations of the legislation. As illustrated, these negative interpretations can lead to privacy laws being wrongly applied and subsequently blamed for obstructing safety. When this occurs there is a propensity for function creep driven by risk thinking to ensue. Should risk thinking take over, surveillance and control will

become the primary function of any information sharing network. This conflicts directly with a balanced approach to privacy and with the balanced framework of the penal-welfare model proposed.

Along with seeking understanding and clarification on FIPPA, universities must also be willing to balance knowledge of the legislation with reasonable limitations on their powers of surveillance. To relate back to Rachels' discussion of controlling our social relationships, if universities adopt an approach that openly and forcefully seeks to manipulate how students interact with the institution, they risk jeopardizing individual privacy and the stability of existing relationships with its students. "Unless...citizens can trust others with their personal details...governmental efficiency, economic prosperity, and the renewal of democratic practices and institutions will suffer." (Bennett and Raab 51) Universities cannot aggressively survey the student population or they will become a spectre of control to be resisted. This is especially important to keep in mind as universities have a dual role for many students as a learning institution and a home.

If students are subjected to arbitrary and intrusive forms of surveillance, they may feel as though they are under attack and pull away from established support systems such as health and counselling services. Students living on campus are already subjecting themselves to a measure of surveillance as it is the role of residence officials to supervise student conduct and ensure the rules and regulations of the university are being adhered to. At Carleton University for example, students are required to sign a contract upon being approved to live in residence. This "Residence Contract" includes a stipulation that students will abide by the directions of residence staff who are there to monitor student

behaviour and intervene if any established rules are violated. (Carleton University Residence Contract)

By imposing an added element of surveillance to these existing mechanisms of behavioural scrutiny, the trust level of students in their university may dwindle significantly. When there is distrust among a population concerning surveillance, resistance can emerge in the form of “smaller, often unorganized actions that individuals use in their struggles with emergent systems of observation, management and control.” (Gilliom 113) This can include such actions as misrepresentation and avoidance. (Gilliom 113) Actions such as this are not helpful to those students who could benefit from intervention as their problems may get driven underground rather than brought forward for help.

In order to avoid “creeping” into risk thinking and the development of aggressive surveillance, Ontario universities can consider certain limitations. The first is to control how information is collected. A knowledge sharing framework should not be an augmentation or extension of existing information collecting bodies on campuses, but rather an opportunity to better utilise *existing* pieces of data. Cho’s residence advisors, professors, the Virginia Tech Campus Police and the Cook Counseling Center all had information pertaining to his fragile mental health. (Report of the Virginia Tech Review Panel 49-52) There was no need to carry out additional surveillance. There was only a need to clarify the provisions for sharing under FERPA and to better utilise Virginia Tech’s Care Team set up to compile vital pieces of information on at-risk individuals.

As stated earlier in this chapter, an information sharing group set up by an Ontario university should operate as a central hub where valuable pieces of information can

converge, at which point further knowledge gathering can be considered if necessary and justified. The ability to build a “big picture” is what Katherine Newman states is the key to identifying at-risk students early on and facilitating positive intervention. (109) That being said, an appropriate limitation to be placed on an information sharing group is one that would see at-risk individuals identified only through information that is *brought* to the group by another recognized university member. Residence advisors, counsellors, or professors for example would be able to provide first-hand accounts of alarming behaviour and act as contact points for students who may have concerns about other fellow students. At-risk individuals should not be sought out by actively and arbitrarily surveying the student population or institutional records – this would be a direct attack on individual privacy. The coordination of student information should only occur after the information sharing group has been alerted to a potentially harmful situation. By avoiding immediate surveillance, a university can reduce the possibility of “creeping” into risk management territory and avoid coming across as “Big Brother”. A reactive sharing group as opposed to a proactive one when identifying at-risk individuals would be more beneficial for this type of structure.

A second limitation that Ontario universities can consider when implementing a knowledge sharing framework is to control the flow of information. The knowledge sharing group should ensure that the information they receive and any findings or decisions they make remain strictly confidential and only accessible by those members of the group for the purposes of aiding an at-risk student. Information should flow into the group, not out of it unless it is deemed necessary that an external party be notified in the best interest of the at-risk individual. The principles behind the penal-welfare model can

help to guide when an outside party should be notified about an individual that may harm themselves or others. As Garland posits, one of the key aspects of this model is the inclusion of various members from civil society to aid in the process of discipline and intervention. (49) Family was one element of Garland's model that can play a role in this structure.

