Interpreting Privacy on Campus:  
The Freedom of Information and Personal Privacy and Ontario Universities

Martin R. Dowding  
Wilfrid Laurier University

ABSTRACT  When the Freedom of Information and Protection of Privacy Act (FIPPA) was imposed on Ontario's university campuses in 2006, faculty and students were made to look closely at their own habits and to reconsider campus traditions relating to privacy. The backdrop to the legislation is a complex matrix of campus relations, policy, sharing of health information, and the use and abuse of information and communication technologies. Part 1 of this article examines the recent history of privacy in general and privacy on campus in Ontario, Canada, and the United States. Part 2 reports the outcome of a series of focus groups held on two Ontario university campuses in which faculty and undergraduate students were asked about their perceptions of privacy on campus and their knowledge and comprehension of FIPPA.

KEYWORDS  Privacy; Law/legislation; FIPPA; PHIPA; New media; Focus groups

In June 2006, the Freedom of Information and Protection of Privacy Act (FIPPA) became law for Ontario universities. The legislation created new rules for the collection, handling, and disclosure of information on campus. Some students, faculty, and staff struggled with the complexity of the legislation. More significantly, the legislation led to a new perception that privacy itself is complex and fraught with paradox. As I dis-

Martin R. Dowding is an Assistant Professor in the Department of Communication Studies at Wilfrid Laurier University, 75 University Avenue West, Waterloo, ON  N2L 3C5. Email: mdowding@wlu.ca.
covered when I conducted focus groups on campus, the introduction of FIPPA highlighted contradictory attitudes to privacy for people who value privacy but give away their most intimate personal information, particularly online, in capitalist market-exchange arrangements. In concert with other legislation, FIPPA allows the disclosure of otherwise sacrosanct health information at times of crisis for the sake of saving lives. The introduction of FIPPA drew attention to the implications of online storage in the United States of Canadians' private information, such as academic research queries, where all information is subject to government surveillance under the USA Patriot Act. This article investigates the reception of FIPPA on campuses required to adopt a universally applied policymaking instrument. FIPPA's implementation led Ontario university administrations to review and revise now outdated or inconsistent privacy policies. It also required universities to explain the new legislation, a task that proved to be unexpectedly difficult.

This article is composed of two parts. The first part considers privacy policy and legislation in Canada and the United States (especially since September 11, 2001) and the contested meanings of privacy itself. This section also considers the effects of new media and online social networks, also known as social networking sites (SNSs), such as MySpace and Facebook. SNSs are popular with university students, who do not appear to recognize the potential dangers of freely exchanging personal information on such services. The article also investigates whether Canadian and U.S. policies regarding the disclosure of personal legislation are adequately interpreted in times of crisis. The second part of the article describes perceptions about privacy on campus by interpreting the outcome of a series of focus groups held in 2008-09 on two very different Ontario university campuses. I embarked on my documentary analysis and focus group interviews with the following positive assumptions: Faculty thought the legislation was necessary; students and faculty would understand FIPPA; the legislation had been introduced through a well-organized process; focus group participants would, therefore, be informed enough to help make and explain policy on their campuses.

Despite my original assumptions, I discovered that the implementation of FIPPA was perceived to have been confusing and incomplete by many faculty and students. There were differences in the comprehension and reception on the two campuses as well as between the two cohorts of faculty and students.

What does FIPPA do?
According to the legislation,

The purposes of this Act are,

(a) to provide a right of access to information under the control of institutions in accordance with the principles that,

(i) information should be available to the public,

(ii) necessary exemptions from the right of access should be limited and specific, and

(iii) decisions on the disclosure of government information should be reviewed independently of government; and
(b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information. (Ontario, FIPPA, 2010, s. 1)

The Act requires that a provincial privacy commissioner work at arm’s length from government to respond to freedom of information requests and breaches of privacy. There is also a federal commissioner whose role is somewhat different.

Why study the reception of FIPPA, and how?

Like all democratic legislation, FIPPA is the result of a formal undertaking designed to guide social action, including policymaking. Ideal civil society responses to policy issues include giving voice to as many persons as possible, as Parsons makes clear when he speaks of policy “critical theorists” who:

> envisage policy analysis as an activity which should be informed by a radical commitment to social change and equality as a prerequisite for improving decision-making. Critical policy analysis advocates a fundamental and far-reaching shift towards a more open decision-making process and the empowering of citizens, rather than improving the way in which decision-makers use information and knowledge. (1995, p. 444)

An analysis of FIPPA requires that research be conducted within the context of “privacy studies” (see Bennett, 2008; Bennett & Grant, 1999; Cavoukian, 2005, 2009; Rule, 2007; Schoeman, 1984; Shade, 2008). The study of FIPPA’s reception is also important in the light of how Ontario universities responded to the Council of Universities’ attempts to regulate freedom of information (FOI) in the spirit of FIPPA, which met with little success. Some universities completely ignored the request to adopt FOI policies, including one of the two where I held my focus groups, while others replied in an uneven fashion. This was made clear in the Ontario College and University Faculty Association’s (OCUFA) report Restricted Entry: Access to Information at Ontario Universities (2004). To help overcome the problem that universities would not respond favourably to OCUFA’s request to accept FOI policies, FIPPA was made law.

