Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

IP Videoconferencing – Issues of Privacy Awareness, Challenges, and Compliance

by

SHERMAN, C. Mooney

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: August 2009

Research advisors:

Dr. Pavol Zavarsky, Director of Research & Associate Professor,

Ron Ruhl, Director, Information Systems Security Department, and Assistant Professor

Dr. Andy Igonor, Adjunct Professor - Management Sciences

IP Videoconferencing – Issues of Privacy Awareness, Challenges, and Compliance

by

SHERMAN, C. Mooney

Research advisors:

Dr. Pavol Zavarsky, Director of Research & Associate Professor,

Ron Ruhl, Director, Information Systems Security Department, and Assistant Professor

Dr. Andy Igonor, Adjunct Professor - Management Sciences

Reviews Committee:

Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

The author reserve all rights to the work unless (a) sprecifically stated otherwise or (b) refers to referenced material the right to which is reserved by the so referenced authors.

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

Concordia University College of Alberta
Masters of Information Systems Security (MISSM) Program
7128 Ada Boulevard, Edmonton, Alberta
Canada T58 4E4

IP Videoconferencing – Issues of Privacy Awareness, Challenges, and Compliance

by

C. Mooney Sherman
mooneysherman@ieee.org

A research paper submitted in partial fulfilment of the requirements for the degree of Master of Information Systems Security Management
March 2009

Academic Advisors:
Dr. Pavol Zavarsky, Director of Research & Associate Professor,
Ron Ruhl, Director, Information Systems Security Department, and Assistant Professor
Dr. Andy Igonor, Adjunct Professor - Management Sciences

This research is, dedicated to my mom Savitri Devi Sherman for being my best friend and mother. She has always encouraged me to pursue my dreams, instilling, and helping me to develop moral and ethical values to serve humanity and for her patience during my pursuit of MISSM.

Acknowledgements

This is primarily my own research based on my experience in videoconferencing, privacy and other related laws not only in Canada but several other countries and investigations conducted by Privacy Commissioners of Alberta, British Columbia and Canada.

I would like to thank my Academic Advisors: Dr. Pavol Zavarsky, Director of Research & Associate Professor, Ron Ruhl, Director, Information Systems Security Department and Assistant Professor, and Dr. Andy Igonor, Assistant Professor - Management Sciences.

My Special thanks to Dr. Gary Hinson for his help and suggestions.

Finally yet importantly, I thank my mom, very special friends and extended family: Mildred Nault, Erwin Loewen, Rose Pileggi, my sisters, Darlene Swelin, Jana Schumacher and Laura Huddy, my Neighbors Shirley and Heinz Perrow for being there for me. Raja as well as Simba for their patience.

Abstract

Videoconferencing over Internet Protocol (IP) is a real-time, collaborative, virtual communication tool. However, current videoconferencing technology has not been built with the protection of the participants' privacy in mind. It is concerned only with the privacy of the conference session, using available techniques such as encryption. The popular use of videoconferencing has led to several compliance issues related to privacy and to the protection of the participants' personally identifiable information (PII).

The purpose of this paper is to identify the privacy risks associated with PII and to raise awareness of the challenges and shortcomings of privacy laws related to both recorded (stored) and unrecorded videoconferencing sessions. It does not address technical challenges incurred during the deployment of the infrastructure or threats to personally identifiable data/information vulnerabilities.

The research is based on the author's experience with videoconferencing while working with Alberta Learning and Alberta Education, as well as on an extensive literature review of secondary sources. This combination of sources reveals the current privacy risks to participants' PII and the challenges to organizations to mitigate these risks. By analyzing the technical, legal, and policy issues involved with videoconferencing, it also identifies the challenges of compliance with the *Privacy Act* [1] in order to ensure that the protection of participants' PII is consistent with the law.

Key Findings

This paper provides recommendations for participants, organizations, and system administrators. Finally, it emphasizes the need for further research. It supports three key findings:

There are compliance concerns. Compliance with the current privacy laws can be challenging in Alberta especially when videoconferencing sessions are recorded.

There are challenges. The current privacy and paramountcy laws [11] make it challenging for organizations to obey privacy laws while participating in a videoconference session unless it is within the organization. Even if the session is not recorded, inter-organizational sessions disclose the participants' PII to third parties. This contravenes Alberta's *Freedom of Information and Protection of Privacy Act* (*FOIP*) [2] unless there is informed participant consent.

There is a need for awareness. Each affected individual must be aware that his or her consent is required by a public body for the collection, use, and disclosure of PII. Informed participant consent cannot be obtained or validated without knowing the identity of the authority; the purpose of all the involved organizations' use, access, and disclosure; and the compliance of such organizations—and the sessions—with applicable laws.

Although the research examined videoconferencing privacy issues in Alberta, many if not all of the above key findings are also applicable globally to any jurisdiction.[1]

[1] Note: In the following discussion, "section *X*" indicates a section in an Act; "s. *X*" indicates a section within this research paper.

1.0. Introduction

Internet-based videoconferencing is becoming increasingly prevalent with the widespread implementation of high-speed Internet in business, government, health, and educational settings. No one can deny the vast benefits of videoconferencing for organizations, people, and the environment. Students have new ways to gain valuable educational information and experiences. Other industries are trying to lower costs, as well as implement business models that use e-services to expand markets to remain competitive and sustainable. These developments have involved a greater use of videoconferencing as a communication tool—an economical and ecologically friendly technology that reduces travel budgets and carbon emissions.

The use of videoconferencing however, does not come without issue. There is a high risk of potential to impact privacy. If an individual or group of individuals is impacted by a breach of privacy, the effects can be alarming and long lasting. Organizations risk losses that could be revenue-based, reputation, undermining of confidence, not only with their clients and staff, but amongst all industries.

The author acknowledges that there are technical challenges during the deployment of videoconferencing technology, such as bypassing or opening ports in the firewall. This paper does not address PII data, vulnerabilities, threats during transmission (e.g., from man-in-the-middle attacks etc.) or threats from a failure of some security mechanism within the organization such as hacking, stolen or lost equipment, poor process, or during storage on other media. It also does not address vulnerabilities, threats, and the impact of several protocols used in videoconferencing (e.g., transmission control protocol/internet protocol (TCP/IP) or the softwares involved (e.g., the applications, device software (router, videoconferencing end points etc.). It also does not address threats from disgruntled employees. All of these are beyond the scope of this paper.

In summary, the paper enumerates the Alberta legislation requirements, their applicability to videoconferencing over IP, and the current status of compliance, and identifies the following considerations:

- Awareness of protection of risks to PII requires an integrated approach that involves the organization, system administrators, and videoconferencing participants regardless of whether the session is stored. This includes the need for the participants' awareness of risks to their PII so that an informed consent can be provided; for organizations/system administrators to ensure that the authority to collect/disclose the participants' PII—its purpose, intent, and use—is clearly conveyed to the participants; and for the organizations/system administrators to conduct a Privacy Impact Assessment (PIA) to obtain participants' informed consent.
- Challenges for the organizations include compliance with the *Privacy Act* [1] and technical challenges during the videoconference session.
- Challenges for the participants include knowing how, where, and by whom their PII is being accessed/used, why it is being used and/ disclosed, and by and to whom their PII is being disclosed.

Finally, the paper provides recommendations to improve privacy protection for participants in videoconferencing. It also provides recommendations for the organizations and system administrators to mitigate the challenges involving privacy, compliance, and protection of participants' PII when using or participating in videoconferencing.

2.0. Legislation and Research

As the research shows, a videoconferencing session must be protected under appropriate privacy legislation.

2.1. Scope

The specific legislation examined is *Freedom of Information and Protection of Privacy Act* (*FOIP*, Alberta) [2] and *FOIP regulations* [3]. *FOIP* [2] is similar to the other provincial privacy Acts for the public sector, to private sector legislation in Alberta including Alberta's *Personal Information Protection Act (PIPA)* [4], and to federal legislation for the private sector including the *Personal Information Protection and Electronic Documents Act (PIPEDA)* [5]. Therefore, many of this paper's conclusions have direct relevance to private sector videoconferencing both in Alberta, across Canada as well as globally.

This is the first research study of its kind that addresses privacy risks for individual participants and compliance challenges for organizations engaging in videoconferencing sessions. Consequently, it was difficult to find literature pertaining to this topic (see Appendix A). The literature review was in four broad areas:

- Privacy law: the relevant subsections of *FOIP* [2], paramountcy laws, investigations conducted by the Office of the Information and Privacy Commissioner, Alberta (OIPC) [6], and other related articles
- A brief review of the Alberta public sector (see Appendix B.)
- Current privacy practices in videoconferencing (s. 5.4)
- An analysis of Privacy laws and videoconferencing in Alberta

The research is based on the following sources:

- *FOIP* [2], including *Regulations* [3]
- *Canadian Institute of Chartered Accountants:* Generally Accepted Privacy Principles (GAPP) [7] (a universally accepted standard—see 3.2 below)
- Statistics and analysis of investigations conducted between 1997 and 2008 by the offices of the privacy commissioners in Alberta [6] (see Appendix C)
- Various studies by graduate law students that were funded by the federal privacy commissioner [10]
- Paramountcy laws in Alberta [11] (See Appendix D)
- A review of 78 public sector websites for the authority to collect PII, as well as posted policies for its use, disclosure, retention, and destruction. Appendix B provides a complete list of these, and the results are discussed in s. 5.1.
- "VC Alberta," a basic online videoconferencing resource for Alberta [12]
- Privacy surveys [13, 14]
- Personal observations during the author's tenure at Alberta Learning and Alberta Education (2000 −2007).

Currently, non-compliance with the *Privacy Act* [1] for videoconferencing is likely a result of insufficient awareness of the need for privacy protection. However, before discussing this, it is important to understand the application of videoconferencing in Alberta.

