Ill-gotten gains?

Natalie Todd surveys the boundaries for evidence gained by covert surveillance & other underhand tactics

IN BRIEF

- It is a general principle of law that evidence obtained unlawfully is not, by default, inadmissible.
- Judges may accept hacked emails, telephone calls and surveillance footage as evidence in the interests of justice unless they find a reason to exclude them.
- However, the courts will always decide what weight to give to such evidence and whether a heavy costs sanction should be imposed.

There is a general English law principle which provides that evidence obtained unlawfully is not, by default, inadmissible (the principle) (*Jones v University of Warwick* [2003] EWCA Civ 151).

The matter often falls to be decided depending on i) the court's discretion—under CPR 32.1, the court has a power, but not a duty, to exclude evidence that would otherwise be admissible; and ii) whether the Human Rights Act 1998, Art 6 of the European Convention on Human Rights (ECHR) (the right to a fair trial)) and Art 8, ECHR (the right to respect for one's privacy and family life, home and correspondence) are relevant.

The rationale for the principle is that, in order to achieve justice in any particular case, it is desirable that the court has access to all relevant evidence when making its decision. The court will, in the exercise of its discretion, weigh up the public interest in discouraging the conduct by which the evidence was made available against the public interest in establishing the true position in the case. If it allows the evidence, it will decide what weight to give it in view of its illegal source.

Hacking

London's private investigators and so-called hacker-for-hire services operate without regulation and, in addition to finding information to support their client's case, they frequently uncover compromising information which can discredit or harm the credibility of their opponent. *Kompromat*, often used in Russia to keep politicians and businesspeople in line, is now frequently being submitted as evidence in the courts of England and Wales.

The Bureau of Investigative Journalism conducted an investigation into the operation run by Aditya Jain, a computer security expert who set up a hacker-for-hire operation from India, which features in proceedings between the state investment entity of Ras Al Khaimah (R) and Farhad Azima (*Ras Al Khaimah Investment Authority v Azima* [2021] EWCA Civ 349).

At trial, R had relied on confidential emails obtained by hacking. Azima counterclaimed that R was responsible for the hacking. After trial, Azima discovered that R had engaged Cyberroot, a hacking company, to carry out work on R's behalf. The Court of Appeal held that the findings of fact on R's claims would still stand irrespective of the hacking, but the evidence of hacking which came to light after trial was allowed in respect of the counterclaim as it was necessary to ascertain whether R was responsible for the hacking and whether R's defence was dishonest. The fact the claims against Azima were based on evidence obtained by hacking did not justify striking out those claims where that would have left R unable to prove its claims and left Azima with the benefit of his fraudulent conduct. The court referred to the fact the documents that were obtained through the hacking were within Azima's control and should have fallen under his standard disclosure obligations. They should therefore be admitted.

In many instances, judges will accept hacked emails as evidence in court in the interests of justice unless they find a reason to exclude them.

Surveillance evidence

Surveillance evidence has tended only to be excluded by the English courts when it has been disclosed very late in the proceedings so as to avoid a 'trial by ambush'. English courts have even allowed parties to recover the reasonable costs of surveillance evidence (*Purser v Hibbs and another* [2015] EWHC 1792 (QB)). The courts are particularly keen not to discourage the use of surveillance evidence given the increasing level of insurance fraud.

This contrasts with the position taken by the European Court of Human Rights in *Vukota-Bojić v Switzerland* [2016] ECHR 1006/07. Secret surveillance and its use as evidence in an insurance dispute was found to be a possible interference with an individual's right to private life within the meaning of Art 8, ECHR. Since the surveillance had not been conducted in accordance with the law, there had been a violation of Art 8. Interestingly, the court considered the use of the secret surveillance tape in the proceedings had not led to a breach of Art 6, ECHR.

The approach of the English courts is likely to be different where the evidence obtained is allegedly confidential. In such circumstances, confidentiality as a substantive right tends to outweigh the principle (*DSM SFG Group Holdings and others v Kelly* [2019] EWCA Civ 2256). It is well established that if information discloses a crime or tort, then any claim to confidentiality is outweighed by the public interest in disclosure. However, in practice, the party wishing to deploy the information may have to first incur the costs and time of defending a breach of confidence claim irrespective of the strength of the other party's claims that the information is truly commercial, confidential and sensitive.

Phone tapping

A recorded call may be inadmissible, depending on the circumstances, if it breaches applicable legislation, such as the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, or the Human Rights Act 1998. A person commits an offence if from the UK, they intentionally intercept a phone call or a public postal service in the course of its transmission without lawful authority (the Investigatory Powers Act 2016). In practice though, English courts have often been willing to accept such evidence.

Conclusion

In circumstances where other jurisdictions have imposed blanket bans on such evidence, does the leniency of the English courts call into question their integrity?

Clearly the English courts do not wish to be perceived as condoning any illegal conduct, and while their general attitude to evidence obtained by questionable means indicates the courts may admit such evidence, the courts always have to decide what weight to give it and whether a heavy costs sanction should be imposed where they disapprove of how the evidence was obtained and to discourage the obtaining of illegal evidence. It ultimately falls down to where the balance of justice should lie and, in my view, the English courts generally have the right measure when it comes to this evidence. NLJ

Natalie Todd, partner at Cooke Young & Keidan (*www.cyklaw.com*).