As mentioned in the previous chapter, although a student may be an adult, if there are signs of concern for their health and safety and that of others around them, a university has a duty of care to that student. (O'Donoghue) I put forth that this duty of care may involve contacting a family member or close relative if it is believed to be in the best interest of the individual. There is an additional consideration within FIPPA along with the four discussed in Chapter Three that allows for a disclosure of personal information without consent that could prove beneficial when determining how to best aid an at-risk individual. Disclosure for "compassionate circumstances" is available under FIPPA, unlike FERPA which contains nothing to this effect. The closest equivalent in FERPA is section (h) which allows an educational institution to notify a parent if their child had been disciplined for conduct that posed a significant risk to themselves or others. Section 42(1)(i) of FIPPA however offers this option:

42(1) An institution shall not disclose personal information in its custody or under its control except,

- (i) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased;

This section permits a disclosure of personal information by a university to someone close to the at-risk individual. The *Personal Health Information Protection Act* (PHIPA)

also provides for a release of information for “providing health care” under section 38(1)(c),

38 (1) A health information custodian may disclose personal health information about an individual,

(c) for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual, if the individual is injured, incapacitated or ill and unable to give consent personally.

To look again at Cho’s situation, there was little to no involvement of his family during the period up to his death. Despite disciplinary action taken against him and psychiatric treatment, his parents had not been notified and, most importantly, there was no attempt to determine whether this would be beneficial to him. When looking at Garland’s penal-welfare model, this failure to share information with those who are part of an individual’s accepted informal disciplinary structure was a poor decision. Rachels’ understanding of the boundaries of social relationships also holds significance, as a parent, relative or loved one can, in many situations, be expected and accepted within the circle of knowledge concerning the well-being of those they are close to. When operating a knowledge sharing framework from a care perspective rather than one of risk thinking, these options need to be included in the consideration of how best to aid an at-risk student. On that same note however, caution should always be taken when determining whether to disclose the health information of a student without their consent even if it is to a family member or close relative. Function creep by universities into the realm of information misuse must be diligently controlled for.

A factor that also concerns information flow is outside access by way of request. It is possible under section 24(1) of FIPPA for an individual to request access to an institution’s records (including those of committees) which could affect the singularly

inward flow of information into a knowledge sharing framework. However, there are exemptions available should an information sharing group ever be faced with such an issue. Section 20 allows an institution to “refuse to disclose a record where the disclosure could reasonably be expected to seriously threaten the safety or health of an individual.” Mental illness is still a highly stigmatized issue in our society, and any students who are labelled as “at-risk” may attract this same stigma from the public. (Greenspon)

At-risk students must be protected from becoming targets for abuse or being ostracized by the rest of the campus community. It is imperative that an information sharing group works to ensure the privacy and confidentiality of those they are discussing so as not to exacerbate any existing difficulties or conditions an at-risk student may be facing. Additionally, section 21(1) of FIPPA disallows the release of personal information to “any person other than the individual to whom the information relates”. Both of these exemptions can protect the information of an at-risk individual collected by a knowledge sharing group should an outside party seek to obtain information through an access request.

Any lapses in attentiveness on this issue will result in a direct infringement of privacy and freedom, as control over what is revealed to the public will be completely removed from the power of the individual which Westin holds as an imperative aspect of a free and democratic society. (42) Along with the structural suggestions made in the first section of this chapter as part of a hypothetical information sharing network, these additional considerations could be added to the priorities of an information sharing committee in order to address these issues:

- a) ensuring that all discussions and information compiled by the knowledge sharing committee remains strictly confidential to protect

the rights, safety and best interests of those potentially at-risk and those found to be at-risk;

- b) to refrain from sharing its findings or collaborating data with any individuals outside of the knowledge sharing committee unless necessary to the health and safety of the student and despite whether that outside individual has provided information to the committee;
- c) only compiling information from what is readily available and/or provided concerning an at-risk individual and refraining from carrying out intrusive and aggressive collection of information on at-risk individuals.

