

Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations

(May 2025)

The *Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations* (“*Commentary*”) presents and discusses principles and best practices to manage data risks associated with dawn raids in criminal and civil/administrative enforcement investigations that may involve multiple jurisdictions. The *Commentary* addresses the unique impacts that dawn raids have on organizations’ abilities to comply with data privacy and data protection requirements in cross-border matters. Part I introduces the issues and describes the scope of the *Commentary*. Part II provides information about the prevalence and risks of dawn raids. Part III sets out eight principles for approaching and managing data risk in dawn raids. Finally, an appendix provides an “Organization Data Checklist in Preparation for Dawn Raids.”

The eight principles set forth in Part III of the *Commentary* are:

- **Principle 1:** Dawn raids should be conducted based on a process that provides for meaningful pre- and/or post-raid review by an independent authority.
- **Principle 2:** The dawn raid procedures that authorities follow should be in writing, readily available, and consistently applied, and should inform private parties of their rights and the processes available to them for protecting those rights.
- **Principle 3:** Dawn raids should be conducted in a manner narrowly tailored and proportionate to the circumstances and purpose of the action, so that the data rights of impacted persons are preserved and respected.
- **Principle 4:** Dawn raids should be conducted with due respect for the data privacy, protection, and localization laws of sovereigns whose citizens and residents are affected by the raids, as well as the rights and interests of persons who are subject to such laws.
- **Principle 5:** There should be meaningful restrictions on the immediate access by authorities to privileged and protected information during a raid, and on the review, use, disclosure, and ultimate disposition of such information.
- **Principle 6:** Organizations and third parties subject to a dawn raid should cooperate in the raid and should not obstruct or otherwise impede its conduct. On the other hand, the mere assertion of rights and attempt to exercise those rights should not be considered lack of cooperation or obstruction.
- **Principle 7:** Organizations should assess the risk of dawn raid occurrence, including to the business, contracts, and protected information, and take reasonable steps to prepare for and mitigate such risks.
- **Principle 8:** Organizations should assess their response to a raid and consider any mitigation and remediation steps appropriate to protect their data rights and those of third parties that are affected by the raid, and to improve future responses.



The full text of *Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations*, is available free for individual download from The Sedona Conference website at:

[https://thesedonaconference.org/publication/Commentary Principles and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross Border Investigations](https://thesedonaconference.org/publication/Commentary_Principles_and_Best_Practices_for_Addressing_Data_Risks_Associated_with_Dawn_Raids_in_Cross_Border_Investigations)

© 2025 The Sedona Conference. Reprinted courtesy of The Sedona Conference.