3.0. Videoconferencing in Alberta

In Alberta, videoconferencing is being rapidly implemented with the acceptance of the technology and its viability for deployment since the completion in 2005 of the Alberta SuperNet, a provincial multiprotocol label-switching network. It enhances and improves the efficiency of organizations with limited resources and expertise, especially those in remote communities. Alberta's videoconferencing over IP standard is *H.323* [15].

3.1. Sponsored by the Government of Alberta

In health, telemedicine, patient monitoring, counselling, and consulting services are available to patients and clients regardless of their location. There is also a strong potential for opportunities in telesurgery.These provide greater efficiency and cost savings due to the reduction in the need for patient transfer to larger urban centers.

In law enforcement, some of the current applications of this technology include protection from dangerous criminals while they appear in court when the safety of a witness or the public is a concern, consultation of an accused with their counsel, and hearings between a judge in court and an inmate who remains in detention.

In education, both K-12 and post-secondary institutions have implemented videoconferencing. Alberta is recognized as a leader in this technology and its integration [16] in the K-12 public and separate school systems. Post-secondary institutions use it for the delivery of distance learning to remote community learners as well as for collaborative activities.

Other ministries are using videoconferencing to share information, consult, and collaborate with their stakeholders and counterparts.

3.2. Local, National, International Context of Privacy Laws

Organizations in Alberta must ensure that they comply with the privacy protection legislation for videoconferencing. They must also consider how the other organizations and jurisdictions both nationally and internationally will protect the privacy of PII in a multi-territory videoconference-over-IP session. The majority of privacy principles globally are based on ten interrelated privacy principles of the Canadian Institute of Chartered Accountants, which are called Generally Accepted Privacy Principles (GAAP) [7]. However, there are differences in how the privacy laws are enacted, implemented, monitored, and enforced, since these are dependent on the political, societal, religious, and cultural environment. The logical step toward achieving universality of privacy protection of PII would be to develop an international standard for privacy protection of individuals whenever PII is shared.

3.3. Privacy Compliance in Alberta

Compliance with privacy Acts is a mandatory requirement in Alberta for all public bodies and private-sector organizations to protect the PII of individuals. All public bodies in Alberta that either have custody or are in control of PII must comply with section 4 of *FOIP* [2] (with some exceptions such as personal note, draft decision etc., of judicial or quasi-judicial capacity) which is discussed in the next section. These include all departments, health providers, libraries, municipalities, law enforcement agencies, and educational institutions fully funded by government. All other organizations must comply with *PIPA* [4] or *PIPEDA* [5]. All of these bodies and organizations must limit the collection of PII to its intent. PII should be destroyed when it is no longer required by sections 5(a), (b) and section 35 of *FOIP* [2] or as directed by paramountcy law[11].

3.4. FOIP Act of Alberta: Protection of Personally Identifible Information in Public Sector

Policy on the protection of PII in the Alberta public sector is based on the Model Code for the Protection of Personal Information [17]. The Model Code is the basis for most provincial protection of personal information legislation as well as for the federal *Privacy Act* [17] and *PIPEDA* [5].

The purposes of *FOIP* [2] are stated in section 2 of the Act:

a) to ensure and contol the public right to access an individual's records in the custody of a public body;

b) to control the manner of collection, use, and disclosure of PII by a public body;

c) to allow and control an individual's right to access their PII in the custody of a public body;

d) to allow individuals their right to request correction of their PII held by a public body;

e) to provide for independent review of decisions made by a public body and resolution of complaints.

3.5. The Scope of The Freedom of Information Protection of Privacy Act (Alberta)

The scope of *FOIP* [2] is defined in section 3. The section that affects the purposes of this paper is 3(e) which controls but does not prohibit access, transfer, storage, and destruction of personal information. Section 33(a) ("No personal information may be collected by or for a public body unless the collection of that information is expressly authorized by an enactment of Alberta or Canada") subordinates *FOIP* [2] to a number of industry-specific paramountcy laws [11], listed here as Appendix D. If there is any conflict between these laws and the provisions of *FOIP* [2], the provisions of the paramountcy laws [11] prevail.

4.0. Methodology

The methodology consists of an extensive literature review, the key findings (see Appendix A), and a modified privacy impact assessment (PIA) (see Appendix F). The modification of PIA was necessary to address the videoconferencing sessions specifically as the original PIA could not adequately address or provide for the considerations for a participant or multi-organizations.

The purpose of the literature review is to assess technical and operational compliance and policy challenges of information about videoconference sessions for awareness of and compliance with *FOIP* [2]. All privacy breach surveys currently available on the Internet (in English) were examined. The key finding was that these surveys are not granular enough and do not categorize PII breaches by the application or the technology used. Therefore, current published data specific to videoconferencing PII breaches does not exist.

The modified PIA of videoconferencing was used to identify the risks (i.e., threats to PII) it has been posing (see s. 5.5). The assessment included identification of elements in videoconference session information and *FOIP* [2] requirements; of the current level of awareness of videoconference session information, and of the current status of compliance, and determination of the applicability of *FOIP* [2] and the authority to collect/disclose PII.

5.0. Analysis of Privacy Awareness, Challenges and Compliance for Videoconferencing Session Information

The analysis of awareness, challenges, and compliance of videoconferencing with the *FOIP* [2] was done extensively through discussion and other tools[2].

5.1. Awareness of Videoconferencing Session Information

Awareness of any risk assessment for PII of any IT solutions should include organizational, information security professionals, system administrators, and data owners. Although this is not done presently, for videoconferencing, it should also include participants' PII risk consideration, so that they can be appropriately informed.

There are no privacy compliance issues with multiple locations within a single organization for videoconferencing, regardless of whether the sessions are recorded, and provided the organization has the informed consent of the participants and use of the content is contained within the organization. If the session is being recorded, the organization will also require the authority under *FOIP* [2] to collect the PII. Assuming that informed consent and proper authority has been identified it is still necessary to implement appropriate access controls.

However, in multi-organizational videoconferencing, organizations need to be aware of how the multi-organizational, national, and trans-national videoconferences can impact the risks to compliance with privacy laws and to the participants' PII. This applies whenever the session is recorded and stored unless it is a public event.

Although awareness of the risks of videoconferencing to participants' PII is not presently made a great concern, it should be so that they will be appropriately informed. Participants in videoconferencing need to be aware of what PII they are disclosing. This seems like a simple and fundamental step. However, without specific consideration, it can be easily overlooked.

5.1.1. Pesonally Identifiable Information at Risk in a Videoconference Session Information

Videoconferencing sessions typically contain all the visible biometric characteristics and some characteristics from the other categories such as intellectual and personal information. Table 5.1 below identifies and categorizes the possible data elements of the PII of a participant in a videoconference session.

Personal Identifiable Information		
Biometric Information	**Intellectual Information**	**Personal Information**
Facial characteristics	Personal opinions	Name
Facial expressions	Personal beliefs	Place of employment
Iris	Personal religious beliefs	Location
Fingerprints	Personal political beliefs	Date of birth (implied)
Movement	Business-related information	Other personal information e.g. an anniversary (implied)
Physical disability	Confidential information	Personal information about family members
Mental disability	Sensitive information	Personal information about friends, colleagues, etc.
Racial/ethnic origin	Strategic information	
Voice	Proprietary information	
Tattoo, scars, birthmarks	Copyright material	

[2] The reader is encouraged to refer to the appendices for details of the information in this section to get the most out of this research.

Table 5.1: Participant's Videoconference Session Information

5.1.2. Applicability of the Freedom of Information and Protection Act to Videoconference Session Information

Section 1(q) in *FOIP* [2] (Alberta) defines a *record* as "a record of information in any form and includes notes, images, audiovisual recordings … photographs, … that produces records …[18]".

The act is applicable to any record that is in the custody or control of a public body Section 96 of FOIP [2].

Section 1(n) in *FOIP* [2] (Alberta) defines *personal information* as "recorded information about an identifiable individual, including [but not limited to] the individual's name, home or business address or home or business telephone number, ... race, national or ethnic origin, … fingerprints, other biometric information, … personal views or opinions, except if they are about someone else [19]."

In numerous investigations, the privacy commissioner distinguishes between public and private space (domain) within the public sector. The information in these two sections and from Table 5.1 leaves little doubt that the contents of a videoconferencing session, when disclosed, recorded, or stored on any media, must comply with *FOIP* [2] if the session is in the private domain of a public body. A private domain of a public body can be defined for the purposes of *FOIP* [2] as one where the contents are only available for use within the organization. For example, a classroom in a school is considered a private domain; a public event is a public domain, and its contents are available to anyone, internally or externally. However, the information in the public domain still must be protected similarly to any other information of the organization. It is important to realize that individual participants' PII is being disclosed regardless of the domain of the public body.

In videoconferencing sessions between multiple organizations (in the private domain, recorded or not), such disclosure contravenes the disclosure criteria of *FOIP* [2], section 40, unless the participants give their informed consent.

Furthermore, if the videoconference session is recorded in Alberta, an individual's permanent record is created and it must comply with *FOIP* [2].

5.1.3. Current Status of Protection of Personally Identifiable Information in Alberta for Videoconference Session Informtion

Most people are accustomed to participating in meetings, inter-organizational events, and seminars with very little thought or concern for PII protection. However, virtual meetings such as videoconference sessions require careful consideration for personal privacy protection especially when the session may be recorded. This is because of the potential of PII becoming a permanent record and being in the custody of external organizations. It means that the individuals are no longer in control of their PII. It is very difficult, if not impossible, for organizations/users to be accountable for the PII contained in videoconferencing sessions. The risks of compromise of PII are increased dramatically when it is stored in multiple locations.

Use of a videophone in an organization is similar to participating in a videoconferencing session; both transmit PII as defined in *FOIP* [2]. Users need to be aware of the risks to their PII, since it may be shared with other organizations within Alberta, nationally, or internationally, users of both technologies should be aware of the risks to privacy in order to make an informed decision. This includes organizations, which should obtain an informed consent in compliance with *FOIP* [2]. McLennan Ross, an Alberta law firm [23], sent a videophone alert of potential abuse of the individual's privacy to all school boards. Similar alerts for videoconferencing do not appear to have been raised.

