Seminar round-up: Cybersecurity and the internet in International Investment Arbitration

18 April 2019

On 11 April 2019 the Hogan Lovells International Arbitration team hosted a seminar on cybersecurity and the internet in International Investment Arbitration. It was a thoroughly interesting and informative session. Our twin panels of preeminent lawyers and industry experts delivered an insightful discussion, followed by a lively Q&A session.

Cybersecurity issues are at the cutting edge of international arbitral practice. Below is a short round-up of what our panels had to say.

Panel 1: Deepfakes, social media and fake news in investment arbitration: detecting unreliable and fake evidence in high profile political cases

Our first panel was chaired by Hogan Lovells associate **Scott Macpherson** and featured **Katja Bego**, a data scientist from Nesta's technology futures team, **Bernhard Maier**, a senior associate in the International Dispute Resolution Group at Squire Patton Boggs and **Emilie Gonin**, a barrister at Doughty Street Chambers. Some highlights from the first panel's discussions were:

- Anyone can make a Deepfake image or video, where images of a person are fed into a deep-learning algorithm in order to create a fake image or video of that person doing or saying whatever the creator wants them to. Since the algorithm is fed with images of a person, high-profile individuals such as politicians and celebrities are particularly at risk due to the large number of images of them available on the internet.

- Deepfake technology is developing to the extent where it is nearly impossible with the naked eye to detect whether the image or video is a fake. The difficulty in detecting a Deepfake may even lead to high-profile political figures suggesting that real videos are Deepfakes in order to avoid assuming responsibility for their words and actions.

- As this technology develops, there are two main responses to the threat available to us: (i) detection; and (ii) prevention. Technology is developing to detect whether a video is in fact a Deepfake by focusing on minor discrepancies in the video that cannot be spotted by the naked eye. Governments also seek to legislate against the creation of fake videos such as Deepfakes.

- Video evidence is increasingly prevalent and also very persuasive; it offers an additional theatrical effect which is often compelling for tribunals. Since investment arbitration often concerns high-profile political figures, it could well become a "*paradise for Deepfakes*."

- There is a heightened standard of proof for a party alleging that a piece of evidence is fake. Given how hard it is becoming to prove that a Deepfake is in fact fake, tribunals may not be able to determine conclusively if the evidence presented is real or fake. Rules on how tribunals treat video evidence and allegations of technological tampering may have to be updated before they fall too far behind the quickly developing technology.

Panel 2: Protecting international arbitration proceedings from hacking: risks to confidential information and national security and the role of parties, institutions and tribunals in preventing data breaches

Our second panel was chaired by Hogan Lovells senior associate **David Turner** and featured **Zoë Rose**, a cybersecurity specialist from Baringa Partners, **Can Yeğinsu**, a barrister at 4 New Square Chambers and **Penelope Nevill**, a barrister at 20 Essex Street Chambers. Some highlights from the first panel's discussions were:

- There is a widespread misunderstanding of what cybersecurity risks are. Hacking attacks are often portrayed as the work of highly sophisticated actors. The reality is that many cybersecurity breaches are not sophisticated: hackers only need to know how to exploit the available technology and may not always even understand deeply how this technology works. Accordingly, simple solutions to counter the risk of hacking are often readily available, but FUD ("fear, uncertainty and doubt") leads people not always to apply these straightforward precautions.

- Hacking amounts to a serious risk and there is every reason for lawyers to be alive to cybersecurity risks in investment arbitration. Interceptions have occurred in previous cases (including the well-known hacking of the PCA's website in the *China v Philippines* arbitration). Tribunals have already been asked to rule as to the admissibility of evidence that has emerged from hacking in a number of instances (as in the *Caratube v Kazakhstan* case).

- Data associated with any arbitration is only as secure as the weakest link in the chain through which that information passes. Therefore, counsel, parties, arbitrators and institutions share a joint responsibility in guarding against cybersecurity risks. We cannot afford to think "*that's not my job*" – as participants in international arbitration, we are all part of the cyber defence plan. This extends to how we conduct our private online presence and our work online presence (especially while travelling or otherwise out of the office).

- Tribunals already have significant case management powers at their disposal, and can exercise those powers in order to implement an effective cybersecurity plan for proceedings. The draft Cybersecurity Protocol for International Arbitration prepared by the Working Group of the International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution and the New York City Bar Association is likely to provide a very useful piece of soft law to guide tribunals and parties in this process.

- Parties and their lawyers should be alive to the risk that tribunals may impose costs on a party responsible for a cybersecurity breach. The *Croatia v Slovenia* case provides an

example of how seriously these issues may become for the parties and the tribunal.

Other authors: **David Turner, Senior Associate**

Contacts

Markus Burgstaller

Partner

Scott Macpherson

Senior Associate

> Read the full article online