Given the fragility of privacy in the public sphere, particularly since the advent and convergence of contemporary information and communication technologies (ICTs), it is also necessary to conduct research in light of “surveillance studies” (see Lyon, 1994, 2006, 2007; Rule, 1974; Whitaker, 1999).

Development of FIPPA

FIPPA was informed by policies and practices developed in other jurisdictions where similar privacy legislation for universities was already in place (for example, in most Canadian provinces, although New Brunswick’s privacy laws do not currently cover universities, and in many U.S. states, Australia, and the U.K.). In addition, the 10-point Model Code for the Protection of Personal Information (first published in 1996), developed by the Canadian Standards Association (CSA), helped Canadian and international legislators develop a variety of privacy laws and policies. Examples of the CSA’s impact on the collection, handling, and disclosure of personal information, besides FIPPA, include Canada’s federal Personal Information Protection and Electronic Documents Act (Canada, PIPEDA, 2000), to which the CSA code is appended.
Before FIPPA the Personal Health Information Protection Act (PHIPA), which regulates the disclosure of private health information, had been applicable to universities since its implementation in 2004. But, unlike FIPPA, the implementation of PHIPA did not arouse widespread confusion. The province’s intention was to clarify privacy issues in a consistent way by implementing FIPPA and PHIPA on campus.

Prior to implementing FIPPA and PHIPA legislation, Ontario universities had no common policies for guaranteeing access to institutional information (such as whether animal experimentation is taking place) or for protecting the privacy of students and faculty. Historically, pre-FIPPA practices on campus that compromised personal privacy included leaving unattended assignments in hallways bearing student names, numbers, and grades, which led to stalking, identity theft, or plagiarism (as persons passing by picked out the best assignments). FIPPA and PHIPA also outlined situations in which counsellors, professors, or campus security can disclose private personal and institutional information, for example if a student is psychologically vulnerable or if there is the potential for violence on campus. This example, in particular, points to the tension in the legislation between protection and disclosure of personal information. Subsequent events show that the legislation in Canada, and similar legislation elsewhere, has been poorly interpreted, in routine situations but particularly in times of crisis.

Privacy defined: An impossible paradox?
Definitions of privacy have a long and varied history, since antiquity (Aristotle: Browne, 1882). Since that time privacy practices have been described by anthropologists (Mead, 1953), contemporary philosophers (DeCew, 1997, 2008; Habermas, 1991), political scientists (Bennett & Raab, 2006), legal experts (Branscomb, 1994; Warren & Brandeis, 1890), and communication scholars (Rauhofer, 2008; Shade, 2008). DeCew (2008) speculates that “there is no single definition or analysis or meaning of the term” (n.p.). Some economists, for example Posner (1981), argue that access to certain information diminishes its value, and that concealment or disclosure of personal information is frequently for personal gain. Some feminists, for example MacKinnon (1989), point out that privacy, especially when domestic violence is kept private, can be detrimental to women’s safety.

The influence of new media technologies further complicates the meanings of privacy. Issues related to precursors to today’s ICTs were first tentatively addressed more than a century ago in an often-quoted essay by Warren and Brandeis, “The Right to Privacy,” published in the Harvard Law Review (1890). The article points out:

[T]hat the individual shall have full protection in person and in property is a principle as old as the common law; but it has often been found necessary from time to time to define anew the exact nature and extent of such protection …. [R]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person … the right ‘to be let alone.’

The “recent inventions and business methods” Warren and Brandeis refer to are “instantaneous photographs and newspaper enterprise,” and what we now might call the “tabloids.” The foundation of their argument is that new media devices (in
their case cheap Kodak cameras, then a recent invention) in the hands of careless or malicious people can cause harm to reputations by breaching privacy. More recently, Solove (2007) cites examples of the harm that can be done to reputations when privacy is breached by journalists, bloggers, or students with cellphone cameras on campus.

Not only can people be wronged when their privacy is breached by others, but people also breach their own privacy by disclosing very personal information, particularly when using new media. My research shows that students and faculty are harmed by others and that they harm themselves by giving up private information for online purchases and social networking without considering what negative consequences might occur, such as third parties gaining access to private information for bullying (Bryce, 2009), marketing purposes (Micheti, Burkell, & Steeves, 2010), scams, or identity theft.

“Reasonable” expectations of privacy
In accordance with legislation such as FIPPA, Ontario common law judicial decisions rely on the “reasonableness” of privacy expectations and the value to public interest of information being disclosed. Because “reasonable” is never clearly defined (in law or the Canadian Charter of Rights and Freedoms, for example), its meaning shifts as social norms and practices change. Twenty years ago few students or faculty on campus would have thought it “reasonable” for closed-circuit TV (CCTV) surveillance to be as ubiquitous as it is today. Since the introduction of social networking sites, it has become “unreasonable” to expect privacy if one is photographed at a campus party while intoxicated, since photographs of the indiscretion can be easily distributed online. It is also “unreasonable” to expect privacy if one commits an indecent act in a public place under surveillance by CCTV, whether one knows about the camera or not. The awareness that there is likely no “reasonable” expectation of personal privacy in any space, private or public, is one of the strongest arguments for personal discretion. Students’ disregard for privacy is the leading cause of harm to their reputations, particularly when background checks are conducted by human resources personnel (Brandenburg, 2008; Solove, 2007). On the other hand, both PHIPA and FIPPA specify that it is “reasonable” to disclose private information in the public interest. In extraordinary circumstances it is in the public interest to name a minor in order to solve a crime, or to name a potentially dangerous or emotionally “at-risk” student on campus.