An example of one attempt to initiate a detailed policy on the deployment of videoconferencing in healthcare is the Alberta Ministry of Health's "Telehealth Videoconferencing Technology Standard [24]." However, it deals with the security of the network, infrastructure, and patient healthcare records from the perspective of the organization. It does not address the additional personal information collected in a videoconferencing session that it would or would not collect as part of the health record if it were from "in-person" care (the patient is in the physical presence of care providers), e.g., additional biometrics and nonhealthcare-related personal comments / opinion exchanges from the patient, consultant, and other staff present.

The requirements for authority for the collection of PII are outlined in section 33 of *FOIP* [2].

In the research, 78 organizations' website were visited to determine the authority to collect PII, disclosure policy, and the use of the records of the individuals served (or employed) by reviewing the posted policies (see Appendix B). For instance, in the case of school boards, the authority to collect PII is defined in the *School Act* (*Alberta Regulation 225/2006*) [20] under student records (section 23) and employee records (sections 33 and 34(2) of *FOIP* [2]). Similarly, other paramountcy laws for public bodies (see Appendix D) define the collection/disclosure of PII.

Paramountcy laws generally limit the collection of PII to the specific parties the laws are intended to actually serve, such as employees, third parties, and stakeholders. For example, in the *School Act* [20] there is no reference to the collection or sharing of biometric information and other PII such as some health information about employees and students, including visible or implied disabilities (Table 5.1) amongst other organizations. Videoconferencing session can be recorded with or without the consent of an organization or the participants. Some biometric information is not secret, however, when it is recorded, it becomes an individual's PII record with a potential susceptibility to threats. The threats include unauthorized access, disclosure, misuse, and abuse. Videoconferencing session information can be recorded with or without the approval of an organization or the participants.

There are two key findings here: One is that there is a need for implementation of appropriate controls for videoconferencing within an organization. Although it currently may have a low potential for threats, this may change as videoconferencing and the gathering of biometric identification become more prevalent. The second, is that generally no authority for inter-organizational holistic PII collection/disclosure is revealed in videoconferencing. Examples of some exceptions would be law enforcement, public safety, and national security. (See Appendix E).

It can be concluded from the above that perhaps the lack of awareness or understanding of the collection/disclosure of videoconferencing session information exists at all of the organizational, system administrator, and participant levels. Further support for this conclusion is also to be found in VC Alberta [12]. VC Alberta [12], a project funded by Alberta Education, is a central resource for the K-12 education sector's videoconferencing community. VC Alberta [12] has plenty of advice for a videoconference: what to wear, how to prepare, scheduling, etiquette during the session, the pedagogy to use, and best practices for a successful session, etc. However, there is nothing on PII awareness or concerns for compliance with *FOIP* [2] or other privacy laws. Again, the absence is likely attributable to a lack of awareness. Finally, this conclusion is further supported by the following facts about the legal position of a public body in regard to videoconferencing:

- It has no authority to collect PII from individuals it does not serve (Appendix E).
- It has no authority to disclose to other organizations the PII of participants it does serve unless it has informed consent from the participant, with some exceptions, such as law enforcement, etc. (Appendix E).
- Some of the websites reviewed (Appendix B) specifically express privacy concern for video surveillance [21] and cell phones [22], and have policies for them.
- There is a general lack of policy specifically for videoconferencing (Appendix B).

It is difficult to conclude that all public bodies are discarding or ignoring the legislative requirements when they organize or participate in videoconferencing sessions, especially when their history of compliance is considered (see Appendix C). Therefore, one possible explanation is that, once again, the non-compliance is likely due to a lack of awareness and understanding of the elements of videoconference session information and its unique requirements for privacy protection. This may be because the videoconference is perceived as just another tool for communication, like email or the telephone. The difference is that videoconferencing discloses a holistic PII (see Table 5.1). Hence, a lack of awareness exists.

To appreciate the complexity of compliance with videoconferencing session information, it is necessary to be clear about the challenges. The next section examines these, in the context of a single organization first, and then in the context of multiple organizations.

5.2. Challenges of Videoconferencing Session Information to the Security of PII

Videoconferencing challenges to the security of PII need to be addressed in the context of the type of videoconferencing sites involved: a single organization in multiple locations, multiple organizations in the same country, and multiple organizations in multiple countries.

5.2.1. Protection for the Participant from Threats to Personally Identifiable Information

In order to make an informed decision about participating in a videoconference, and during the videoconference itself, a participant should require satisfactory information in answer to the following questions:

- What PII will be disclosed?
- Can the disclosure of PII be limited?
- Has the public body provided sufficient information in terms of the purpose, intent, and use of PII to provide an informed consent?
- If not what else is needed?
- Is the information being recorded?
- If yes, who will be recording it and why?
    - How and where will it be stored?
    - Who will have access within the organization?
    - Who will it be disclosed to?
- If not, what steps are being taken to mitigate unauthorized recording?
- How will access be provided to the participants?

5.2.2. Protection for the Organization from Threats by Participants

An organization that initiates a videoconference should protect itself from recrimination by participants by obtaining satisfactory information in answer to the following questions:

- Is there an informed consent from the participant?
- Is the videoconferencing session being recorded? If yes then:
    - Who is the data owner/custodian?
    - How will the PII be protected?
    - Are there appropriate security policies and controls in place?
    - How and where will it be stored?
    - Who will have access within the organization?
    - What steps can be taken to mitigate unauthorized recording?
- How will access be provided to all the participants?
- Who will disclose, and to whom and how will the PII of an individual be disclosed, since it is in the aggregate records of multiple participants and possibly multi-organization and multi-nations?
- Who will correct inaccuracies and how will that be accomplished?
- How long will the information be retained?
- Who will destroy the PII and by what means?
- Is there a legal requirement to inform all PII owners in case of privacy breaches? If so, how will it be addressed in a multi-organization and multi-nation context?

5.3. Compliance of Videoconferencing Session Information

This is a complex area for videoconferencing. When the *Privacy Act* [1] or the *FOIP Act* [2] was written and amended, it did not consider the broader picture of the extent to which multi-organization and multi-national (distributed environment) collaboration resulted in the sharing of PII.

5.3.1. The Freedom of Information and Protection of Privacy Act and Paramountcy Laws in Videoconferencing

This section discusses when *FOIP* [2] and paramountcy laws [11] apply. section 5 of *FOIP* [2] states that the Paramountcy laws [11] prevail over *FOIP* [2]. *FOIP* [2] compliance requirements include obtaining the following information:

- Authority for the collection of PII
- Purpose of the collection of PII
- Informed consent for the collection of PII from the individual, trustee, or guardian or parent
- Use of collected PII
- Access of PII
- Disclosure of PII
- Third party access, storage, and disclosure
- Storage of PII
- Accountability of PII in its custody

The exception to this is when the retention and destruction are specified in other legislation for the specific industry as stated in section 3(e) or if none exist then as per section 35 of *FOIP* [2].

In addition, if other elements of the compliance are also defined in the paramountcy laws, then specifically the *Regulations* [3], sections 15-17 apply.

5.3.2. Determining the Authority for Collection of Personally Identifiable Information

In Alberta and Canada, a public body is required to determine whether it has the authority to collect PII through a legislative enactment. This also applies to videoconferencing. The determination of authority should be applied to all the participating sites; this requires addressing the following concerns:

- Do all the videoconferencing sites belong to a single public body?
    - Are all the sites in Alberta?
    - Are all the participants employees and/or individuals it serves?
    - What is the authority for collection of PII?
- Do the videoconferencing sites belong to multiple public bodies?
    - Is this videoconferencing in the public or private domain of the public body(ies)?
    - Does this require informed consent by the participants?
    - Are all the sites in Alberta?
    - Are some of the sites in other parts of Canada?
    - Are some of the sites in other countries?
    - Are all the participants employees and/or an individuals it serves?
    - What is the authority for collection of PII from multiple organizations?
- Do some of the videoconferencing sites belong to multiple public bodies and/or private bodies?
    - Is this videoconferencing in the public or private domain of the public body(ies)?
    - What is the authority for collection of PII?

5.3.3. Defining the Purpose (Intent) for Collection of Personally Identifiable Information

Privacy Protection under *FOIP* [2] ideally requires addressing the following questions for each videoconference session:

- Is there authorization to collect the PII of the participants at all sites involved (paramountcy law or federal law)?
- Does the disclosure of PII meet *FOIP* [2] criteria?

- Is it in a private domain or a public domain of the public body? It will depend on the intent, but if it is in the private domain of the public body then, it must comply with *FOIP* [2].
- What should be done when one of the sites is not a public body? *FOIP* [2] Investigation [6] deals with a public body and a private body that is operating in Alberta but is headquartered in the USA. If the private body was just operating in Alberta or within Canada, *PIPA* [4] or *PIPEDA* [5] respectively would apply to it, while *FOIP [2]* would apply to the public body. In this case, the private body's head office is in the USA and therefore Canadian Privacy Acts do not apply to the information stored in the USA. *FOIP [2]* does not specifically address this in the international context. Therefore, for international context it will be necessary to evaluate specific country's laws to determine the impact if sites are located outside Canada.
- Do other jurisdictions have similar definitions of public and private domain within the public bodies? This is dependent on the province/state or country.
- Are the requirements for protection of privacy also similar? Within Canada, they should be; however, this may not be the case internationally.
- Do all organizations involved in the videoconference have the same intent?
    - If not how should this be addressed?
- Do all organizations involved in videoconference have similar security policies and appropriate security controls?
    - How will it be determined?
    - If not, how should this be addressed?
- Do all organizations involved in videoconferencing have the informed consent of the participants?
    - Should the organization require copies of consent from the participants at all sites?
    - Should the organization require a confirmation from the participating organizations that they have the necessary consents from all the participants.
- Are any or all organizations involved in videoconference recording the session?
    - If yes to the two questions immediately preceding, who is the data owner/custodian?
    - How will it be used?
    - How will it be stored?
    - How long will it be retained?
    - Who will have access?
    - To whom and how can it be disclosed?

