Kluwer Arbitration Blog

Admissibility of 'Hacked Evidence' in International Arbitration

Guillermo García-Perrote (Herbert Smith Freehills LLP) · Wednesday, July 7th, 2021 · Herbert Smith Freehills

An emerging consideration in international arbitration is the use of evidence acquired illegally. Illegally obtained evidence can take a variety of forms, including, for example, illicit recordings, information obtained by trespass, and 'hacked evidence'.

'Hacked evidence' refers to materials obtained through unauthorised access to an electronic system (either directly or through a third party), and usually includes emails, digital documents, electronically stored audio and video recordings, instant messages and logs, or financial transaction records.

Arbitration rules give wide latitude to tribunals to determine the admissibility of illegally obtained evidence (and evidence issues more generally). Typically this involves conducting a balancing exercise which considers (1) the process and circumstances through which the material was obtained (and its compatibility with obligations of good faith, procedural fairness and equality of the parties); and (2) the probative value of the evidence itself (including considerations of privilege and relevance).

Position in International Arbitration

Arbitration rules

Arbitration rules confer broad discretion to decide issues of admissibility. As a starting point, UNCITRAL Model Law Article 19(2) states that '*the power conferred upon the arbitral tribunal includes the power to determine the admissibility, relevance, materiality and weight of any evidence*'. This is mirrored in most arbitration rules. By contrast, the ICC Arbitration Rules remain silent as to admissibility of evidence.

The IBA Rules on the Taking of Evidence in International Arbitration ('**IBA Rules**') state that '*The Arbitral Tribunal shall determine the admissibility, relevance, materiality and weight of evidence*'. (Article 9(1)) Similarly, the ICSID Arbitration Rules ('**ICSID Rules**') state that '*The Tribunal shall be the judge of the admissibility of any evidence adduced and of its probative value'*. (Rule 34(1)) The SIAC Rules provided that '*The Tribunal shall determine the relevance, materiality and admissibility of all evidence. The Tribunal is not required to apply the rules of evidence of any applicable law in making such determination*'.(Rule 19.2)

In particular, the 2020 IBA Rules directly address illegally obtained evidence. Article 9.3 provides that the '*Tribunal may, at the request of a Party or on its own motion, exclude evidence obtained illegally*', which reinforces the tribunal's discretion to rule on evidence acquired illegally. The Commentary to the revised Rules emphasises the discretionary aspect:

> *The 2020 Review Task Force contemplated capturing specific circumstance in which such evidence should be excluded but concluded that there was no clear consensus on the issue. National laws vary on whether illegally obtained evidence should be excluded from evidence in both criminal and civil court proceedings. Similarly, arbitral tribunals have reached different conclusions, depending on, among other things, whether the party offering the evidence was involved in the illegality, considerations of proportionality and whether the evidence is material and outcome-determinative, whether the evidence has entered the public domain through public "leaks", and the clarity and severity of the illegality. The 2020 Review Task Force has sought to allow for this diversity by providing that the arbitral tribunal "may" exclude evidence under Article 9.3 whereas it "shall" exclude evidence where the grounds of Article 9.2 are present.*

Given that Article 9.2 compels a tribunal to exclude evidence, upon finding that one of the criteria therein is satisfied, parties seeking to prevent the admission of illegally obtained evidence might therefore choose to advance their objection on the basis of both Article 9.3 as well as any applicable categories in Article 9.2. For example, illegally obtained information could conceivably be within paragraphs (e) to (g) of Article 9.2, relating respectively to, '*commercial or technical confidentiality*', '*special political or institutional sensitivity*', and '*considerations of … fairness or equality of the Parties*'.

Decisions of Arbitral Tribunals

Hacked evidence

Prior to the introduction of Article 9.3, some tribunals had adopted procedures for dealing with the admissibility of hacked evidence in lieu of a fixed rule allowing the exclusion of such matter.

In *Caratube International Oil Company LLC v Kazakhstan* ('***Caratube***') (ICSID Case No ARB/08/12), Award of 27 September 2017, para. 156, the Tribunal admitted hacked evidence from a site called 'KazakhLeaks' to the extent the evidence was non-privileged. More generally, in *Yukos Universal Ltd v Russian Federation* (under the UNCITRAL Rules) and *ConocoPhilips v Venezuela* (ICSID), WikiLeaks cables were relied upon by the parties in order to assert matters of fact, with no issues of admissibility being ventilated.[1)]

Conversely, in *Libananco Holdings Co Ltd v Turkey* ('***Libananco***') (ICSID Case No ARB/06/8), *Preliminary Issues* of 23 June 2008, para. 82, Turkey procured around 2000 privileged and confidential emails from Libananco by way of domestic court-ordered interception of electronic communications for what it claimed was an anti-money laundering operation unrelated to, and informationally segregated from, the arbitral proceedings. The Tribunal ordered that the privileged

and confidential materials be excluded from evidence.