When Sun Microsystems CEO Scott McNealy said, “You have zero privacy anyway. Get over it” (Sprenger, 1999), he was referring to how vulnerable ICTs are to hacking and how third-party appropriation of personal information diminishes guarantees to privacy. But to show why there are even fewer “reasonable expectations” of privacy, despite privacy legislation, I want briefly to consider surveillance in the light of laws such as section 215 of the USA Patriot Act, the European Union Cybercrime law, and the still-to-be determined Canadian “lawful access” legislation. “Lawful access” allows state authorities to secure private personal information, such as email and online searches, for “security” reasons.

All of these laws challenge Warren and Brandeis’ concept of the “right to be let alone.” At this writing the Conservative Canadian government’s “lawful access” legis-
ulation entitled Investigative Powers for the 21st Century (IP21C) is in limbo, after Parliament was prorogued in December 2009.\(^5\) IP21C was introduced after earlier efforts by the Liberals to create a similar law, in response to pressure from other international efforts (Dowding, 2005; Geist, 2009). IP21C would demand that Internet service providers (ISPs, including university information technology services) surrender to police all subscribers’ personal information, without clear justification, and without anyone necessarily knowing that they are under suspicion or why. IP21C could also require ISPs to preserve data that users have saved on their system.

Although Canadians do not yet have “lawful access” legislation, equivalent to other countries, we have been subject to U.S. “lawful access,” under the Patriot Act, introduced in 2001. President Obama signed legislation to continue the Patriot Act, unchanged, in early 2010. That legislation impinges on us whenever information crosses the border due to legally binding obligations to share “trans-border data flows.” Multilateral agreements, in NAFTA or others arrived at through the World Trade Organization (WTO), for example, have been negotiated to control banking, trade, and international money-laundering crime. The U.S. surveillance apparatus, in the guise of the Patriot Act, indicates that great vigilance is required to maintain the privacy of our personal information.

An example of how the Patriot Act affects Canadian campuses is the controversy surrounding RefWorks. According to its website, RefWorks, “an online research management, writing and collaboration tool—is designed to help researchers easily gather, manage, store and share all types of information, as well as generate citations and bibliographies” (http://www.refworks.com). Controversy arose when it was revealed that Canadian electronic academic records stored on U.S. computer servers were subject to section 215 of the Patriot Act, which breached, at least, Canadian universities’ trust in their relationship with the U.S. security apparatus. While using RefWorks to ease the burden of research sounds promising, the U.S. surveillance apparatus, working under the aegis of the Patriot Act, could also (through RefWorks) “easily gather, manage, store and share all types of information” in an attempt to find research being conducted about sensitive issues such as terrorism. Canadian academic research, undertaken through RefWorks, was subject to unwarranted searches by the United States. Given the secrecy of section 215 of the Patriot Act, we may never know what kinds of searches the FBI undertook (ACLU, 2006).

Once librarians and faculty in Canadian universities and colleges realized that privacy related to campus activities was potentially under attack, during the period of 2006-07 many academic institutions abandoned the U.S. server and created a Canadian equivalent, at the University of Toronto, where Canadian searches are now stored (although that move may be moot, given the revival of Canadian “lawful access” legislation). In light of the RefWorks incident and the Patriot Act’s impact in general, concern for privacy welfare can be felt anywhere outside the United States, including on Ontario’s university campuses.

**Giving up privacy on campus: Students and social networks**

Research into transformed international privacy regulation is important because of the chilling effect of the Patriot Act and legislation like it. But privacy on campus has also been affected by social networking sites (SNSs). The work of two cyberspace schol-
ars, John Palfrey (see Coutu, Joerres, Fertik, Palfrey, & Boyd, 2007) and Patricia Sanchez Abril (2007), is particularly informative about university students’ attitudes to privacy. Palfrey’s work on SNSs introduced the concept of young “digital natives” (undergraduate students, for example) who have lived with the newest media all their lives and “digital immigrants,” such as aging academics, who have adapted to new ICTs. Sanchez Abril critiques Palfrey’s work by pointing out that many students are not, in fact, tech savvy, and many octogenarians are completely plugged in. Both scholars, however, address SNSs as critical agents in privacy research, on one hand providing a new form of community, and on the other hand providing a new opportunity for carelessness and moral panic.

Whether people are new media “natives” or “immigrants,” maintaining control over privacy on SNSs is difficult, especially because new ones are invented so often and privacy settings are difficult to negotiate, due to their length and legalese. Although the technologically savvy “natives” may be coming to campus with more intensive online experience than faculty, it is often narrower experience with games and SNSs. The older “immigrants” are more than likely to have a better sense of the cost-benefit “minimax” factor developed by Mill (1843; 1956), by which people attempt to maximize their social benefits and minimize their social cost. The student “natives” will also bring to campus less awareness of what VanLear (1987) calls “self-disclosure reciprocity,” also related to the cost-benefit value of degrees of social engagement. The “immigrants” have, at least, experienced more social behaviour in general and are, therefore, more wary of online dangers and the value of limited self-disclosure. In their relatively brief encounters with privacy in day-to-day life, the student “natives” have been subject to greater attempts at online privacy invasion than any other generation. Popular online cyber worlds such as Barbie.com (launched 2001), Webkinz (launched 2005), and Neopets (launched 1999) are, in part, to blame. To enter these cyber worlds, children give up a great deal of personal information. And although the sites may have privacy policies, they are often difficult for children and teens to understand, as pointed out by Micheti, Burkell, and Steeves (2010).