Additional compliance questions when considering the participation in a videoconference are presented in the next section.

5.3.4. Compliance Challenges for Personally Identifiable Information

There are numerous legal implications for the organization from both the organization's and the individual participant's perspective:

In cases where all sites in a videoconference session may fall under the public domain of the public body, *FOIP* [2] does not apply because this is considered a public event. However, there may be issues surrounding the general protection of intellectual property such as copyright (if copyrighted or pending copyright material is used) and the participants' own ideas, opinions, and artistic creations. It is important to recognize that the risks to the PII of the individual participant do not diminish just because it is in a public domain of the public body.

In cases of multipoint videoconferencing, an organization may not have authorization through its paramouncy law to collect or disclose PII or have informed consent from individuals at remote sites.

In cases where confidentiality is a concern, the transmission of PII across the Internet poses in-transit vulnerabilities and threats.

In cases where all sites in a videoconference session fall under the private domain of the public body, *FOIP [2]* issues must be addressed.

In cases where some sites in a videoconferencing session fall under public domain while others fall under private domain (in the public body context), for example, one organization may collect the PII for promotional purposes, the other for use within its own organization. Disclosure under *FOIP* [2], sections 40 and 17, will still apply. Since neither the provincial *FOIP* [2] nor the national *Privacy Act* [1] addresses this mix, how should it be addressed?

5.3.5. Policy Challenges for Personally Identifiable Information

Appropriate policies, implementation, and enforcement for access and disclosure are necessary to ensure due diligence in an organization's security framework and management.

Although disclosure of PII that is not recorded is not an issue in Alberta, it may be in other jurisdictions. In Alberta, privacy issues for videoconferencing sessions are only applicable to a permanent record of PII—hence, to recorded sessions—whereas this may not be the case in other jurisdictions. For example, when sessions are exported, some jurisdictions require a license (e.g., New Zealand) while others specifically prohibit export of PII (e.g., Sweden).

Regardless of this, it is important to realize that disclosure and perhaps collection of individual participants' PII may occur. The risk to the PII of participants in both the public and private domains of the public body is the same.

5.4. Current Compliance Practices for the Protection of Personally Identifiable Information in Videoconferencing

A review of current privacy policies in Alberta organizations in Appendix B, *FOIP [2]* and *Regulations* [3], paramountcy laws [11], and other research as discussed in previous sections shows that they do not address the unique requirements of videoconferencing session information for the authority for collection, intent, consent, retention, storage, disclosure, or destruction. This section examines that situation in more detail.

Most public bodies do not appear to have the authorization to collect the PII for persons they do not serve (see Table 5.1). There are some exceptions, but only if the videoconferencing session(s) can be justified under section 33(c) of *FOIP* [2].

Defining the permitted use of videoconference session information can be challenging when one or more external organizations are involved, and they may or may not be located in Alberta (as discussed in previous sections). This is because an organization has no way of knowing whether the sessions are being recorded and how the other organizations will use the information. Section 39 of *FOIP [2]* sets out the use of PII.

Public bodies do try to comply with the privacy legislation in Alberta, however, there is room for improvement as evidenced by the fact that the number of complaints lodged annually to the privacy commissioner of Alberta has not declined, but rather has been consistent since 1997 (see Appendix C).

5.4.1. The Private Sector

A brief look at the private sector is warranted here because some of the videoconference sites may be in the private sector. The Canadian Internet Policy and Public Interest Clinic conducted one study, funded by the privacy commissioner of Canada, "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up? [25]." It concluded that the majority of privacy policies of organizations (online shopping, etc.), do not comply with the *Privacy Act* [1]. It is likely the same in other areas of compliance with privacy protection. Privacy protection procedures do not address the risks involved when PII is transmitted over the Internet.

In informal discussions with some of the videoconference organizers and moderators, it was apparent that they receive training in using the videoconference technology. However, the organizers, system administrators, participants, and moderators were not trained in the privacy risks, compliance, and potential abuses of PII.

Alberta organizations, especially in the education sector, often engage in trans-national videoconferencing sessions. There may be other silent stakeholders involved that are not obvious or identified. The silent stakeholders may have the legal authority through other legislation (e.g., anti-terrorism laws) to potentially intercept communication or redirect a copy of the information being transmitted to collect, retain, store or disclose it to a third party. This is apparent from the 37 class-action suits against internet service providers in the USA by a former employee of AT&T, as reported in the broadband report "Mr. Klein Goes To Washington [26]."

Potential liabilities from situations like these have also not been addressed so far, although this is understandable since there is a lack of awareness and understanding of the elements of videoconference session information (as discussed earlier). Problems may also arise if the videoconference session information is intercepted for ethnic, political, or religious profiling. Although such a case has not yet surfaced or at least been identified as such for videoconference session information, there have been a few cases where inaccurate information about individuals collected by law enforcement was shared with other foreign intelligence organizations. As in the example of Maher Arar [27], the consequent personal inconvenience and distress to the victim resulted in a settlement of great cost to the taxpayers of Canada. An article entitled "Why are so many individuals singled out when they travel? [28]" brings to light a number of examples of select profiling.

Privacy impact assessments (PIAs) [29], if at all conducted, are from the perspective of the organization rather than of the participants, either in the preliminary stages or during the various stages of the videoconference project. Public bodies are encouraged to conduct PIAs, but it is not a mandatory step for public bodies in Alberta except in the healthcare sector under the *Health Information Act* [30].

OIPC Alberta [6] maintains a registry of accepted PIAs from all public bodies. This registry has 1204 PIAs [31] as of the writing of this paper. Only one PIA for videoconferencing from Capital Health [31] was accepted in 2002**,** prior to the deployment of videoconference over IP. In March of 2008, a second PIA was accepted from the David Thompson Health Region [32], in which a single student (patient), school staff, and perhaps technical staff and health professionals may be involved in a given videoconference session. Although it is a multi-participant videoconference, it involves a single participant that the organizations jointly serve.

5.4.2. The Public Sector

All public bodies are connected in Alberta through Alberta SuperNet [33]. Therefore, one of the options for connectivity between the health provider and the school jurisdiction would be to use a separate Multi-protocol Label-Switching (MPLS) Virtual Local Area Network (VLAN) on Alberta SuperNet. This has the advantage of ensuring that the information remains within Alberta during the transmission, thus reducing some of the in-transit threats.

It can be further shown from the literature review of *FOIP* [2] investigations [6] that if there is no informed consent, then the collection, retention, storage, etc. of personal information are also not in compliance. In addition, public bodies must have the authority to collect PII under the industry-specific paramount law that takes precedence over *FOIP* [2]. For instance, currently, the Alberta *School Act* [20] authorizes only the collection of PII to its employees and the students it serves (enrolled), including their parents/guardians. Therefore, if two Alberta school boards participate in a videoconferencing session and record it, they will not comply with *FOIP* [2] (authority to collect PII of individuals, the organization does not serve). This is also true for disclosure of PII, and therefore it will not comply with section 40, *FOIP* [2]. However, some provinces (e.g. British Columbia) even limit storage of and access to PII to within Canada [8], so trans-national videoconferencing will be a challenge for compliance.

It has been demonstrated in this section that, overall, public bodies do not comply with *FOIP* [2] for videoconference sessions when they are recorded, and compliance under the current *FOIP* [2] is challenging. A number of issues concerning trans-organizational and trans-national videoconferences need resolution in *FOIP* [2] in order for the organization to remain compliant with the legislation.

5.5. Privacy Impact Assessment

The PIA process is similar to a continuous risk management approach and includes planning, analysis, and education (awareness). In the case of videoconferencing, the sites are always changing and therefore it is necessary to emphasize the importance of conducting a PIA for each videoconference session. However, this is not practical due to the limited organizational resources and therefore a compromise is necessary by conducting PIA for typical scenarios that are relevant to an organization.

PIA consists of four core components: project initiation, data flow analysis, privacy analysis, and a privacy impact analysis report [35].

This research paper deals only with project initiation because the other three core components will be organization-specific.

The next section uses a modified PIA to demonstrate the importance of this.

5.5.1 Project Initiation

The project initiation component of the PIA process helps organizations to determine whether basic privacy requirements and policies continue to meet compliance, especially when new technologies, information systems, initiatives, proposed programs, or changes in delivery method of a program are deployed. It also assists an organization to anticipate the public's reaction to any privacy implications of a proposal, and as a result, helps in preventing costly program, service, or process re-engineering.

The checklist (Appendix F) shows the results of the videoconference-over-IP project-initiation modified PIA checklist, based on the Government of Canada checklist [36]. Appendix F demonstrates that it is necessary to conduct a full PIA [37,38] from the participants' perspective by each organization before deploying videoconferencing (because of the the use of more intrusive method of delivery and if it is recorded then additional PII is collected).

5.6. What Needs to, be Protected?

To comply with *FOIP* [2], all PII of participants in a videoconference session needs to be protected by a public body. However, this will be determined by whether it is recorded and whether it is in the public or private domain of the public body.

5.7. Results of Analysis

There is a lack of awareness of the vulnerability of information at videoconferencing sessions by both organization/system administrators and participants (s. 5.1) and numerous challenges to compliance with privacy legislation (s. 5.2).

Videoconferencing technology is relatively new. The ramifications and potential liability of PIA misuse is a risky unknown. Compliance for the use of this technology for communications still in it's infancy at best. Videoconferencing is introducing a whole array of possible risks that require consideration, scrutiny, review and new guidelines for compliance, to protect the participants and and organizers (all industries), particularly in cross-organizational, and international use.