It is vital that universities remain aware of the possibility and potential for a reappropriation of purpose and scope if they choose to create an information sharing initiative. These limitations and cautions as to how information is collected and used can help Ontario universities regulate themselves and control for a shift into a purely risk thinking model. In Cho's situation, his individual care became a distant concern relative to the risk management of the institution. Cho himself was ultimately blamed for the tragedy, notwithstanding his mental instabilities and the institutional failures in his care. (Report of the Virginia Tech Review Panel 53) As the Review Panel stated "While Cho's emotional and psychological disabilities undoubtedly clouded his ability to evaluate his own situation, he, ultimately, is the primary person responsible for April 16, 2007; to imply otherwise would be wrong." One can speculate as to whether intervention would have ever helped Cho in the final analysis, but placing the lack of care he received solely upon his shoulders when the university failed to make proper use of their own student care resources illustrates that the priorities on this issue may have been distorted.

IV.III Negotiating the Balance: The Final Weigh-In

Much of this thesis has been dedicated to addressing the issue of whether Ontario universities can share information on at-risk individuals and how they can go about doing

so within the law. This chapter has attempted to balance that ability to share by addressing when and how it should be done in order to maintain an equal consideration of individual privacy rights along with the public interest. Ontario universities have the benefit of a thorough and comprehensive piece of legislation to guide their ability to share information during pressing circumstances. However, they also possess a duty to uphold and protect the privacy of those individuals who are at-risk and whose information may be shared. “Individuals are often unable to understand that their personal details are being collected and processed every day in a wide variety of mundane activities, much less being able to control the situation.” (Bennett and Raab 76)

Students should not be made to feel that they lack control over their personal information or that their privacy is under attack. Each university must endeavour to clearly inform the student body that should a cause for concern ever arise, their information may be shared in the interest of ensuring their health and safety and by extension that of the student body as well. This is done only in order to best address how to help an at-risk student, not in order to control or segregate them. An information sharing group must remain transparent in purpose and conscientious in action in order to maintain the vital balance between the rights of the one and interests of the many. The parameters of the relationship between a university and its students should be clearly laid out so as not to enable the university to step past its boundaries. Not only is the academic success of a student the business of a university, but so is their overall wellbeing.

The administration at Virginia Tech realized too late that their failure to understand and clarify the provisions of the *Family Educational Rights and Privacy Act* (FERPA) would result in a fatal cost of vast proportions. It was a complete lack of

understanding of FERPA that allowed much of the valuable information concerning a distraught young man to be fragmented, ignored, and kept confidential. The Report of the Virginia Tech Review Panel stated that “information privacy laws are intended to strike a balance between protecting privacy and allowing information sharing that is necessary or desirable.” (63) Yet, the only way this balance can find expression is when those responsible for administering the law are fully aware of when and how to apply it. Individual privacy rights and the public interest are impossible to reconcile if there is no understanding of how to use the tools intended to find equilibrium. Should tragedy strike a university with no foundation of knowledge upon which to stand, they risk having their rational decision-making power swept away among an emotional tide of moral panic and public outrage.

Ontario universities have a responsibility to build this strong foundation of knowledge around privacy legislation. However, along with this responsibility, these institutions also have a duty to ensure their students are still being afforded the full scope of privacy protection offered to them under FIPPA. Institutions have demonstrated a clear lack of effort “to assess carefully the risks of privacy invasions that are not the direct result of security breaches or equipment failures, but that have to do with more routine exposure of individuals to the ubiquitous processes by which their data are collected and used.” (Bennett and Raab 58) An information sharing initiative must not “creep” into the role of silent, pervasive risk management. It must remain strictly dedicated to the singular purpose of compiling existing personal information for care purposes and disclosing this information to an outside party only when it is in the best interests of the at-risk individual to do so.

As the previous section cautioned, function creep driven by a risk thinking approach within an information sharing framework can upset the balance between individual privacy and the public interest. This danger must be acknowledged and controlled for if an institution wishes to uphold the ideals of autonomy and democracy we associate with our individual privacy. Any perceived attack upon these values will irreparably damage the credibility and trustworthiness of an institution and the confidence of those residing therein. Universities need to clearly establish that their relationship with students is one that contains an element of preserving individual well-being along with promoting academic excellence, but that this relationship is not one that will endanger the stability of individual privacy rights. During pressing circumstances threatening a student's welfare and security, the sharing and disclosure of personal information is done to best address the individual at risk, not to impede upon their privacy as part of a risk management plan. Institutional risk management should not be a central element to any care based approach. The reduction of risk and enhancement of safety for a campus as a whole will emerge as a product of strong legislative knowledge and sound application of the law.