Since Neopets was launched in 1999, millions of undergraduate students entering university now have had more than 10 years to become accustomed to giving up their private, personal information willingly. Students who “graduate” to social networking sites such as MySpace (launched 2003) and Facebook (launched 2004) might bring with them the kind of trust (or naïve commitment) they developed through their earlier online experiences and disclose more sensitive information about themselves than they realize.

Evidence points out that, while there are, indeed, savvy online “natives,” they have trouble understanding what information is true in cyberspace, as a recent report supported by the John D. and Catherine T. MacArthur Foundation indicates. Editors Andrew J. Flanagan and Miriam J. Metzger’s Kids and Credibility: An Empirical Examination of Youth, Digital Media Use, and Information Credibility (2010) shows that for young people it is where information is found that makes it credible, even if it is identical in both sources. This suggests that if a young person is asked to submit personal information on the credible sites, he or she is more likely to do so there rather than on
a site considered to be less reliable. Characteristics of credible websites include a web address (URL) that ends with a recognizable “suffix” (for example: .com; .ca; .edu). A credible website will have legitimate contact information and let the reader know its true purpose. If a site asks for payment, offers something that is “too good to be true,” or asks for more of your personal information than you are comfortable giving up, it may well not be legitimate. If your search has led you to “advertorial” opinion, and you were looking for “facts,” you may question its authority and legitimacy.

Surveillance, security, and reputation
Given that Net “natives” may not worry about the potential dangers of online activity, it is not surprising that many students in the focus groups I conducted do not worry about closed-circuit TV or other IT surveillance on campus. Their profiles and favourite behaviour are already known to the world through SNSs. Campus security at many universities plan to increase CCTV coverage to virtually blanket the campus. Are such security efforts appropriate—and do such challenges to privacy change (or control) behaviour on campus? That depends on whom you ask, as Jeffrey R. Young points out in “Smile! You’re on Campus Camera” (2003). Building on the work of James Rule from the 1970s, the Surveillance Studies Centre at Queen’s University (Kingston, Ontario), directed by David Lyon, has undertaken research on the subject on society-wide surveillance since the 1990s. In The Electronic Eye: The Rise of the Surveillance Society (1994), Lyon cites Rule as well as foundational works on surveillance, such as Jeremy Bentham’s all-seeing “panopticon” (1995), Michel Foucault’s (1995) response to it, Orwell’s 1984 (1949), and Margaret Atwood’s Handmaid’s Tale (1989), all of which have set the “standard” of fear of surveillance for older readers. Lyon is part of a research group, the Surveillance Camera Awareness Network (SCAN, based at Queen’s), that published A Report on Camera Surveillance in Canada (2009). The report analyzes the perceived need for and deployment of CCTV and, significantly, reveals the relationship between CCTV and privacy regulation.

In my courses and focus groups, students typically respond to queries about surveillance technologies by saying that if they have done nothing wrong, there is nothing to fear. But that answer is only viable in a culture of complete social stasis. If students never worsen their behaviour and surveillance remains the same, and if expectations of appropriate behaviour do not change, students may really have “nothing to fear.” So far, despite new media, behaviour has not changed much, given students’ willingness to appear in compromising situations at campus parties that later appear on CCTV, YouTube, or Facebook, situations that are potentially available forever—and are often searched for by human resources departments when graduates apply for jobs (Brandenburg, 2008).

Both provincial and federal privacy commissioners have shown their concern about SNS privacy policies and practices. In 2009, Ontario’s information and privacy commissioner, Ann Cavoukian, published a report on her website that encourages young people to “consider the ‘5 Ps’ (Predators, Parents, Professors [teachers], Prospective Employers, and Police” when they are posting messages online. Since the summer of 2009, federal privacy commissioner Jennifer Stoddart has been investigating Facebook’s privacy settings and publicizing the company’s lack of clarity in explaining how
it handles personal information. However, while privacy commissioners work to keep personal information secure, they also interpret FIPPA and PHIPA to urge the disclosure of personal health records in certain situations. By doing so, they point to some of the paradoxes inherent in the legislation.

“Healthy” disclosure

Health records are usually considered sacrosanct. However, in questions of life and death, should university officials and others attain access to personal health information? Is the privacy of a student who is of age jeopardized if health officials disclose his or her fragile psychological condition (which may portend self-harm or harm to others) to university authorities, police, or family, despite the student’s “right to be let alone”? Legislation and recent experiences on campuses make it clear that divulging such private information to persons not usually legally allowed to see it is not only possible but also sometimes required in particular circumstances, as outlined below.