In a single public organization (body) with multiple locations (in Alberta), a videoconferencing session is in compliance regardless of whether it is being recorded. The assumption is that all information is stored and located within a single organization as well as that participants' informed consent has been obtained.

In a multi-public organization within Alberta, a videoconferencing session is in compliance if the session is not recorded and an informed consent is obtained. In the case of the K-12 sector, the consent would be required from parents/guardians because the participants are under the age of consent.

Using the current PIA toolkits [35, 36] can be a challenge for controlling videoconference session information and hence the use of modified PIA in the previous section. The current PIA [35, 36] does not adequately address videoconference sessions information. The assumption is that all information is stored and located within a single organization. This may not be the case with videoconference sessions. Organizations have no control over what the other organizations may be doing—recording or not recording.

In a multi-territory, multi-organization or a mix of public/private organization or multi-national videoconferencing it is not possible to be compliant with the current section 40, *FOIP* Act [2] because of the disclosure of PII.

6.0. Recommendations for Videoconferencing

The following sections provides recommendations (based on literature review, analysis in the sections above, and personal observations of the author) for organizations, system administrator, legislatures and participants. The

recommendations address awareness, challenges and compliance and are both general and specific.

6.1. General Recommendations for Organizations and System Administrators

The following list of general recommendations is not exhaustive by any means but as a minimum to address the compliance with privacy legislation.

- Establish a clear and well-defined purpose within the organization and ensure that this is conveyed to the participating organizations
- Conduct a PIA from the perspective of all the involved organizations, security/system administrators, and participants before engaging in a videoconference session.
- PIA should be conducted for select videoconferencing scenarios (relevant to the organization) such as single organization, multiple- public organizations, multiple- public/private organization combination, and multi-nations.
- Become familiar with the laws of the jurisdictions of other sites, organizations' security policies, and enforcement in order to determine the intent and enforcement of security policies.
- Secure a formal agreement from all the involved sites to ensure that the purpose does not change between the organizations.
- Obtain legal advice when necessary.
- A videoconference session should not be recorded unless there is a business case and the PII risks have been taken into consideration.

Ensure that compliance is met, by not recording the videoconference session.

6.2. Recommendations: Privacy Awareness Issues for Organizations and System Administrators

Establishing and reinforcing privacy protection not only requires awareness of risks but also modification in behaviour.

- Deliver effective training and periodic refreshers to both the organization's personnel and participants to create and maintain awareness of the potential threat of videoconferencing to privacy, so that they can make an informed decision about consent. In the case of school children, include the parents/guardians.
- Discourage participants from using full names during a videoconference session; instead, encourage the use of pseudo-names whenever possible.
- Discourage participants from revealing any personal information about themselves, their friends, and/or their relatives.
- Advise participants as to whether a session will be recorded or not, and who it will be shared with. This may limit discussion regarding any material or topics that pertain to "original ideas", copyright concerns, and ownership of these.

6.3. Recommendations: Technical and Operational Issues for Organizations and System Administrators

The Technical and operational issues for organizations and system administrator address only the protection of PII of the participants and compliance with privacy legislation.

- Mitigate in-transit threats by using encryption and Virtual Private Network (VPN) or Virtual Local Area Network (VLAN) technologies as a default method for transmitting videoconference sessions.
- Limit recording of videoconferences: it should not be done unless all compliance criteria of *FOIP* [2] and the paramountcy laws [11] have been met.
- Classify and access videoconference session information appropriately.

- Regularly monitor and scan the network resources to mitigate unauthorized access and removal of storage media.
- IT department and security teams should ensure that proper controls are in place, that users (participants) are well trained in using the equipment, and that they are aware of the potential of videoconferencing for compromising PII.

6.4. Recommendations: Privacy Compliance Issues

Issues concerning noncompliance for videoconferencing information under the current *FOIP* [2] and *Privacy Act* [1] can be addressed by revisiting these and related Acts, and incorporating appropriate amendments into the Acts for emerging technologies such as videoconferencing to protect the PII of all participants (whether they are served by a an organization or not). Some examples of where this might be appropriate are as follows:

- *Disclosure*: It is necessary to ensure that there is authorization for disclosure, either through legislation or through individual consent.
- *Authorization*: Under *FOIP* [2], collection by the public body must be authorized legislatively, depending on the industry of the public body. In the case of K-12, the *School Act* [20] authorizes only the collection of student records (PII) from the students it serves, so it would appear that one school jurisdiction could not collect personal information from another in Alberta or anywhere else: under the current laws, it would not be in compliance. *FOIP* [2] and the related acts must be revisited to bring this into alignment with emerging technologies such as videoconferencing.
- *Consent*: An organization requires an informed consent with regard to use as well as disclosure of his/her PII from the participant, and since the risks for the participants have not even been identified by the organizations, it is highly unlikely that the participants can make an informed decision at the present time. However, that would be something for the courts to decide. If it appears that there is no valid consent, then the collection or transmission of the information is also noncompliant.

Once these three fundamentals have been addressed, other issues come into play:

- *Storage*: *FOIP* [2] requires that the information in custody of a particular organization must be secure, but videoconferencing is borderless and may or may not be contained within that organization.
- *Recording*: Public sector organizations need to define the roles and responsibilities of recording videoconferencing by establishing policy for conditions when recording is allowed and who owns the data (the author is aware that currently the access to recording device(s) is not necessarily secure and is available to participants as well as to others).
- *Access, disclosure, retention, and destruction*: These issues should also be covered by specific and clear policy.
- *Videoconference session information*: This should be appropriately classified and contained by effective access controls.
- *Organizations*: Organizations should audit and monitor their systems regularly to ensure that unauthorized access and storage of information is mitigated in a timely manner.
- *Top management of an organization*: It has the responsibility to ensure that proper controls (such as policies, standards, and procedures) are in place to mitigate unauthorized access, collection, storage, distribution, disclosure, retention, third-party involvement and destruction are addressed for videoconferencing. This should include regular external and internal audits to identify any areas of non-compliance.
- *Awareness and training*: Participants, system administrators, and staff will require this in order to make informed decisions. Use of posters and reminders for awareness could also be used to modify behaviour.

6.5. Recommendations: Legislative and Legal Issues in Protection of Personal Identifiable Information

The following recommendations are made in an effort to reduce incidents of non-compliance of *FOIP* [2] / *Privacy Act* [1].

- All privacy Acts and related Acts for both public and private organizations (provincial and national) need to be revisited and amended to address trans-jurisdictional (provincial) and trans-provincial (national) transmission, ownership, use, disclosure, and retention and destruction of personal information of individuals to align with current and emerging technologies.
- Regular reviews of the Acts need to be in place to keep abreast of the fast changes and capabilities of technology.
- All national governments need to collaborate and develop an international directive for the protection of privacy. This will provide assurance to the individuals that their PII will be protected in a standardized manner.

6.6. Recommendations: Awareness for Participants' of Personally Identifiable Information

Participants need to understand the various threats presented to their PII during videoconferencing sessions:

- Participants need to ensure that they have the necessary information from the organization to provide an informed consent before participating in videoconferencing.
- Limit the PII exposed during videoconferencing session.
- The participants should assume that the videoconferencing session is being recorded even if the information provided by the organization states otherwise. This is because the organization has no way of ensuring or preventing recording from occuring at other locations or organizations.
- Avoid holding private side-coversations that occur frequently and often go undetected during in-person physical meetings because in virtual meetings the presence of microphones/cameras can result in risk that the private coversations may be recorded.

7.0. Videoconferencing in the National and International Context

Videoconference sessions as discussed in this paper present unique challenges since they are an aggregate of the PII of individuals from multiple organizations, locations, and nations. Currently, no international effort addresses this, but such an effort is necessary for the protection of privacy of all global citizens. The potential risks and privacy trends can be understood and assessed by examining global surveys, such as the one conducted by the UK-based organization Privacy International [39]. Each year since 1997, Privacy International and the US-based Electronic Privacy Information Center [40] have undertaken a comprehensive survey of global privacy.

The International Association of Privacy Professionals [34] is also doing some work for privacy protection in the e-commerce sector (IAPP) that has members from 32 countries.

8.0. Conclusion

Videoconferencing is without question beneficial, and this paper is certainly not advocating that it should be banned or abandoned. This paper shows the need to be proactive and accept the paradigm shift from privacy within an organization to multi-jurisdictional aspects.

Videoconferencing session information is almost a complete set of PII (Table 5.1 and *FOIP* [2]) that may or may not be related to commercial activities. A videoconferencing session is a collaborative activity for sharing knowledge. This fact also deserves consideration in an international context because of the potential magnitude of its adverse impact on the lives of the individual. For example, on April 3, 2008, Globe and Mail Update and Canadian Press reported that Saskatchewan NDP released a sixteen year old video recording of a private party (taped in 1991, inside the Progressive Conservative campaign headquarters of Grant Devine who was making an unsuccessful bid for re-election as Saskatchewan premier) that featured the Conservative MP Tom Lukiwski and and a young Brad Wall that contained sexist, racist and homophobic comments[3]. This resulted in an apology in the house of Common by Tom Lukiwski. It remains to be seen whether this will cause embarrassment, end someone's career, and destroy the

[3] This story appeared on April 8th 2008 http://www.theglobeandmail.com/servlet/story/RTGAM.20080403.wMPontape0403/BNStory/National/home?cid=al_gam_mostview)

reputation of the individuals involved. This exposes the possible ramifications of any recorded media, although that is beyond the scope of this paper.

It is challenging for organizations to participate in videoconference sessions and remain in compliance with the current privacy and paramountcy laws unless the sessions are contained within the organization. Even if the session is not recorded, inter-organizational sessions disclose the participants' PII to third parties, which is in contravention of *FOIP* [2].

Informed consent cannot be obtained or validated without defining all the involved organizations' purposes and identifying the authority, use, access, and disclosure as well as compliance with the applicable laws.