Ontario universities have been provided with a clear and comprehensive set of tools that can achieve balance between individual privacy rights and the public interest. What is needed is the effort to learn how to wield them correctly. Virginia Tech's system "failed for lack of resources, incorrect interpretation of privacy laws, and passivity." (Report of the Virginia Tech Review Panel 2) By actively investing the time, effort and resources into clarifying and comprehending the intricacies of their own provincial privacy laws, Ontario universities can ensure their approach to at-risk individuals is one

founded upon knowledge and understanding. With this clarity of thought and approach, it is easy to realize that FIPPA is not intended, nor is it structured in a way, that would remove or override our sense of humanity and common sense. This legislation was not created in a void, away from the influence of human thought and reason. These qualities can function when faced with a difficult situation, while still respecting individual rights. As Ontario's Privacy Commissioner Ann Cavoukian stated so succinctly, "life trumps privacy." (Cavoukian 2008) This sentiment has form and substance within the legislation if one simply takes the time to look for it.

Works Cited

- Attallah, Paul. "The Audience". Mediascapes: New Patterns in Canadian Communication. Scarborough: Nelson, Thompson Canada Limited, 2002. 90-106.
- Banerjee, Neela. "Amid the Chaos of Deaths, a Minister Attends to Those Who Are Grieving". New York Times. 19 Apr. 2007, late ed.: 19.
- . "On a Stunned Campus, Longing for the Normal But Enveloped by Grief". New York Times. 20 Apr. 2007, late ed.: 20.
- Bailey, Dennis. The Open Society Paradox: Why the 21st Century Calls for More Openness – Not Less. Washington: Brassey's, Inc., 2004.
- Bauman, Zygmunt. "Social Issues of Law and Order". British Journal of Criminology. 40 (2000): 205-221.
- Belluck, Pam. "Intersecting on a Fateful Day, Lives That Spanned the Country and the World". New York Times. 18 Apr. 2007, late ed.: 19.
- Bennett, Colin J, and Charles D. Raab. The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge: The MIT Press, 2006.
- Broder, John M. "32 Shot Dead in Virginia; Worst U.S. Gun Rampage". New York Times. 17 Apr. 2007, late ed.: 1.
- Brooks, David. "The Morality Line". New York Times. 19 Apr. 2007, late ed.: 27.
- "Campus shootings draw world scrutiny." CTV News 9 July 2007
<[http://www.ctv.ca/servlet/ArticleNews/print/CTVNews/20070417/world_reax_sshootings_070417/20070417/](http://www.ctv.ca/servlet/ArticleNews/print/CTVNews/20070417/world_reax_shootings_070417/20070417/)>
- Carey, Benedict. "For Rampage Killers, Familiar Descriptions, 'Troubled' and 'Loner,' but No Profile". New York Times. 18 Apr. 2007, late ed.: 21.
- . "When The Group Wise". New York Times. 22 Apr. 2007, late ed.: 1.
- Carleton University Hazard Reporting Policy, enacted June 2005
<http://www.carleton.ca/secretariat/policies/Hazard_Reporting.html>
- Carleton University Patrol Services. 2005. Carleton University, Department of University Safety. 20 Feb 2008. <<http://www.carleton.ca/patrol/index.html>>
- Carleton University Residence Contract, 2007-2008
<<http://www.carleton.ca/housing/ResidenceContract2007-2008.pdf>>