At the time of writing the most significant campus incident that might have been averted by disclosing a student’s psychological condition was the 2007 Virginia Tech massacre. The Virginia Tech shooter, Cho Seung-Hui, had a history of threatening behaviour on campus. Some students, health officials, faculty, and senior administration already knew about that behaviour, but no group or individual acted on that knowledge. The administration was blamed by the media for prizing Cho’s privacy over concerns for security. But respect for Cho’s privacy, itself, was not to blame. The Virginia state governor’s Report of the Virginia Tech Review Panel points to insufficient awareness of what could have been done to coordinate campus security, health officials, and police. Section 5 of the report, “Information Privacy Laws,” says:

The widespread perception is that information privacy laws make it difficult to respond effectively to troubled students. This perception is only partly correct. Privacy laws can block some attempts to share information, but even more often may cause holders of such information to default to a nondisclosure option—even when laws permit the option to disclose. Sometimes this is done out of ignorance of the law, and sometimes intentionally because it serves the purpose of the individual or organization to hide behind the privacy law. A narrow interpretation of the law is the least risky course, notwithstanding the harm that may be done to others if information is not shared.

(Virginia, Office of the Governor, 2007, p. 63)

The treatment of health information on Ontario campuses is governed, in part, by the Personal Health Information Protection Act (PHIPA), which immediately applied to universities when it was enacted in 2004. It includes a section entitled “Disclosure,” cited here in part.

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. (Ontario, PHIPA, 2010, c. 3, Sched. A, s. 40[1])
FIPPA also includes a “Disclosures” section, which allows private personal information to be released:

(g) where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

(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;

(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. (Ontario, FIPPA, 2010, s. 42[1])

In 2005, Cavoukian made it clear how privacy should be dealt with during times of crisis in a “Fact Sheet” on the commission’s website. The “Fact Sheet” is derived directly from PHIPA. In it Cavoukian notes that “Custodians of Information” are permitted to, and may not have a legal duty to, make available personal information usually kept private, under the following circumstances. All four are relevant to Virginia Tech as well as to incidents in Canada:

1. Public Interest and Grave Hazard.
2. Health and Safety of an Individual/Risk of Serious Harm to a Person or Group.
3. Disclosures to Public Health Authorities.
4. Compassionate Circumstances [reporting to parents a student’s psychological condition, for example]. (Cavoukian, 2005)

Institutional policy and provincial and national legislation in Canada (and the U.S.), then, make it clear that “Custodians of Information” (university registrars and campus health officials, for example) are responsible for and can justify reporting impending danger to police or campus security without fear of repercussions for breaching private information.

Such disclosures apply not only to mass endangerment but also to the protection of the individual, for example, in cases such as the suicide of a Carleton University student whose body was found in Ottawa’s Rideau River in 2008 (Simons & Walsh, 2010). The student’s parents were not advised that she was taking antidepressants and speaking to a counsellor (Tam, 2008). Cavoukian, with former British Columbia privacy commissioner David Loukidelis (Cavoukian & Loukidelis, 2008), prepared a toolkit entitled Practice Tool for Exercising Discretion: Emergency Disclosure of Personal Information by Universities, Colleges and Other Educational Institutions (which cites the incidents in Ontario and Virginia, concluding that “life trumps privacy, and our laws reflect that” (p. 1; emphasis in the original). Since 1994, Ann Cavoukian and her colleagues have conducted annual educational presentations on campuses throughout Ontario. “Teaching” privacy through such policy advice and in the classroom, as suggested by students in the focus groups discussed below, would help to clarify the implications of privacy policy and disclosure.
Focus group responses
The incidents cited above and my observations of the introduction of FIPPA led me to conduct a series of focus groups on two quite different Southern Ontario campuses in 2008-09. In agreement with Parsons’ (1995) argument that “[c]ritical policy analysis advocates a fundamental and far-reaching shift towards a more open decision-making process and the empowering of citizens” (p. 444), I began with the following optimistic assumptions:

1. The legislation was perceived to be necessary by faculty.
2. Students would understand and appreciate the intention of FIPPA.
3. Given that universities are devoted to teaching and the dissemination of knowledge and the introduction of FIPPA had been carried out through a comprehensible and well-organized process.
4. Focus group participants would be well enough informed to contribute to policymaking on their campuses.

Focus group procedures
For my analysis procedure I used qualitative narrative analysis (Kaplan, 1993) to arrive at conclusions about privacy policy on campus that will lead to understanding what people know, or do not know, about the beginning, middle, and end of the privacy “story” and how to interpret their role in the story. The study included separate groups of faculty and students from two different-sized universities. I chose the participants using “known-group” sampling (Hocking, Stacks, McDermott, 2003), in which participants are all from the same group (or institution, in this case), and “snow-ball” (p. 210) sampling, in which I asked each potential participant to recommend others, until I arrived at a suitable number from a variety of disciplines (six or seven, depending on participant availability, among other considerations, according to Morgan & Scannell, 1998). However, at the larger university, where there were fewer strong ties among faculty, sending emails and approaching persons in their offices was necessary.