This paper has identified that the awareness of issues and associated risks is an essential element to making an informed decision with regard to consent to participate in videoconference sessions. The need for awareness training/refreshers for all the personnel involved and for the participants is also essential, as participants are the ones that potentially could lose the most—their PII, forever.

"Flows of computerized data and information are an important consequence … in national economies. With the growing economic interdependence … flows acquire an international dimension [41]." This is an acknowledgement that there are concerns when data traverses national borders. In 1980, The Organization for Economic Co-operation and Development (OECD) [41] developed Guidelines on the Protection of Privacy, and Trans-border Flows of Personal Data which remain an important international standard in privacy protection. The guidelines were expressly designed to promote international harmonization of privacy protection while protecting the free flow of personal information related to commerce. So far, there is no consensus except that the issue needs to be addressed.

The efforts of the OECD [41] show the necessity for international involvement; however, the OECD [41] mandate is limited to commercial transactions of commercial organizations. The public and non-commercial private organizations could initiate something similar for videoconferencing and other information-sharing activities by leveraging the efforts of the OECD [41] to-date.

This paper has highlighted the complexities of the issues surrounding the protection of PII while utilising videoconferencing and it is obvious that privacy protection needs to be addressed in all areas and at all levels—governments, organizations, and individual participants.

We need to ask ourselves; what are the implications of videoconferencing in the public sector under the present provincial privacy laws? Obviously, the laws are not adequate, but urgently require revisiting and updating, to include the current and emerging technologies, as well as a regular scheduled reviews to keep the laws current with ongoing technical innovations.

Another area of concern is accountability. This area of *FOIP* [2] as well as other privacy protection laws, provide for an individual's access, and an obligation on the part of the organization, to correct inaccuracies. In the case of videoconferencing, it may not be able to meet the accuracy of record requirement; people's opinions and beliefs evolve during their lifetimes, so that what was regarded as "true" five years ago may not be true today. Therefore, if the "record" is no longer accurate, then how can it be addressed?

In summary, this paper has

- raised the awareness of privacy protection risks for videoconferencing participants;
- demonstrated the need for training;
- highlighted the challenges for compliance with privacy protection of PII; and
- emphasized the need to revisit and align privacy laws, including dependent (paramountcy) laws, to address the challenges of privacy protection from emerging technologies—from the time the laws were enacted or amended, and including the ones to address what is emerging now.

Further research in several disciplines is needed, before privacy issues related to videoconferencing are resolved. They include looking into appropriate changes by various levels of government to the privacy legislation, paramountcy laws, and organizations; quantitative data for privacy breaches specific to videoconferencing; and awareness of technical matters, personnel, and participants.

As technology makes more and more information available and easily accessible, it becomes necessary to treat that data with the level of guardianship that we would want for our own private information. Data, including PII, can be seen as a commodity. Due diligence and regulations are required to protect what each citizen has a right to be kept private (assuming no criminal activities), as everyone should have the right to protect what is inherently theirs to begin with. When we share this with an organisation, it becomes their responsibility to protect this with the same rigour as we would individually.

Without awareness and guidelines in place and enforced, it is easy for organisations to not realise the impact of making this information readily available.

Education, guidelines, laws and regulations are a fundamental part of ensuring that as the success of videoconferencing becomes a basic of our lives, that each of us has our PII protected.

REFERENCES

1. *Privacy Act*, R.S., 1985, c. P-21 (Canada). Almost all provinces have their own public and private sector privacy laws based on the federal law which in turn is based on Model Code for the Protection of Personal Information [17], http://laws.justice.gc.ca/en/P-21/index.html.
2. *Freedom of Information and Protection of Privacy Act*, R.S.A., 2000, C. F-25 (Alberta), http://foip.gov.ab.ca/ [*FOIP*]
3. *Freedom of Information and Protection of Privacy Act Regulations (alberta), http://foip.gov.ab.ca/legislation/regulation/index.cfm [FOIP Regulations]*
4. *Personal Information Protection Act* (Alberta), http://www.pipa.gov.ab.ca/ [*PIPA*]
5. Canada, *Personal Information Protection and Electronic Documents Act* (Canada), http://www.privcom.gc.ca/legislation/02_06_01_e.asp [*PIPEDA*]
6. Investigations conducted by the Office of the Information and Privacy Commissioner of Alberta, http://www.oipc.ab.ca/orders/investigation.cfm [OIPC Alberta]
7. Canadian Institute of Chartered Accountants: Generally Accepted Privacy Principles, http://www.cica.ca/index.cfm/ci_id/36529/la_id/1 [GAAP]
8. Office of the Information and Privacy Commissioner for British Columbia, http://www.oipcbc.org/sector_public/resources/index.htm [OIPC BC]
9. Office of the Privacy Commissioner of Canada, http://www.privcom.gc.ca/index_e.asp [OIPC Canada]
10. Various studies of graduate law students funded by federal privacy commissioner, http://www.privcom.gc.ca/resource/cp/p_index_e.asp
11. Paramountcy laws (Alberta), http://foip.gov.ab.ca/legislation/pdf/paramountcy.pdf
12. VC Alberta, http://www.vcalberta.ca/
13. Computer Security Institute 2007 Survey, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf
14. Deloitte & Touche LLP and Ponemon Institute LLC: 2007 Privacy & Data Protection, http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf
15. *H.323* ("an umbrella Recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network," http://en/wikipedia.org/wiki/H.323
16. Article – *Videoconferencing Insight Newsletter* - Alberta videoconference, http://www.vcinsight.com/default.asp?artID=3823
17. Model Code for the Protection of Personal Information, http://www.csa.ca/standards/privacy/default.asp?load=code&language=english#model%20code
18. "Record": http://foip.gov.ab.ca/legislation/act/section1.cfm
19. "Personal information": http://foip.alberta.ca/legislation/act/section1.cfm
20. *School Act*, R.S.A. 1980, c. S-3 (Alberta): http://www.qp.gov.ab.ca/Documents/acts/S03.CFM
21. Video surveillance policy, http://www.btps.ca/images/docs/board/policies/FLA.pdf
22. Cell phones policy, http://www.btps.ca/images/docs/board/policies/HIBG.EXHIBIT%204.pdf
23. Videophone Alert. McLennan Ross, LLP, http://www.mross.com/law/Publications/Email+Alerts?contentId=887
24. Telehealth Videoconferencing Technology Standard (Alberta), http://www.health.alberta.ca/about/HISCA_TelehealthStandardsPartC_V1.pdf
25. "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?" http://www.cippic.ca/uploads/May1-06/PIPEDAComplianceReport.pdf
26. "Mr. Klein Goes To Washington: Whistleblower tells Congress not to deliver spying telco legal immunity," http://www.dslreports.com/shownews/89223
27. Maher Arar, http://www.csmonitor.com/2005/0811/dailyUpdate.html
28. "Why are so many individuals singled out when they travel?" http://www.travelwatchlist.ca/stories
29. PIA - four core components http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piapg-pefrld-1-eng.gif http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod4/mod4-2-eng.asp

References, cont'd

30. *Health Information Act*, R.S.A. 2000, c. H-5 (as ammended 2006), http://www.emp.ca/index.php/chapter-8-client-information-and-records

31. OIPC PIA Registry search results for videoconferencing PIA, (Alberta), http://www.oipc.ab.ca/Search/Index.cfm?searchvar=1

32. PIA from David Thompson Health Region for videoconferencing (Alberta), http://www.oipc.ab.ca/ims/client/upload/Summary_H1856_Pediatric_VC_Mar_080001.pdf

33. Alberta Supernet, (a high-capacity network that connects Alberta schools, hospitals, libraries, and government offices for information sharing and service delivery), http://www.albertasupernet.ca

34. The international association of privacy professionals (IAPP), http://www.privacyassociation.org

35. PIA - four core components, (British Columbia), http://www.oipc.bc.ca/legislation/FIPPA/Freedom_of_Information_and_Protection_of_Privacy_Act(May_2008).htm#section30.1 Or, http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piapg-pefrld-1-eng.gif Or, http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod4/mod4-2-eng.asp

36. Government of Canada: PIA checklist, http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod4/mod4-3-eng.asp

37. OIPC - Full PIA Form (Alberta), http://www.oipc.ab.ca/ims/client/upload/piaform-full.dot

38. Treasury Board of Canada Secretariat guidelines, http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod4/mod4-2-eng.asp

39. Privacy International, http://www.privacyinternational.org

40. Electronic Privacy Information Center, US, http://epic.org/

41. The Organization for Economic Co-opertion and Development , http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html (OECD)