- Carter, Bill. "Package Forced NBC to Make Tough Decisions". New York Times. 19 Apr. 2007, late ed.: 18.
- . "NBC News Defends Its Use of Material Sent by the Killer". New York Times. 20 Apr. 2007, late ed.: 21.
- Cavoukian, Ann. "The Laws Didn't Fail." Washington Post. 10 Sept. 2007: A14.
- . "Privacy not an absolute." National Post. 25 April 2008: A13.
- Cohen, Stanley. Folk Devils and Moral Panics: The Creation of the Mods and Rockers, 3rd Ed. New York: Routledge, 2002.
- Cohen, Noam. "The Latest on Virginia Tech, From Wikipedia". New York Times. 23 Apr. 2007, late ed.: 4.
- de Lint, William, Sirpa Virta, and John Edward Deukmedjian. "The Simulation of Crime Control: A Shift in Policing?" American Behavioral Scientist 50 (2007) 1631-1647.
- d'Entrèves, Maurizio Passerin, and Ursula Vogel eds. Public & Private: Legal, Political and Philosophical Perspectives. New York: Routledge, 2000.
- Department of Health and Human Services (U.S.), Department of Education (U.S.), Department of Justice (U.S.) Report to the President on Issues Raised by the Virginia Tech Tragedy. Washington: DHHS, DOE, DOJ, 2007.
- Dewan, Shaila. "Drumbeat of Shots, Broken by Pauses to Reload". New York Times. 17 Apr. 2007, late ed.: 1+.
- and John M. Broder. "Rampage Gunman was Student; Warning Lag Tied to Bad Lead". New York Times. 18 Apr. 2007, late ed.: 1+.
- and Marc Santora. "Officials Knew Troubled State of Killer in '05". New York Times. 19 Apr. 2007, late ed.: 1.
- Eaton, Leslie and Michael Luo. "Shooting Rekindles Issues of Gun Rights and Restrictions". New York Times. 18 Apr. 2007, late ed.: 20.
- "Eight Years After Columbine". New York Times. 17 Apr. 2007, late ed.: 26.
- Etzioni, A., "A Contemporary Conception of Privacy." Telecommunications and Space Journal. 6 (1999): 8-114. 15 Oct 2007
<http://www.gwu.edu/~ccps/etzioni/A270.html#N_17_>
- Fairfield, Paul. Public/Private. New York: Rowman and Littlefield Publishers, Inc., 2005.

- Feeley, Malcolm M. and Jonathan Simon. "The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications." Criminology. 30 (1992): 449-474.
- Fernandez, Manny and Marc Santora. "In Words and Silence, Hints of Anger and Isolation". New York Times. 18 Apr. 2007, late ed.: 1.
- Fischer, Karen. "Report to President Bush on Virginia Tech Tragedy Faults Federal Privacy Laws." The Chronicle of Higher Education 13 Sept 2007
<<http://chronicle.com/daily/2007/06/2007061402n.htm>>
- Find A University. 2008. Ministry of Training, Colleges, and Universities. 20 February 2008. <<http://www.edu.gov.on.ca/eng/general/list/univers.html>>
- Garland, David. The Culture of Control. Chicago: University of Chicago Press, 2001.
- Geddes, John, "A Life of Its Own." Maclean's 19 June 2000: 16-21.
- Goode, Erich and Nachman Ben-Yahuda. Moral Panics: The Social Construction of Deviance. Oxford: Blackwell, 1994.
- Greenberg, Josh, and Brian Wilson. "Youth Violence, Moral Panic, and the Canadian Media: News Coverage of School Shootings in the United States and Canada." Mediascapes: New Patters in Canadian Communication. Toronto: Thomson/Nelson, 2006. 95-113.
- Greenspon, Edward. "Speak your mind – and erase a stigma". Globe and Mail. 20 June 2008: A1.
- Ha, Stephanie. "Universities beef up security measures in wake of report on Virginia Tech shootings." The Charlatan 17 Sept. 2007
<http://www.charlatan.ca/index.php?option=com_content&task=view&id=277&Itemid=149>
- Haggerty, Kevin D. and Richard V. Ericson eds. The New Politics of Surveillance and Visibility. Toronto: University of Toronto Press, 2006.
- Halchi, Abigail. "Social Movements." Understanding Contemporary Society: Theories of the Present. London: Cromwell Press, 2000. 463-475.
- Hall, Stuart at. al. "The Social Production of News." Policing the Crisis: Mugging, The State and Law and Order. London: MacMillan Press, Ltd., 1978. 55-77.
- Herbert, Bob. "A Volatile Young Man, Humiliation and a Gun". New York Times. 19 Apr. 2007, late ed.: 27.