I adopted Maclean’s magazine terms to describe the universities:8 one is a “Primarily Undergraduate University” with approximately 12,000 students largely in the humanities and social sciences. The other is a “Comprehensive University,” with roughly 30,000 students in a variety of professional, humanities, and social science departments. I visited each campus and asked focus group members a series of questions that ranged from what constitutes “good privacy,” or “good privacy on campus,” to questions about what constitutes a breach of privacy and how they would respond to such a breach of trust. I asked whether participants have become more conscientious about their privacy since FIPPA was adopted. I also asked them whether they know how to find out about their institution’s privacy policy, and who would interpret it for them. And I inquired how engaged they are about privacy on campus. (The appendix at the end of this article lists the foundational questions; others arose as the focus groups were conducted.) From the 80 pages of transcripts, I present and interpret here some of the most intriguing or informative focus group responses.

Misunderstanding FIPPA
From my findings it became evident that the first introductions to FIPPA by the uni-
versity confused faculty and students alike. The most immediate effect for faculty was that they were required to desist from posting students’ names, numbers, or grades publicly—in an attempt to limit stalking and identity theft, for example. But many faculty members were also under the impression that they could no longer say students’ names in class, take attendance, or pass around sign-up sheets for presentations. Most faculty members had been on campus long enough to have experienced the before-and-after effect of FIPPA’s deployment. Their replies to the focus group questions reveal obvious commonalities. But faculty responses also vary, according to their disciplines, the size of their institution, and their engagement in university policy. Students in both focus groups at both universities displayed considerable naïveté about the effects of technology on their privacy. Almost all students and faculty concurred that trust and privacy are inextricably connected.

The Primarily Undergraduate University, where the first focus group was conducted, is, like a small town, inhabited by a wary, not entirely trusting population, especially of faculty, who all know each other personally. In response to the first question—“What is good privacy?”—most faculty replied that they want control of their personal information and choice about what to disclose, in keeping with FIPPA’s intentions, although only a few knew much about the legislation itself. A biologist added that she wants to control “everything emanating from me … physical, medical, blood.” In replying to question 2—“What is good privacy on campus?”—one faculty member, who had suffered personal trauma because of a careless graduate student’s public relating of their professional relationship, hoped people on campus would respect and maintain the privacy between faculty and student, as one would between a patient and client (that is, in a professional relationship one should be very cautious with “disclosures”). A librarian, who cited the RefWorks case (previously discussed), noted that the basic tenet of librarianship is to keep clients’ research and identity private. Everyone concurred with a sociologist who observed that “we are a small school in a small community … Information ‘bleeds’ off campus.”

Question 3 asked: “Think back to the last time you felt your privacy on campus was jeopardized. Did it cause you to change your privacy behaviour or ask others to change theirs? What kinds of problems did you encounter?” In answering this question, a faculty member found that damaging, threatening, ill-informed gossip about sensitive research on others’ sexuality had spread quickly around the university. When the faculty member asked for assistance in controlling the rumours, it became evident that the university did not (or would not) offer assistance to control the problem by, at least, calling for civility regarding sensitive information. Most participants recalled similar lack of confidentiality among colleagues and students.

When I asked faculty to explain their responses to FIPPA, there were universal expressions of bitter disappointment about how poorly the legislation had been introduced. As a result, there was at least a year of confusion about when it was permissible to record and disclose names in class. When asked if they knew how to obtain information about privacy on campus, only a few participants knew there is privacy information online, or in any form, at their institution. No one knew about the existence of the university privacy officer or their identity; most did not know about Ontario’s
The students at the Primarily Undergraduate University, like their faculty counterparts, all knew each other. The generational differences between the students and faculty were truly fascinating. The questions “What is good privacy” and “What is good privacy on campus?” drew virtually the same answers—as though they were both about campus. That is, to the students, campus is their life. One marked difference between faculty and students was the students’ constant but not altogether positive linkages between technology and privacy. One student, who uses Facebook and shops online, revealed her limited experience with self-disclosure reciprocity (VanLear, 1987, described above) by saying: “It’s just creepy to know somebody you don’t know knows more about you than your name.”

In response to the question “Think back to the last time you felt your privacy on campus was jeopardized. Did it cause you to change your privacy behaviour or ask others to change theirs?” two students recalled how their student debit cards were compromised but did not know what behaviour to change. A student said, “I don’t want anybody to know my student number or grades,” and another said, “When attendance sheets go round you have to write your student number … I wonder if anybody could do anything knowing my name and student number … it’s the students I’d have an issue with.” In spite of this anxiety about what other students might be able to do with their student identification, the students agreed that they trust professors with their personal information. All of the students concurred that the legislation had not been explained well. One exclaimed that “there was no pamphlet, the profs had all become annoyed about it….. Aren’t profs our guardians of privacy?” They agreed that email, pamphlets, and the student newspaper were the best ways to hear about privacy legislation, but not one student had seen a detailed article about privacy on campus published in the student newspaper not long before. Not one student wanted to navigate the university’s website to locate appropriate information, claiming the site is too confusing. Few of them knew or cared about computer privacy settings. Were these students the so-called tech savvy “digital natives” we keep hearing about? Or were these “text savvy” students who, in a way, were digital immigrants, but different kinds of immigrants than their professors?

When I spoke with faculty members at the Comprehensive University (30,000 students), I was struck by the diffuse campus culture and non-homogenous makeup of the professors and by the fact that no one knew anyone else in the group. However, they all agreed with the first participant’s statement that “[p]rivacy protects people’s private information when there’s no compelling reason that it should be made public.” The second question—“What is good privacy on campus?”—provoked a variety of replies, including a common thread of respect for others’ privacy in general. But one comment from a humanities professor that “student transcripts should be available to faculty, although no one should speak openly about grades” caused an engineer to recall that, in his undergraduate years in India, grades along with names and student numbers were announced in class. He was comfortable with that and said, “Different cultures look at privacy differently.”