Appendix A: Literature Review

Summary of Literature Review		
Literature	**Purpose of Review**	**Key Findings**
FOIP [2].	o Understand what is protected under the act, who does it apply to, the requirements of privacy protection and its applicability to videoconferencing session information.	o All provincial government departments, agencies, boards, and commissions including municipalities are public bodies and they generally do not have the authority to collect PII as stated under FOIP [2] Sections 33(a) and 33(b) other than for the individuals they serve. Section 33(c) may allow collection if the public body can demonstrate that such collection is directly related to and is necessary for an operating program or activity of the public body. o FOIP [2] requirements for compliance for the protection of PII. o What needs to be protected? o Applicability of FOIP [2] for videoconferencing over IP for recorded (stored) and not recorded (not stored) sessions. o Compliance with FOIP [2] is required when videoconferencing session is recorded (stored) as it becomes an individual's permanent PII record. o Compliance with FOIP [2] is required concerning disclosure of PII to third parties even when videoconferencing session is not recorded. This requires informed consent of the individual or guardian or parent (if the individual is under the age of consent).
FOIP [2] Sections 33(a), 33(b) and 33(c).	o Determine the authority to collect PII.	o Authority of a public for collection of PII body is generally limited to the individuals it serves or employs. The exception being when *FOIP* [2] Section 33(c) applies.
FOIP [2] Sections 40 and 17.	o Determine the disclosure rules of PII.	o Disclosure of PII with some exceptions must be in accordance to the purpose and use of collection of PII. *FOIP* [2] Sections 40 and 17. o The exceptions to collection/disclosure would be where public safety, law enforcement, national security, or anti-terrorism is involved.
Paramountcy laws [11].	o Determine the authority for the collection of PII. o Determine limitations of collection of PII and under what circumstances.	o Paramountcy laws prevail over *FOIP* [2].
GAPP [7] Model Code [17] *FOIP* [2], *PIPA* [4], *PIPEDA* [5].	o Determine if there were any differences between them.	o Privacy principles of GAPP [7] and Model Code [17] are similar to *FOIP* [2], *PIPA* [4], *PIPEDA* [5].
Investigations conducted by the Office of Privacy Commissioners (OIPC) of Alberta [6], British Columbia [8], and Canada [9] (1997-2008).	o Determine and understand problematic areas of awareness, challenges, and compliance.	o Authority to collect PII is required through an Alberta or Canada legislative enactment. o Obtaining an informed consent.
OIPC, Alberta [6] investigations from 1997 to 2008.	o Obtain a solid understanding of intent, consent, collection, use, disclosure, retention, and disposal/destruction of personal information for the compliance of privacy protection legislations.	o That informed decisions for consent are often a source of problems for participants.
An analysis of the statistics in OIPC, Alberta [6] annual reports from 1997-2008.	o Obtain statistical data of complaints to OIPC, Alberta [6].	o Public bodies appear to be more compliant since they record fewer privacy complaints with the OIPC, Alberta [6] (see Appendix D). There have been 466 investigations relative to the 4200 locations of 1200 public bodies since 1997 (see Appendix D). o However positive this may seem, they do not appear to have stated or implemented policies, related to the protection of PII in videoconferences.

Literature	Purpose of Review	Key Findings
Various studies by graduate law students that were, funded by the federal privacy commissioner [9].	o Determine the state of privacy policy in organizations. o Determine if there were any studies conducted about the emerging technologies.	o Private sector policies do not comply with the privacy laws. o Storage of Canadians' PII in another country breaches the Privacy Acts.
78 public sector websites (Appendix A).	o Authority to collect PII, as well as posted policies for its use, disclosure, retention, and destruction of personal information.	o Absence of videoconferencing policy. o Absence of authority to collect biometric data such as images.
VC Alberta [12]. A central resource for K-12 videoconferencing community in Alberta.	o Review documentations available for the videoconferencing community.	o There was plenty of advice concerning what to wear, how to prepare, the scheduling of videoconferencing sessions, etiquette during the session, the pedagogy to use or best practices for conducting a successful videoconferencing, etc. o Nothing on privacy awareness, concerns, or issues
Privacy surveys: Computer Security Institute 2007 survey [13]. 2007 Privacy & Data [14] Protection by Deloitte & Touche LLP and Ponemon Institute LLC [14].	o Locate relevant quantitative and qualitative data for videoconference privacy breaches.	o Surveys did not categorize PII breaches and therefore specific data for videoconferencing PII breaches does not exist.

Appendix B: List of Websites Examined

Provincial government ministries (4)	
o Service Alberta	o Alberta Health and Wellness
o Alberta Education	o Advance Education
Public and Separate School Boards (52)	
o Aspen View Regional Division No. 19	o Battle River Regional Division No.31
o Black Gold Regional Division No. 18	o Buffalo Trail Public Schools Regional Division No. 28
o Calgary School District No. 19	o Canadian Rockies Regional Division No.12
o Chinook's Edge School Division No. 73	o Clearview School Division No. 71
o Edmonton Schools District No. 7	o Elk Island Public Schools Regional Division No. 14
o Foothills School Division No. 52	o Fort McMurray Public School District
o Greater St. Albert Catholic Regional Division No. 29	o Grasslands Regional Division No. 6
o Grande Prairie School District No 2357	o Fort Vermillion School Division No. 52
o Grande Yellowhead Regional Division No. 35	o Greater St. Albert Catholic Regional Division No. 29
o High Prairie School Division No. 48	o Horizon School Division No. 67
o Livingstone Range School Division No. 68	o Lloydminster School Division
o Northern Gateway Regional School Division No. 10	o Parkland School Division No. 70
o Peace River School Division No. 10	o Peace Wapiti School Division No. 76
o Pembina Hills Regional Division No. 7	o Prairie Land Regional Division No. 25
o Red Deer School District No. 104	o Rocky View School Division No. 41
o St. Paul Educational Division No. 1	o Sturgeon School Division No. 24
o Westwind School Division No. 74	o Wetaskwin Regional Division No. 11
o Wild Rose School Division No. 66	o West Creek School Division No. 72
o Calgary Roman Catholic Separate School District No. 1	o Christ the Redeemer Catholic Separate Regional Division No. 3
o Edmonton Catholic Separate School District No. 7	o East Central Alberta Catholic Separate Schools Regional Division
o Elk Island Catholic Separate Regional Division No. 41	o Evergreen Catholic Separate Regional Division No. 2
o Fort McMurray Roman Catholic Separate School District No. 32	o Grande Prairie Roman Catholic Separate School District No. 28
o Holy Family Catholic Regional Division No. 37	o Holy Spirit Roman Catholic Separate Regional Division No. 4
o Lakeland Roman Catholic Separate School District No. 150	o Living Waters Catholic Regional Division No. 42
o Lloydminster Roman Catholic Separate School Division	o Medicine Hat Catholic Separate Regional Division No. 20
o Red Deer Catholic Regional Division No. 39	o St. Albert Protestant Separate School District No. 6
Public Colleges (4)	
o Grant MacEwan Community College	o Mount Royal College
o Grande Prairie Regional College	o Northern Alberta Institute of Technology
Public Universities (4)	
o University of Alberta	o University of Calgary
o University of Lethbridge	o Athabasca University
Regional Health Authorities (9)	
o Chinook Regional Health Authority	o Palliser Health Region
o Calgary Health Region	o David Thompson Regional Health Authority
o East Central Health	o Capital Health
o Aspen Regional Health Authority	o Peace Country Health
o Northern Lights Health Region	
Other Public Bodies (4)	
o Edmonton Economic Development Corporation	o City of Edmonton
o City of Calgary	o VC Alberta

Appendix C: Office of the Information and Privacy Commissioner, Alberta Activity

Year	Orders	Investigation Reports	Adjudicator Orders	Judicial Reviews	Other Decisions	
1996	22	0	1	1	0	
1997	20	0	0	0	0	
1998	21	16	0	0	0	
1999	41	9	0	0	0	
2000	34	9	0	0	0	
2001	42	11	0	0	0	
2002	30	12	1	1	1	
2003	25	5	2	1	3	
2004	32	3	1	0	0	
2005	30	5	0	1	1	
2006	32	3	0	0	0	
2007	32	7	0	0	1	
2008	10	0	0	0	0	
TOTAL	371	80	5	4	6	466

-
- Source: http://foip.alberta.ca/dsp_commissioner.cfm
- 1200 public bodies: http://foip.alberta.ca/pbdirectory/index.cfm
- Four Thousand two hundred sites source: http://www.gov.ab.ca/acn/200509/18828F93E02E6-F2D6-4F55-99D3CC5C2E0424EF.html
- Four hundred and twenty nine: http://www.gov.ab.ca/acn/200509/18828F93E02E6-F2D6-4F55-99D3CC5C2E0424EF.html

Appendix D: Acts and Regulations Paramount over the *Freedom of Information and Privacy Protection Act* [11, 2]

Minister Responsible	Act or Regulation Paramount over the FOIP Act	Sections Paramount
Aboriginal Affairs and Northern Development	*Metis Settlement Land Registry Regulation* (AR 361/91)	Sections 68(3) and 92(3)
Children's Services	*Child, Youth and Family Enhancement Act* (R.S.A. 2000, c. C-12)	Sections 3.1(2), (3), 74.1(2) and 126.1(1) (Paramountcies established in Sections 3.1(4), 74.1(2), and 126.1(3) of that Act)
Education	*Student Evaluation Regulation* (AR 177/2003)	Section 8(2)(c)
Energy	*Coal Conservation Regulation* (AR 270/81)	Sections 51, 52, 57, 58, and 59(2) (Paramountcy established in Section 9(3.1) of the Coal Conservation Act, R.S.A. 2000, c. C-17)
	Electric Utilities Act (S.A. 2003, c. E-5.1)	Section 137 (2) (Paramountcy established in Section 137(1)(a) of that Act)
	Gas Utilities Act (R.S.A. 2000, c. G-5)	Section 28.8(2) (Paramountcy established in Section 28.8(1)(a) of that Act)
	Metallic and Industrial Minerals Regulation (AR 66/93)	Section 15.1(1)
	Mines and Minerals Act (R.S.A. 2000, c. M-17)	Section 50(1), (1.1), (3) and (4) (Paramountcy established in Section 50(1.1), (3), and (4) of that Act)
	Natural Gas Marketing Act (R.S.A. 2000, c. N-1)	Section 17(1) (Paramountcy established in Sections 17(1.1) and (4) of that Act)

Appendix E: Current Status of Freedom of Information and Protection of Privacy Act Compliance for Recorded Videoconferencing Session

