OPENEYE WEB SERVICES (OWS) AND CANADIAN PRIVACY REGULATIONS

CANADIAN PRIVACY REGULATIONS AND USING OWS

OpenEye Web Services (OWS) provides many benefits to IT administrators and users for managing and viewing video from recorders. In Canada, the storage and transmission of video or data containing personally identifiable information (PII) is covered by the Personal Information Protection and Electronic Documents Act (PIPEDA) and other Provincial Privacy acts. For Canadian residents, businesses, and public sector bodies, it is important to understand the requirements imposed by PIPEDA, and other Provincial Privacy acts, and how they may impact their use of OWS.

WHAT PRIVACY REGULATIONS ARE IN PLACE IN CANADA?

Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000. This act outlines how public and non-public sector bodies may collect, use and disclose personal information in the course of commercial business. PIPEDA was passed at the federal level and applies to all businesses, domestic or foreign, doing business with any Canadian business or individual.

In addition to PIPEDA, several provinces have passed privacy acts further restricting how personally identifiable information (PII) should be handled for businesses and individuals residing within each province.

Examples of PII include:

- Full name
- Email address
- Physical address
- IP Address – When linked to user
- Facial pictures
- Birthday
- Login name
- Phone number
- Job title
- Facial Video

OWS CONFORMANCE WITH PIPEDA AND PROVINCIAL PRIVACY ACTS

After reviewing the requirements of PIPEDA and other Provincial Privacy acts, OpenEye believes it conforms to their requirements, **with the exception of some Provincial Privacy Acts which further regulate how PII data may be transmitted across Canadian or Provincial borders**.

At the time of this guides publication, the OWS architecture centralizes all user account data, including PII, within the United States of America. This allows us to provide optimal service to our customers and ensure the integrity and reliability of our service.

Because OWS transmits PII data across Canadian and Provincial borders, it is important for public and non-public sector bodies to educate themselves on their responsibilities to comply with the requirements of PIPEDA and other Provincial Privacy acts.

OpenEye highly encourages users to review the specific requirements for transfer of PII data, across provinces, territories and international boarders, of any provincial privacy acts which may supersede PIPEDA in their jurisdiction.

OpenEye's privacy policy can be found at the following web link: https://www.openeye.net/privacy-policy

PIPEDA REQUIREMENTS

PIPEDA REQUIREMENTS CAN BE ORGANIZED INTO TEN CORE PRINCIPLES :

Accountability - Organizations are responsible for information under their control, and must designate an individual responsible for compliance with the legislation. Organizations remain accountable for information transferred to a third party and contractual means must be used to ensure adequate protection.

Identifying purposes - The purpose(s) for which personal information is collected must be specified at the time of or before the collection.

Consent - An individual's informed consent must be obtained for the collection, use or disclosure of their personal information. For consent to be meaningful, the purposes for which the information may be used must be disclosed so that the individual can reasonably understand the use of their information.

Limiting collection - The collection of personal information must be limited to that which is necessary for the purposes disclosed by the organization. Collection must be through fair and lawful means.

Limiting use, disclosure and retention - Personal information cannot be used or disclosed for a purpose other than that for which it was collected, without consent, unless permitted or required by law. Personal information can be retained only as long as necessary for the disclosed purposes.

Accuracy - Organizations must keep personal information as accurate, complete and up-to-date as necessary for the purposes for which it will be used.

Safeguards - Personal information must be protected by safeguards appropriate to its sensitivity. These safeguards must include physical, organizational and technological security measures.

Openness - Organizations must make their policies and practices regarding personal information available to individuals. This information must include contact information for the person accountable for compliance.

Individual access - On request, individuals must be informed of the existence, use and disclosure of their personal information, and must be granted access to it. Narrow exceptions to individual access exist, such as information that includes the personal information of another individual or material subject to solicitor-client privilege. Individuals can request the correction of their personal information.

RESOURCES

PIPEDA - https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Alberta PIPA - http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507

British Columbia PIPA - http://www.bclaws.ca/civix/document/id/consol17/consol17/00_03063_01

Quebec PIPA - http://www.legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1

Overview - https://content.next.westlaw.com/6-502-0556?transitionType=Default&contextData=(sc.Default)&__lrTS=20170518234842106&firstPage=true&bhcp=1