In addition to diverse views on privacy, there was also a variation in familiarity
with the legislation. An English professor had independently attended an off-campus training workshop not sponsored by the university. The rest of the humanities faculty members knew nothing about the legislation. They said they would welcome a website for students, staff, and faculty, as one said, “so we can know the rules by which we are supposed to play.”

Question 7, asking participants whether they would attend a workshop about privacy on campus, prompted a split response. Three participants did not think they would have time to attend a workshop. The English professor would definitely attend because she had heard at her original workshop that privacy on campus would be driven by case law, over time. A librarian, alluding to librarianship’s “basic tenets” of privacy, agreed she would attend as well. One of the humanities professors would want to attend, to learn “more about how to respect the privacy of others.” The final question, asking what participants would like to see in a proposed website, prompted several innovative responses. The English professor suggested all Ontario campus privacy sites should be linked. The librarian suggested different types of sites for different users—“staff, faculty, students, librarians, because different users have different needs.”

I directed one last question to the engineer. “What would you do to keep other engineers from using an invention you were developing before you had it patented or on the market?” He said that, because he works with graduate students, he usually has a discussion with them about privacy and the security of research and development when they are working on a project. “There’s no ambiguity,” he said. “The whole thing about academia is to share knowledge. But there has to be a certain amount of trust [about privacy]. It’s an ethical issue.”

The student focus group at the larger Comprehensive University was composed of humanities and urban planning students. They agreed that good privacy is respect for knowing the limits of disclosing information—and how not respecting the limits could cause physical and emotional harm. The humanities students, however, were worried about how to understand the legislation more clearly. “The most private should be the default,” one student said. A humanities student also assumed that with the FIPPA legislation, “quite a lot of good privacy rules are in place.” Another presumed that “if our privacy is invaded we’ll have something to fall back on.” In replying to question 3, about their own privacy being jeopardized and changes in behaviour, one of the humanities students recalled that unknown students had invaded her residence room while she was sleeping—but, fortunately since it was no more than a prank, no harm was done. When asked if that changed her privacy behaviour, she said she would consider, at least, locking her door. Another humanities student asked, “Isn’t privacy on campus legislation about intellectual stuff? That’s huge.” And referring to the residence room incident he asked, “What about the invasion of physical space?”

Question 5 asked participants whether they had heard that legislation designed to guarantee privacy on campus had been implemented and what they would want to know about it. An urban planning student observed that “privacy is an ongoing process,” and asked what repercussions there would be if personal privacy had been violated. A humanities student asked how the legislation defines privacy, to which I replied by alluding to DeCew’s (2008) view that “there is no single definition or analy-
sis or meaning of the term.” Both students agreed that privacy is a kind of “taxonomy” based on case history, economics, and context. In other words, they observed, opinions about privacy change over time, for many reasons.

With question 6—“There are a lot of ways to get information about privacy and privacy on campus. What do you think is the best way to get that information? How would you like to get it?”—the conversation turned to technology again. One participant said that, because all students frequent websites, that would be the simplest way to access privacy information. But then she said, almost surprised, “The Internet brings another level of privacy concerns into it,” which prompted another discussion about how “tech savvy” the students felt they were. The ensuing conversation addressed concerns similar to those at the Primarily Undergraduate University about how much the students knew about the technology they use. An urban planning student reverted to the poster idea suggested at the Primarily Undergraduate University. A student in humanities insisted, “I need a personal level—someone to speak to us during frosh week or the first days of classes.” When this student was asked about her motivation to engage in privacy issues, she registered despair about Facebook. “Sometimes I wonder if this really matters because I feel people are going to find out somehow, some way, everything about you.” Most of the participants agreed that they would be motivated to follow the issue of privacy on campus if they could be convinced that privacy is a right, a concept that, as DeCew (2008) points out, is frequently challenged.

All of the student participants agreed that a website dedicated to privacy on campus should include examples of adverse repercussions of privacy violations. They wanted to know to whom they could turn on campus if a privacy breach occurred. I told them there was a campus privacy officer, as mandated in FIPPA. Not one of the participants knew about that person or office on campus.

The focus groups altered the earlier assumptions with which I embarked upon my research.

1. The legislation was perceived to be necessary by faculty.
2. Students would understand and appreciate the intention of FIPPA.
3. Given that universities are devoted to teaching and the dissemination of knowledge, FIPPA had been carried out through a comprehensible and well-organized process.
4. Focus group participants would be well enough informed to contribute to policymaking on their campuses.

As a result of the implementation of FIPPA, many inappropriate practices, such as posting student names and numbers, were ended. However, my research suggests that:

1. Some faculty had not heard about the legislation at all; most of those who had did not fully understand it; and some were still not following all of FIPPA’s requirements.
2. Students knew very little about the legislation and were quite uninformed about privacy in general.
3. The implementation of FIPPA was not organized well enough to have helped the faculty and students to understand the purpose and meaning of FIPPA and why it was deployed.