- Heffernan, Virginia. "Online, Students Say 'Reach Out to Loners'". New York Times. 19 Apr. 2007, late ed.: 1+.
- Hernandez, Raymond. "A Friend, a 'Good Listener' and a Victim in a Day of Tragedy". New York Times. 17 Apr. 2007, late ed.: 18.
- . "Inside Room 207, Students Panicked at Rampage and Then Held Off Gunman's Return". New York Times. 18 Apr. 2007, late ed.: 19.
- Information and Privacy Commissioner of Ontario. Access and Privacy Excellence...20 Years in the Making 20th: Anniversary Collection. Toronto: IPC, 2007.
- . 2004 Annual Report. Toronto: IPC, 2005.
- . 2006 Annual Report. Toronto: IPC, 2007.
- "Information On Order." Globe and Mail 19 July 1985: P6.
- Jones, Paul. "Moral Panic: The Legacy of Stan Cohen and Stuart Hall." Media International Australia 85 (1997): 6-16.
- Killingbeck, Donna. "The Role of Television News in the Construction of School Violence as a 'Moral Panic'". Journal of Criminal Justice and Popular Culture. 8 (2001) 186-202. 15 Nov. 2007
<<http://www.albany.edu/scj/jcipc/vol8is3/killingbeck.html>>
- Kipp, Rachel. "DSU teen dies from shooting injuries". The News Journal. 10 Nov. 2007. <<http://www.choosecampus911.com/news-pdfs/Wilmington,%20DE%20-%20Oct%202007.pdf>>
- Kleinfield, N.R. "Before Deadly Rage, A Lifetime Consumed By a Troubling Silence". New York Times. 22 Apr. 2007, late ed.: 1+.
- Klosek, Jacqueline. The War on Privacy. Westport: Praeger Publishers, 2007.
- Kulish, Nicholas. "Another Young Man Who Was Angry and Lonely, but Unarmed". New York Times. 22 Apr. 2007, late ed.: 11.
- Lee, Suevon. "Praying for 'Troubled Soul' And Mourning for Victims". New York Times. 23 Apr. 2007, late ed.: 14.
- Lewin, Tamar. "Unsettled Day on Campuses Around U.S.". New York Times. 18 Apr. 2007, late ed.: 18.
- . "Laws Limit Colleges' Options When a Student Is Mentally Ill". New York Times. 19 Apr. 2007, late ed.: 1.

- “List of Major Incidents”. CTV News. 10 Nov. 2007.
<http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060913/violence_timeline_060913/20060913/>
- Luo, Michael. “U.S. Rules Made Killer Ineligible to Purchase Gun”. New York Times. 21 Apr. 2007, late ed: 1+.
- Lyon, David. “9/11, Synopticon, and Scopophilia: Watching and Being Watched.” The New Politics of Surveillance and Visibility. Toronto: University of Toronto Press, 2006.
- Marsh, Bill. “An Accounting of Daily Gun Deaths”. New York Times. 22 Apr. 2007, late ed: 14.
- McRobbie, Angela. “The Moral Panic in the Age of the Postmodern Mass Media.” Postmodernism and Popular Culture. New York: Routledge, 1994. 198-219.
- Michaluk, Dan, and Catherine Peters. “Students at Risk – Maintaining balance after Virginia Tech.” Client Update 12 July 2007
<<http://www.hicksmorley.com/hicksmorley/publications/updates/2007/CU-StudentsAtRisk.htm>>
- Ministry of Finance Ontario Legislature Approves Spring Budget Bill. Toronto: MOF, 2005. 11 Feb 2008 <<http://www.fin.gov.on.ca/english/media/2005/nr11-sbb.html>>
- Monahan, Torin. “War Rooms of the Street: Surveillance Practices in Transportation Control Centers.” The Communication Review. 10 (2007): 367-389.
- Moynihan, Colin. “Professor’s Violent Death Came Where He Sought Peace”. New York Times. 19 Apr. 2007, late ed.: 20.
- Newman, Katherine S. The Social Roots of School Shootings. New York: Basic Books, 2004.
- Nelkin, Dorothy and Laurence Tancredi. Dangerous Diagnostics: The Social Power of Biological Information. Chicago: University of Chicago Press, 1994.
- Oakley, Barbara. “The Killer in the Lecture Hall”. New York Times. 19 Apr. 2007, late ed.: 27.
- O’Donoghue, Mary. Sharing Information in the Educational Sector: What are the Boundaries? Hot Issues in FIPPA and MFIPPA for School Boards, Colleges and Universities, 16 Jan 2008, The Law Society of Upper Canada. Toronto, Ontario: 2008.