General Treatment of Illegal Evidence

In *Methanex Corporation v United States* (‘***Methanex***’) (NAFTA Chapter 11 arbitration), Award of 3 August 2005, pt II ch I para. 56, the Claimant trespassed into the office of a lobbying organisation on multiple occasions and obtained private correspondence and privileged material through ‘dumpster diving’. The Tribunal excluded the illegally obtained evidence, noting that it would be ‘*wrong for Methanex to introduce evidential materials obtained by Methanex unlawfully’*, and that the ‘*conduct offended basic principles of justice and fairness required by all parties in every international arbitration’*. Interestingly however, that was not the end of the inquiry. The Tribunal then proceeded to address a second issue, materiality. On this issue, the Tribunal noted that the documents were ‘*of only marginal evidential significance’* and that they could not have been used to discredit the witnesses, as initially intended.

Similarly, in *EDF (Services) Ltd v Romania* (‘***EDF’***), (ICSID Case No ARB/05/13), Procedural Order No 3 of 29 August 2008, para. 38, the Tribunal excluded a copy of an illegal audio recording, which captured confidential commercial discussions and the offer of a bribe. Notwithstanding the incriminating and potentially probative nature of the recording, the Tribunal was unprepared to admit the evidence, in light of expert evidence that the authenticity of the copy of the recording could not be ascertained without forensic examination of the original (there being some question over whether the copy had been tampered with). The Tribunal emphasised that the principles relating to the admissibility of unlawfully obtained evidence ‘*are to be found in public international law, not in municipal law’*, and, in excluding the evidence, held that:

> *Admitting the evidence represented by the audio recording of the conversation held in Ms. Iacob’s home, without her consent in breach of her right to privacy, would be contrary to principles of good faith and fair dealing required in in international arbitration.* (paras 36-38)

Obligations of good faith, procedural fairness, and equality between the parties were important factors in each of these decisions, yet the ultimate outcome will turn on the facts of each case. Based on the analysis applied in these cases, tribunals would appear to find the following of relevance when addressing the admissibility of hacked evidence:

- Does the party seeking to admit the evidence have ‘unclean hands’, so as to offend the principles of good faith, procedural fairness and equality of parties?
- Does the information contain privileged or confidential material? If so, can that material be preserved through selective redactions?[2)]
- Is the material publicly available? If so, this would favour admitting the evidence, as it could produce an injustice for the tribunal to issue a decision in denial of facts in the public domain.
- Finally, are there any other policy considerations, or matters in relation to fairness or equality between the parties, that the tribunal ought to take into account?
- Domestic Law Approaches

While there is no set rule that arbitral tribunals must adopt on the question of the admissibility of illegally obtained evidence, the approach adopted in the cases identified above is not dissimilar to that taken in some common law court systems. This is perhaps unsurprising given the legal backgrounds of some tribunal members in the arbitrations in which these issues have arisen. For example, in Australia, sections 135 and 138 of the *Uniform Evidence Acts* provide for general powers of the court to exclude evidence. Section 138 provides that evidence obtained improperly or in contravention of an Australian law is not to be admitted '*unless the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained*'. Hacked evidence acquired as a result of a contravention of, for example, section 478.1 of the Commonwealth *Criminal Code*,[3] would prompt the court to undertake this balancing exercise, and potentially exclude the evidence.

In the United Kingdom, evidence is regarded as prima facie admissible if relevant, subject to the court's discretion under part 32.1 of the Civil Procedure Rules to '*exclude evidence that would otherwise be admissible'*. In *Ras Al Khaimah Investment Authority v Azima*, the Court of Appeal considered whether email correspondence obtained by hacking could be admissible at trial, and concluded it was.[4] The Court chose not to disclose the evidence finding that, in circumstances where the evidence was important to the issues at hand and it would have been disclosed through production anyway, disapproval of the unlawful conduct could be expressed in other ways than through the exclusion of that evidence. (paras 43–45)

Conclusion

There is no hard and fast rule in relation to the admissibility of hacked evidence in arbitration. It remains the case that arbitral tribunals enjoy significant flexibility and discretion to make determinations of evidential admissibility, which is reconfirmed by the revised 2020 IBA Rules, which provide a framework for parties and tribunals to consider the parameters of a tribunal's evidentiary powers.

The author would like to thank Jesse Tizard and Seung Chan Rhee for their assistance with this blog post.

---

uncover potential conflicts of interest.

References

?1 See Cherie Blair and Ema Vidak Gojkovic, 'WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence' (2018) 33(1) *ICSID Review* 235, 247–50.

?2 See IBA Rules, Article 9.2(b), '*privilege under the legal or ethical rules determined by the Arbitral Tribunal to be applicable*'. See also Article 9.4 which outlines the factors a tribunal may take into account in considering legal privilege.

?3 *Criminal Code Act 1995* (Cth) s 478.1, an offence titled, '*Unauthorised access to, or modification of, restricted data*'.

?4 *Ras Al Khaimah* [2021] EWCA Civ 349, [41] (Lewison, Asplin and Males LJJ), quoting *Helliwell v Piggott-Sims* [1980] FSR 356 (Lord Denning MR).

This entry was posted on Wednesday, July 7th, 2021 at 9:27 am and is filed under Admissibility, Document Production, Evidence
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.