TDM Call for Papers: Special Issue on Cybersecurity in International Arbitration

We are pleased to announce a forthcoming Transnational Dispute Management (TDM, ISSN 1875-4120, www.transnational-dispute-management.com) Special Issue on "**Cybersecurity in International Arbitration.**"

International arbitration has the advantage over litigation of allowing parties to resolve their disputes privately and confidentially if desired. In our increasingly digitized world, attention to cybersecurity in individual arbitration matters is required in order to maintain that advantage and the confidence of parties in the integrity of the arbitral process.

International arbitration typically involves multiple participants in multiple locations, the storage and transmission of significant amounts of confidential, sensitive and commercially valuable digital data and numerous electronic communications. Even where the proceeding is public or non-confidential in part, certain aspects, such as arbitrator deliberations and party internal communications and work product, almost always must remain confidential to protect the integrity of the process.

In a world where businesses, law firms, government entities, educational institutions and other large data custodians are under threat or already have been breached, international arbitration obviously is not immune. There are already a few documented instances where the process has been compromised and anecdotal evidence of attempted intrusion into proceedings and data held by various participants.

There is a manifest need for the international arbitration community to begin to develop a shared understanding of the scope of the threat and the appropriate response. There is an emerging consensus that cybersecurity is an important consideration that should be addressed early in the international arbitration process and that reasonable cybersecurity measures should be adopted. Nonetheless, questions abound, including, to cite just a few examples, the specific responsibilities of the various participants in the process, the scope of measures

that should be adopted, the scope of party autonomy to determine such measures, the availability of resources and concerns that cybersecurity requirements may increase the expense of arbitration and create a resource gap that could disadvantage less-resourced participants.

It is hoped that papers submitted for the Special Issue will advance the conversation by addressing some of the questions described here and potentially identifying issues the international arbitration community will need to consider.

Suggestions for possible paper topics include:

- Commentary on the Draft ICCA-CPR-New York City Bar Association Protocol for Cybersecurity in Arbitration (available here)
- Cybersecurity best practices for different participants in the arbitral process, including institutions, counsel, arbitrators, parties, and experts, and suggestions as to model language to be used in procedural orders, stipulations, expert engagement letters, etc. For example, what factors should parties considering using a third-party platform to share and store arbitration-related information take into account? An article on the arbitrator's responsibility to protect the integrity of the process is linked here and here.
- What can and should be done on a systemic basis to address cybersecurity in international arbitration? Should cybersecurity be the subject of soft law, for instance? If so, in what form and who should lead?
- How should tribunals resolve party conflicts about reasonable security measures, breach notification obligations, and related costs?
- How should cybersecurity breaches or failures to implement required cybersecurity measures in the arbitral process be addressed? For example, should there be a default presumption regarding the admissibility of evidence attained from a data breach? Should arbitrators entertain applications for damages and/or sanctions?
- Are there limits to party autonomy to determine the cybersecurity measures to be applied in individual matters? Are there institutional or tribunal interests that may in some circumstances override the parties' agreement? If so, how are these interests defined and where does the power derive to apply them?
- What is the correct liability standard for cybersecurity breaches? Should there be a safe harbor?

- What is the correct standard to test the adequacy of cybersecurity measures? Is a reasonableness standard adequate to protect the process?
- Comparative analysis of ethical rules and obligations governing the conduct of lawyers around the globe in relation to cybersecurity and conclusions as to implications for international arbitration proceedings and the existence of either transnational norms or conflicts
- How do considerations of fairness and equality relate to the implementation of cybersecurity measures in international arbitrations? For instance, how should differences in infrastructure and party resources be taken into account in assessing the appropriate level of cybersecurity measures in individual matters? Is there a minimum level of security required to protect the integrity of arbitration process that should be implemented in all arbitrations?
- How do data privacy regimes relate to cybersecurity and what are the implications for international arbitration proceedings?
- Arbitration of business-to-business data breaches

This special issue will be edited by independent arbitrators **Stephanie Cohen** and **Mark Morril**.

This call for papers can also be found on the TDM website here https://www.transnational-dispute-management.com/news.asp?key=1707