- Office of the Information and Privacy Commissioner/Ontario Health Information Custodians Working for Non-Health Information Custodians. Toronto: IPC, 2006.
- Office of the University Secretariat. 2008. Carleton University. 25 July 2008.
<<http://www.carleton.ca/secretariat/>>
- “Oyster data is ‘new police tool.’” BBC News. 4 June 2008.
<http://news.bbc.co.uk/2/hi/uk_news/england/london/4800490.stm>
- Pappano, Laura. “You Better Watch Out”. New York Times. 22 Apr. 2007, late ed: 17.
- Pateman, Carol. The Sexual Contract. California: Stanford University Press, 1988.
- Perez-Pena, Richard. “Media Outlets Ease Off Video of Killer, but Not Because of Complaints, They Say”. New York Times. 21 Apr. 2007, late ed: 13.
- “Quotation of the Day”. New York Times. 17 Apr. 2007, late ed.: 2.
- ”. New York Times. 18 Apr. 2007, late ed.: 2.
- Rachels, James. “Why Privacy is Important”. Philosophy and Public Affairs. 4 (1975): 323-333.
- Reiss, A. “The Legitimacy of Intrusion into Private Spaces”. Private Policing. Beverly Hills: Sage, 1987. 19-44.
- Report of the Virginia Tech Review Panel, Presented to Timothy M. Kaine, Governor Commonwealth of Virginia. Mass Shootings at Virginia Tech. Virginia: Virginia Tech Review Panel, 2007.
- Rose, Nikolas. “Government and Control”. British Journal of Criminology. 40 (2000): 321-339.
- Roy, Lucinda. “A Black Day in the Blue Ridge”. New York Times. 17 Apr. 2007, late ed.: 27.
- Santora, Marc and Christine Hauser. “Students Knew Killer’s Demons By His Writings”. New York Times. 20 Apr. 2007, late ed: 1+.
- Saunders, Eileen. “Good Kids/Bad Kids: What’s a Culture to Do?”. Mediascapes: New Patterns in Canadian Communication. Scarborough: Nelson, Thompson Canada Limited, 2002. 136-157.
- Schissel, Bernard. Still Blaming Children: Youth Conduct and the Politics of Child Hating. Halifax: Fernwood Publishing, 2006.

- Schoeman, Ferdinand David. Privacy and Social Freedom. Cambridge: Cambridge University Press, 1992.
- Scott, A.O. "Drawing A Line From Movie To Murder". New York Times. 23 Apr. 2007, late ed: 1.
- Scott, Ian (Attorney General). "Introduction of Bills: Freedom of Information and Protection of Privacy Act." Debates of the Legislative Assembly of Ontario. 12 July 1985: Morning. 21 March 2008. <http://www.ontla.on.ca/web/house-proceedings/house_detail.do?Date=1985-07-12&Parl=33&Sess=1&locale=en#P334_87203>
- Scullion, Aaron. "Smart cards track commuters." BBC News. 4 June 2008 <<http://news.bbc.co.uk/2/hi/technology/3121652.stm>>
- Shapira, Ian, and Tom Jackman. "Gunman Kills 32 at Virginia Tech in Deadliest Shooting in U.S. History." Washington Post. 17 April 2007: A01.
- Shuchman, Miriam. "Falling through the Cracks – Virginia Tech and the Restructuring of College Mental Health Services." The New England Journal of Medicine 357 (2007): 105-110.
- "Some California Schools Close After Threat". New York Times. 20 Apr. 2007, late ed: 21.
- "Some Had Made Their Marks, and Many Others Were Just Beginning". New York Times. 18 Apr. 2007, late ed.: 21.
- Special Constables. 2008. The Ottawa Police Service. 22 June 2007. <http://www.ottawapolice.ca/en/serving_ottawa/support_units/constables_main.cfm>
- Steinhauer, Jennifer. "Korean-Americans Brace for Problems in Wake of Killings". New York Times. 19 Apr. 2007, late ed.: 19.
- Stanley, Alessandra. "Deadly Rampage and No Loss for Words". New York Times. 17 Apr. 2007, late ed.: 19.
- . "Amid Chaos, One Notably Restrained Voice". New York Times. 19 Apr. 2007, late ed: 1+.
- Staples, William G. Everyday Surveillance: Vigilance and Visibility in Postmodern Life. Maryland: Rowman and Littlefield Publishers, Inc., 2000.
- . The Culture of Surveillance: Discipline and Social Control on the United States. New York: St. Martin's Press, 1997.

Steinberg, Jacques. "In the Wake of Campus Killings, Talk Radio Tries for Humor and a Political Advantage". New York Times. 20 Apr. 2007, late ed: 21.

Sullivan, John. "Metro Briefing New York: Stricter Gun Checks Proposed". New York Times. 23 Apr. 2007, late ed: 6.

Sypnowich, Christine. "The civility of law: between public and private." Public & Private: Legal, Political and Philosophical Perspectives. New York: Routledge, 2000.

"The Silence of Politicians". New York Times. 19 Apr. 2007, late ed.: 26.

