



Digital tension with the law

Tom Pritchard asks whether it's time for digital witnesses following the Law Commission report on electronic execution



Tom Pritchard

Tom Pritchard is an associate at Russell-Cooke
russell-cooke.co.uk



Witnessing electronic execution of deeds remotely via video link feels like a natural extension of our use of technology

In September 2019, the Law Commission published a new report on the electronic execution of documents. That, in itself, is not surprising. With the increasing ubiquity of digital commerce, the old-fashioned methods of signing documents are rapidly fading in popularity and making way for the digital execution of deeds and documents.

What is perhaps more surprising is that the Law Commission, chaired by Sir Nicholas Green, is encouraging the judiciary to adopt a more permissive approach to the evidence necessary to prove electronic execution of deeds. This is surprising because the Law Commission and the judiciary have historically sought to promote certainty with regard to the evidential burden necessary to prove the valid execution of legal documents.

Deeds in particular pose unique challenges for methods of electronic execution given the legal requirement that they must be witnessed as well as signed.

Much of the law relating to the execution of deeds dates back to the Law of Property Act 1925. In the leading case of *R (on the Application of Mercury Tax Group Limited and another) v HMRC* [2008] EWHC 2721 (which led to the practice of virtual closings and signings) it was held that the key documents had not been signed properly after the cli-

ents signed a hard copy of the draft form of the agreement in question; and the signatures were subsequently transferred to a final version containing different details.

The *Mercury* ruling brought some much needed clarity to the issue of electronic execution of documents, however, the following problems have still been identified:

- The law has developed in a piecemeal fashion, so the most current law governing the issue is unclear;
- it is hard to create a clear delineation between the laws that apply to handwritten signatures and those applying to electronic signatures;
- some argue that electronic signatures are more susceptible to fraud given the ability of hackers to breach computer security systems. For instance, some say that hackers are already persistently working on ways to reverse engineer the signing process but that due to the technical know-how required, the operation is presently limited in scale; and
- as mentioned, when signing a deed the law often requires each signature to be witnessed and this feels somewhat unnatural in the digital world. The rules around 'remote' witnessing are at present unclear.

true subject of the video. With such power, it is not difficult to envision how deepfake technology could be misused in the witnessing videos mentioned above.

However, the challenges of evidencing execution are not new. If we look at the court's permissive approach to the practices held to be satisfactory when signing documents, perhaps there will not be a significant raising of the risk presented in authenticating execution.

In relation to handwritten marks, the court has already deemed the following to be valid signatures:


- Signing with an X;
- signing with initials;
- signing with a mark, even where the party executing the document is known to be able to write; and
- signing with a sufficiently unambiguous description such, Your Mother.

These principles have flowed through to decisions regarding electronic execution; and a permissive approach can again be seen in relation to electronic signatures where the following have been accepted electronic forms of execution:

- A name typed at the bottom of an email;
- clicking an 'I accept' tick box on a website; and
- the header of a SWIFT message.

Clearly, the Law Commission should be commended for attempting to tackle contemporary issues. Witnessing electronic execution of deeds remotely via video link feels like a natural extension of our use of technology; and the metadata that would lie behind such videos (which would leave signs of inauthenticity unless expertly amended or concealed) must ultimately make forgery more difficult. If that is the case, then creating a forgery should become more, not less difficult as greater technical expertise will be required to produce a fake video than to copy the handwritten signature of an individual.

However, what is not yet clear is the evidential burden this places on those seeking to rely on such methods. Will the court seek to develop its own expertise in video and streaming metadata? How would another party to an agreement even become aware of such a forgery if dealing with an unscrupulous party?

Another chapter in the story of technology's tension with the law looks set to be written. 

A NEW APPROACH

As a result of these problems, the court has often been faced with difficult evidential decisions when considering whether an electronically signed document is properly executed in accordance with the law.

The Law Commission's report has, however, clarified what we have long known – that an electronic signature is admissible as evidence in legal proceedings. It is admissible, for example, to prove or disprove the identity of a signatory and or the signatory's intention to authenticate the document.

More controversially, the Law Commission report advocates for the use of video technology to allow the remote witnessing of signatures. This then raises issues about the ways of recording and presenting the evidence. Should parties save a video of the live stream of the signatory signing the document and or witnesses viewing it? Unfortunately, these are issues that go beyond the scope of the report.

Conceivably, this could create new evidential burdens and issues, for example, time and date stamps would need to match. There could be ambiguity as to the identity of the individuals in a video, particularly now we have entered the era of 'deepfake' videos. Deepfake videos are still in their infancy, however, it is already understood that these videos use artificial intelligence-based technology to alter video content so that almost anyone's face can be superimposed on another while maintaining lifelike movement of the facial features.

Alternatively, deepfake technology has been used to change the movements of the



How would another party to an agreement become aware of such a forgery if dealing with an unscrupulous party?