The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines (October 2019)

Legal service providers (LSPs) and third-party service providers that assist them in their legal practice rely on various forms of technology to communicate, create, share, and store information in the course of business. Technology poses risks to privacy and information security, including the confidentiality of privileged communications. This *Commentary* sets out a framework for mitigating these risks.

The focus of the *Commentary* is on personal and confidential information (PCI). Personal information is any information about an identifiable individual, such as contact information, medical or financial information, or biometric identifiers such as an individual's voice recording. Confidential information may relate to individuals or legal entities and includes any information subject to a lawyer's duty of confidentiality or a class of privilege.

Ethical rules, statutes, regulations, and the common law all impose duties on lawyers, paralegals, and less directly, on much of the legal services industry, to safeguard PCI belonging to clients and third parties. Engagement agreements may also contain requirements about the safekeeping and handling of PCI. This *Commentary* suggests some prospective and remedial measures that LSPs should consider in order to meet or exceed these obligations.

The discussion in this *Commentary* is informed by the following guiding principles:

Principle 1: **Know the law**: LSPs should know the relevant law in order to identify, protect, and secure PCI they control in their practices.

Principle 2: **Understand the PCI you control**: LSPs should understand what PCI is, and know the types of PCI in their control.

Principle 3: **Assess risk**: LSPs should periodically conduct a risk assessment of the PCI within their control. The risk assessment should consider the PCI's sensitivity and vulnerability, and the harm that would result from its loss or disclosure.

Principle 4: **Develop policies and practices**: After completing a risk assessment, LSPs should develop and implement appropriate policies and practices to mitigate the risks identified in the risk assessment.

Principle 5: **Monitor regularly**: LSPs should monitor their operations on a regular basis for compliance with privacy and security policies and practices.

Principle 6: **Reassess**: LSPs should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

This *Commentary* is intended to help all LSPs—sole practitioners, law firms of all sizes, paralegals, law clerks, and legal support entities—determine which policies and practices are best suited for them. It aims to give practical guidance to LSPs by exploring "real-life" scenarios involving the loss of PCI, or the breach of security measures designed to protect it, commonly experienced in practice.

This version of *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines* is open for public comment through January 10, 2020. Please send your comments and suggestions to comments@sedonaconference.org.

The full text of *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Sedona_Canada_Commentary_on_Privacy_and_Information_Security.