Compliance	Relevant Sections FOIP [1]	Concerns/Analysis/Explanation
Authority to the collection of data NOT Compliant	**Division 1: Collection of Personal Information** **Section 33 – Purpose of Collection of Information** No personal information may be collected by or for a public body unless (1)(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada, (1)(b) that information is collected for the purposes of law enforcement, or (1) (c) that information relates directly to and is necessary for an operating program or activity of the public body. 1994 cF-18.5 s32;1999 c23 s19	Section 33 (1) (a) This will present challenges for identifying the purpose of collection of personal information for some of the public bodies. For instance, the school has the authority to collect personal information under the School Act; however, they can only collect this for the students, parents, or guardians of those students for whom it provides services. Therefore, the collection can only occur for the schools within a school jurisdiction. Therefore, consent will be required from all other non-jurisdictional organizations. Section 33 (1) (b) is not applicable except to the law enforcement bodies. Section 33 (1) (c) Although it may be possible for the schools to justify to some extent that it enhances ICT curriculum program mandated by Alberta Education. However, this is open to challenge, as other less intrusive methods exist.
Intent of collection of data NOT Compliant	**Division 1: Collection of Personal Information** **Section 33 – Purpose of Collection of Information** No personal information may be collected by or for a public body unless (1)(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada, (1)(b) that information is collected for the purposes of law enforcement, or (1) (c) that information relates directly to and is necessary for an operating program or activity of the public body. 1994 cF-18.5 s32;1999 c23 s19 (2) Despite subsection (1), but subject to subsection (3), a post-secondary educational body may use personal information in its alumni records for the purpose of its own fund-raising activities. (3) A post-secondary educational body must, when requested to do so by an individual, discontinue using that individual's personal information under subsection (2). (4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner. 1994 cF-18.5 s37;1999 c23 s24	Section 33 (1) (a) Videoconference sessions may involve participants that are not residents of Alberta but Canadians as well as non-Canadians where neither Alberta nor Canada has any legal jurisdiction respectively. It appears that public bodies cannot collect personal information because they do not have authorization under an enactment of Alberta or Canada paramountcy laws [10]. Section 33 (1) (b) Even law enforcements can do this only under limited circumstances where non-Canadians are involved. There cannot be an informed valid consent if there is no authorization to collect or disclose the information in the first place. Section 33 (1) (c) may allow the collection of PII from a videoconference sessions but OIPC warns that this Section has a potential of challenge and organizations should be prepared to defend it. Sections 33 (2) and 33 (3) are self-explanatory. Section 33 (4) could be also be used to challenge Section 33(c).
Informed consent for the collection of data from the individual or trustee or guardian or parent NOT Compliant	Part 2: Protection of Privacy Section 34 - Manner of collection of information Part 2: Protection of Privacy: Division 2: Use and Disclosure of Personal Information by Public Bodies If the individual the information is about has identified the information and consented, in the prescribed manner, to the use.	The key here is informed consent for collection, use, and disclosure of personal information. The paramountcy laws limit the collection of personal information by a public body. S 38 sets out the disclosure rules. The disclosure of personal information including visible or implied health issues is inevitable in a videoconference session. The literature review has shown that organizations have not identified the complex issues of privacy protection of individuals in a videoconference session. Therefore, it is reasonable to state that the participants have not been informed of the

Compliance	Relevant Sections FOIP [1]	Concerns/Analysis/Explanation
		potential risks. Hence, an informed consent cannot be obtained. An organization is accountable for the data that is in its custody or when it is shared to ensure that, it is protected. So how can an organization be certain about the use of data by the other participating organizations regarding their security, access control, purpose, and use of the data to provide such an assurance? Without formal agreements, this will require enormous trust and faith, especially in trans-national sessions.
Storage NOT Compliant	Section 38 of the **FOIP ACT** states that: The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. 1994 cF-18.5 s36;1996 c28 s21	Depending on who is involved and where the participants are located, this may be an issue. It will also depend on the storage media used, its portability, and potential abuses. If the informed consent and authorization are not there (explicit or implicit), then, there is no authority to store the personal information, that would have other authorized custodians normally. Enforcing this beyond Alberta boundaries will present its own challenges.
Retention NOT Compliant	Section 35 of the **FOIP Act** sets the retention period for a minimum one (1) year, which requires that personal information used to make decisions directly affecting individuals must be accurate and complete and be retained for at least one year after using it so that an individual can obtain access to it.	Since consent, authorization, and storage are questionable, then so is the retention.
Access NOT Compliant	Division 1: Obtaining Access to Records, Section 6 - Information rights will apply to determine how and if access will be provided. Section 7 - How to make a request Section 8 – How to address Abandoned request Section 9 – How to address Continuing request Section 13 - How access will be given Section 15.1 - Request under Section 7 deemed to be a request under HIA (Health Information Act of Alberta)	How should organizations deal with videoconference session information that is a conglomeration of individual records of the participants? How will the participants know where their personal information is stored or keep track of it? Sections 9, 13, and 15.1 will need consideration for each incoming request.
Disclosure NOT Compliant	Division 2: Exceptions to Disclosure Section 16 - Disclosure harmful to business interests of a third party Section 17 - Disclosure harmful to business interests of a third party Section 18 - Disclosure harmful to individual or public safety Section 19 and 20 - Confidential evaluations Section 21 - Disclosure harmful to intergovernmental relations Section 22 - Cabinet and Treasury Board confidences Section 23 - Local public body confidences Section 24 - Advice from officials Section 25 - Disclosure harmful to economic and other interests of a public body Section 27 - Privileged information Section 28 - Disclosure harmful to the conservation of heritage sites, etc. Section 29 - Information that is or will be available to the public Division 3: Third Party Intervention	How should organizations manage the videoconference data disclosure for an access request from a participant? Please note that this is a conglomeration of individual records of the participants. It is technically possible to block images and distort voices. This may mitigate some of the risks but not all, such as beliefs or opinions. For most organizations, this solution is likely cost prohibitive. Also, the context is lost for the participant who accesses the information. It could result in further complications should the PII be misused or abused.

Compliance	Relevant Sections FOIP [1]	Concerns/Analysis/Explanation
	Section 30 - Notifying the third party	
Use and Disclosure	**Division 2: Use and Disclosure of Personal Information by Public Bodies** Section 40 – Disclosure of Personal Information Section 41 - Consistent Purpose Section 42 – Disclosure for Research or Statistical Purpose **Part 3: Disclosure of Information in Archives** Section 43 – Disclosure of Information in Archives	How to manage the videoconference data sine it is a conglomeration of individual records of the participants? If two public bodies' paramount laws have different requirements - how should, this be addressed?
Accountability	Division 1: Obtaining Access to Records Section 10 - Duty to assist applicants Section 11 - Time limit for responding to access request Section 12 - Contents of response Section 14 - Extending time limit for responding Section 15 - Transferring a request and responsibilities of requested party Division 2: Exceptions to Disclosure Section 26 - Testing procedures, tests and audits Section 27 - Privileged information	How should organizations manage the videoconference sessions data that is a conglomeration of individual records of the participants stored in perhaps trans-jurisdictions and trans-nations? How will accountability work for the PII to the individual? The public body would normally have the PII of the people it serves in its custody and control but in a videoconference session, it has been disclosed and now resides in multi-organizations?

Appendix F: Checklist for Conducting a Preliminary PIA for Videoconferencing

A Checklist to Determine whether PIA is Required for Videoconferencing			
	Questions that Need to be Answered	**Not recorded**	**Recorded**
1. a	Is the organization designing a new program or service?	No.	No.
1. b	Is the organization significantly changing delivery method of program or service?	Yes.	Yes.
2.	Does the program require the organization, to collect, use or disclose personal information?	No	Maybe, but it is usually done for making it available on demand. It may or may not be a business requirement.
3.a	Will the program require the organization to collect, use, or disclose additional personal information or more sensitive information than in the past?	No	Yes. Since the information is a collection of participants' PII from other sites, organizations, jurisdictions or countries along with the local data.
3.b	Is the organization shifting from informed consent to indirect collection of personal information?	No.	Currently there is no explicit informed consent process although there may be an implied consent through participation but it is not an informed consent – more a case of trust or lack of awareness.
4.a	Will it be necessary to develop mechanisms to notify individuals about their privacy rights?	Yes - it should be, as currently the remote site is free to record if they wish to do so.	Yes - it should be, as currently the remote site is free to use the information as the laws of their jurisdiction permit.
4.b	Will it be necessary to obtain the consent of individuals to collect, use, and disclose their personal information?	Yes – disclosure of PII beyond FOIP [2] disclosure Section 40 to external organizations.	Yes. Currently there is very little awareness of its implications to privacy in the videoconferencing participants' community or guardians.
5.	Will the program require the organization to collect personal information from other programs within the host organization, other organizations, other governments, or private sector?	No.	Yes, depending on who the participants are, it is possible, that a single videoconferencing session involves all types of organizations, multiple jurisdictions, and countries. Each organization/location then has the ability to collect the personal information of the participants.
6.	Will the personal information generated by the program be used in decision-making processes that directly affect individuals, such as eligibility for programs or services or for enforcement?	No.	Maybe – it is possible, but it may well have other legitimate uses and illegitimate uses.
7.	Will the personal information generated by the program be used for any other purposes, including research and statistical purposes?	No.	May be but as above it has a potential for abuse and misuse.

A Checklist to Determine whether PIA is Required for Videoconferencing			
	Questions that Need to be Answered	**Not recorded**	**Recorded**
8.	Will the personal information be shared with other organizations for any purpose than its original purpose of collection?	No.	The organization may share the information with its original collection parameter, but the remote organization may not be required to comply with it by the laws in its jurisdiction.
9.	Does this require new common client identifiers or use of SIN without legislative authority?	No.	No - unless the organization uses metadata tags or indexing of the participants.
10.	Is there a reason to anticipate that the public will have any privacy concerns regarding the proposed program or service?	Yes – disclosure to third parties.	Yes, Privacy concerns may arise once the public fully understands the privacy risks and its implications.
11.	Is this introducing changes to the business systems or infrastructure architecture that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information?	Yes, a new business delivery and infrastructure models are, introduced; videoconferencing requires changes to firewall configurations or bypassing it all together. In fact, it may be desirable by some organizations to by-pass the firewall by using the MCU.	Yes, a new business delivery and infrastructure models are, introduced; videoconferencing requires changes to firewall configurations or bypassing it all together. In fact, it may be desirable by some organizations to by-pass the firewall by using the MCU.