**Suggested solutions to the problem**

Below are some recommendations made by the focus group members about privacy on campus and the way FIPPA should be revisited annually. First is the problem, introduced mostly by students, regarding the simultaneous public disclosure of their name and student number. On the whole, this issue has been dealt with in sensible ways, such as disaggregating names from numbers on posted or circulated lists, although some students claimed they continued to provide unnecessary personal information out of habit. Nearly all of the students were in favour of a dedicated privacy website. The students at the “Primarily Undergraduate University” had some novel ideas about using a multimedia approach to alert fellow students to the site—beginning with a large poster of an eye, displayed throughout campus, changed periodically to gradually include text and the website’s URL.

The focus group responses also spoke to trust by faculty that colleagues and students would keep personal issues private; trust by faculty that colleagues and graduate students would keep unpublished research private; and trust by students that their professors keep their personal information private. In closing conversations, students and faculty generally agreed that privacy policy and legislation should be “taught” at some point(s) during their university career, either as part of their introduction to campus life, as formal courses, or in workshops.

Everyone wished to see a series of “clear, humane, and ethical” privacy guidelines on a website or in some other format. Most participants agreed that it is best to have well-known or “visible” privacy officers on campus to maintain discretion and be directly responsible for addressing inappropriate privacy disclosures in as limited a bureaucratic manner as possible.

The engineer’s closing words once again brought together the common thread relating privacy to trust, in legislation, policy, and personal relationships on campus—it is necessary for faculty and students to interpret privacy and surveillance in ways conducive to their own campus cultures. To reiterate the engineer’s words: “There’s no ambiguity. The whole thing about academia is to share knowledge. But there has to be a certain amount of trust. It’s an ethical issue.”

**Conclusion**

There are historic personal tendencies and institutional tensions regarding privacy regulations that may, over time, be resolved. However, it is difficult to encourage an interest in privacy in the information society without robust legislation, regulation, policies, and the willingness to “teach” why privacy is necessary and sometimes in jeopardy. Although some agreement exists about the beginnings of privacy as a social institution, the middle and end stages of the narrative are confounded by changing media and new governance strategies necessary to respond to the changes. Even the most experienced ICT users and well-informed campus populations are subject to the changing
norms of privacy—as the necessary paradox of maintaining privacy for the sake of saving reputations contrasts with breaching privacy for the sake of saving lives.

Acknowledgment
The author wishes to thank Wilfrid Laurier University for its generous funding without which the focus group research could not have been conducted.

Notes
1. The roles of federal and provincial privacy commissioners are similar but somewhat different, given their responsibilities relative to their federal and provincial legislation. See Office of the Privacy Commissioner of Canada (OPC) website.

2. Except for California and Hawaii, the United States has no equivalent state or federal commissioners, although the Federal Trade Commission informs consumers about privacy issues. Many U.S. NGOs are dedicated to privacy concerns, including the Privacy Rights Clearinghouse and the Electronic Privacy Information Center (EPIC).

3. Speaking as a policy analyst, Parsons is not referring to the Frankfurt School when he speaks of “critical theory” but is instead speaking of policy scientists such as Harold Lasswell, whose concerns include eliminating distortion in policy through rational analysis of goal-oriented actions in complex social conditions.

4. Parsons’ description, then, justifies acquiring policymaking knowledge in a variety of ways and from a variety of people. I interpreted his conclusion to include focus groups to further my privacy policy research.

5. All pending legislation being considered by Parliament dies at the end of a session, either through prorogation or any other reason for the House not to be in session.

6. Young interviewed Lauren Gelman, assistant director of Stanford University’s Center for Internet and Society, who said: “College students are at that age when they’re sort of going out exploring who they are and who they want to be … There shouldn’t be a record later in life of what is going on, and there shouldn’t be a constant surveillance state on campus” (Young, 2003).

7. The student’s death was due, in part, to advice she had received to commit suicide on an online chatroom, in what might be considered the ultimate privacy breach. Michael Melchert-Dinkel, a former U.S. nurse, was charged with aiding suicide; see Simons and Walsh (2010).

8. The stringent Ethics Research Board requirements at the two universities do not allow me to identify them.

9. Although the question might best be answered by referring to the Criminal Code of Canada, as an issue of “break and enter,” the U.K. NGO Privacy International cites such activity as a breach of “territorial privacy.” (See under “websites”)

Websites
Facebook. http://www.facebook.com
Myspace. http://myspace.com
Privacy International. https://www.privacyinternational.org
References


Appendix: Focus group questions

Privacy on campus

1. What do you consider good privacy?
2. For you what is good privacy on campus?
3. Think back to the last time you felt your privacy on campus was jeopardized. Did it cause you to change your privacy behaviour or ask others to change theirs? What kinds of problems did you encounter?
4. What helped you or would have helped you most in making changes?
5. Explain to me how you feel about the FIPPA legislation designed to guarantee privacy of personal information?
6. There are a lot of ways to get information about privacy and privacy on campus. What do you think is the best way to get that information? How would you like to get it?
7. Suppose a workshop on Privacy on Campus were held. Would you attend?
8. Many of us think it is difficult to stay motivated about issues such as privacy and privacy on campus. What would motivate you? What would keep you interested?
9. I am going to develop a Web site and information program about privacy on campus. As I begin the project what advice do you have for me?