Thompson, Judith Jarvis. "The Right to Privacy." Philosophy and Public Affairs. 4 (1975): 295-314

Toner, Robin. "Renewed Scrutiny For Gun Controls". New York Times. 17 Apr. 2007, late ed.: 25.

University of Toronto Campus Community Police, Special Constable Service. 2008.
University of Toronto Campus Community Police. 20 Feb 2008.
<<http://www.campuspolice.utoronto.ca/community/about.htm>>

Urbina, Ian and Manny Fernandez. "On Quiet Weekend at Virginia Tech, Reminders of a Tragedy and Hope for the Future". New York Times. 23 Apr. 2007, late ed: 14.

--- and Manny Fernandez. "University Explains the Return of Troubled Student". New York Times. 20 Apr. 2007, late ed: 21.

--- and Suevon Lee. "For School, Several Ties to Shootings". New York Times. 18 Apr. 2007, late ed.: 18.

Van der Werf, Martin. "Florida Panel, Appointed After Virginia Tech Tragedy, Recommends Sharing Information About Troubled Students." The Chronicle of Higher Education 15 July 2007
<<http://chronicle.com/daily/2007/05/2007052502n.htm>>

"Victims' Talents Are Remembered". New York Times. 19 Apr. 2007, late ed.: 19.

"Virginia Tech Defends Decision". New York Times. 20 Apr. 2007, late ed: 1.

Welcome to the IPC Website! 2006. Office of the Information and Privacy Commissioner of Ontario. 18 Feb. 2008. <<http://www.ipc.on.ca>>

Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967.

Whitcomb, Christopher. "Building a Better Lockdown". New York Times. 20 Apr. 2007, late ed: 23.

Legislation

Bill 197 2nd Session, 38th Legislature, Ontario 54 Elizabeth II, 2005 (Chapter 28 Statutes of Ontario, 2005) An Act to implement Budget measures

Family Educational Rights and Privacy Act 20 USC S. 1232g 10 Sept. 2007.
<<http://epic.org/privacy/education/ferpa.html>>

Freedom of Information and Protection of Privacy Act R.S.O. 1990, CHAPTER F.31

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 104th Congress 6 Nov. 1997. <<http://aspe.hhs.gov/admsimp/pl104191.htm>>

Personal Health Information Protection Act, 2004 S.O. 2004, CHAPTER 3 Schedule A

Police Services Act R.S.O. 1990, CHAPTER P.15

The Anti-Terrorism Act R.S., c. C-46

Appendix A

The following is a list of all Ontario Universities recognized by the Ministry of Training, Colleges and Universities. Current reference information on the health and/or counselling services offered by each institution is listed, and where a direct online link is missing, contact information has been provided.

1. Brock University
<http://www.brocku.ca/healthservices>
2. Carleton University
<http://www.carleton.ca/health>
3. Dominican University College
(613) 233-5696
info@dominicancollege.ca
4. Lakehead University
<http://healthservices.lakeheadu.ca>
5. Laurentian University
<http://142.51.14.1/Laurentian/Home/Departments/Health+Services/Homepage.htm>
6. McMaster University
<http://www.mcmaster.ca/health>
7. Nipissing University
<http://www.nipissingu.ca/administration/StudentAffairs.asp>
8. Ontario College of Art & Design
http://www.ocad.ca/students/student_services/health_wellness.htm
9. Queen's University
<http://www.queensu-hcds.org/hs>
10. Royal Military College
RMC Liaison Office
(613) 541-6000 ext. 6984
11. Ryerson University
<http://www.ryerson.ca/student services/healthcentre>
12. Trent University
<http://www.trentu.ca/studentaffairs/healthservices.php>
13. University of Guelph
<http://www.studenthealth.uoguelph.ca/services.shtml>

14. University of Ontario Institute of Technology
http://www.uoit.ca/EN/main/11259/11270/campus_health_centre.html
15. University of Ottawa
http://www.uottawa.ca/health/health-services/services_offered.html
16. University of Toronto
<http://www.utoronto.ca/health/index.html>
17. University of Waterloo
<http://www.healthservices.uwaterloo.ca/index.html>
18. University of Western Ontario
<http://www.shs.uwo.ca>
19. University of Windsor
<http://www.uwindsor.ca/health>
20. Wilfrid Laurier University
<http://www.mylaurier.ca/health/info/home.htm>
21. York University
<http://www.yorku.ca/yorkweb/currentstudents/campuservices/supportservices.html>