Article

Electronic signatures and reliance

by Nicholas Bohm and Stephen Mason

The Law Commission is presently working on the 13th programme of reform, with a project to consider electronic signatures. As a result, the authors thought it would be useful to prepare something on the reliability of electronic signatures. The discussion below is predicated on the extensive case law and wealth of materials brought together in the standard book on the topic (which is now available as open source), *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016).

It is intuitively clear that there are important differences between signatures made with ink on paper and those made electronically on documents in electronic form. We suggest that a fruitful framework for analysing the legal implications of these differences can be found by looking at who relies on a signature, and for what purpose, at different stages in a transaction. This note explores reliance in the context of handwriting on paper before addressing the implications of adopting forms of electronic signature.

A signature on a letter, a cheque, a signature-card payment voucher, a land transfer form, a form transferring intangible property such as a patent, an application for a service such as the supply of electricity or water, or a form notifying a registry such as Companies House of the appointment of a director, all have a similar purpose in common. That is to facilitate action by the recipient based on evidence of the origin of the signature inherent in the unique characteristics of a signature on paper.

SCRUTINY AND ACCEPTANCE OF A SIGNATURE

The scrutiny of a signature by a recipient varies with the circumstances. A bank will have a specimen of its customer's signature for comparison with that on a cheque presented for payment, which will be carried out (at least for cheques above a certain value) by an experienced person who may well have received training in it. The signature on a signature-card payment voucher will be compared with the signature on the card presented by the customer, but the person making the comparison may have limited experience and probably no training. Signatures on forms submitted to keepers of registries very probably receive no scrutiny beyond a check that there is in fact a signature. Registries may have no specimens to use for comparison, but even if in principle a signature should match that on an earlier document received by the registry, the routine retrieval of earlier documents may be impracticable. Recipients of applications for services like the supply of utilities are unlikely to have any specimen for comparison.

Scrutiny and acceptance of a signature, and the action taken in consequence, may mark only the beginning of a train of events. If an account is charged with a payment, or the transfer of an asset is recorded, or a person is recorded as being a director of a company, or utilities are supplied and charges made for them, then sooner or later the person on whose purported authority (or with whose purported consent) such things have been done may repudiate the signature supposed to evidence the giving of the authority or consent which has been relied on.

In that event the recipient who has acted on the basis that the signature is genuine, and in some cases third parties who have derived an ensuing benefit (such as purported transferees of assets), have an interest in producing evidence that the signature was genuine; but the repudiating party has the opposite interest. The relevant evidence is not necessarily confined to expert evidence about the signature itself, and whether or not it was made by the purported maker. In many cases there will have been correspondence and meetings between parties to the transaction in which the signature played its part, and evidence might be directed to the participation in that correspondence or those meetings of the purported signatory so as to connect him or her to the signature itself. Such evidence may in some cases carry greater weight than a document examiner's evidence that the signature was not made by the purported signatory: it may demonstrate convincingly, for example, that the purported signatory had arranged for the "forgery" of his own signature by having another person sign his name with a view to subsequently repudiating it. (Such a signature is not in law a forgery, having in fact been made with the authority of the signatory by whom it purports to be signed.)

There will also be cases where the only or main evidence is derived from scientific examination of the disputed signature. Usually the original recipient who acted on the signature will seek to uphold its genuineness and the purported signatory will contend that it is forged. The literature commonly refers to the original recipient as the relying party. Although the usage is not wrong, it neglects the fact that at the later stage when the issue is joined the purported signatory who has repudiated the signature is also relying on the signature to prove that he or she did not make it, and can thus equally considered to be a relying

party. This leads to the question of how good a safeguard a handwritten signature really is.

Unfortunately this is a question to which there probably cannot be a certain answer for all cases, because there is no objective way of quantifying the skills of the best forgers or those of the best document examiners. In cases where the forger's objective is both that the signature shall be accepted by the original recipient and that it shall survive scientific examination in a subsequent dispute, there must therefore be uncertainty that the truth will prevail. The forgery of a will is likely to be a case where the forger wishes his work to withstand serious scrutiny, since a challenge from disappointed relatives is foreseeable. Whether a highly skilled "professional" forger is likely to be engaged to forge a will seems debatable, however. Much more commonly a forgery will accomplish the forger's objective if it is accepted by the original recipient – a cheque or credit card voucher is accepted, or a property sale or charge is completed, money changes hands, and the forger disappears (or if he is found, the money is not). It is unlikely to be the forger's objective to have the forgery accepted as genuine in the ensuing dispute between banker and customer, or between rival claimants to an interest in land. It therefore seems unlikely that the forgery will have been made good enough to withstand more than the comparatively lightweight examination typical on initial receipt. The forger has no interest in the outcome of the ultimate dispute, and has no reason to incur more trouble and expense over the quality of the forgery than is necessary for his own limited purpose. Where this analysis applies there is every reason to expect that forgeries which have initially deceived their recipient will be detected by scientific examination.

LEGAL POSITION OF A FORGED DOCUMENT

Having completed this sketch of reliance as it operates with handwritten signatures on paper, and before turning to the effects of introducing electronic signatures, this note briefly outlines the legal position of a forged document. It is a nullity and has none of its purported effect. It is thus no answer for a person who has acted on a forged authority to plead that he acted honestly and reasonably having taken due care. It is however an answer to plead estoppel – that the purported signatory is precluded by his conduct from asserting the forgery, eg because he has previously accepted as binding on him similar signatures by the same forger. In the case of cheques and other bills of exchange the law was codified by section 24 of the Bills of Exchange Act 1882. Although codification did not change the common law as it then stood (and now stands), it has the convenient advantage for bank customers that it appears to override any attempt to alter its effect by contract, eg by providing that a bank may debit an account with a forged cheque if it has been deceived despite having taken due care to detect the forgery.

ELECTRONIC SIGNATURES

In this note "electronic signature" means any mark made in an electronic document, or in a separate file appropriately connected with it, for the purpose of signing it. One form of electronic signature is the "digital signature," namely a signature made using public key cryptography. The attraction of the digital signature is that if the purported signatory's verification key can be used to verify a signature, that fact provides strong evidence (a) that the purported signatory's signature key was used to make that signature, and (b) that the document has not been altered since it was signed. But it must be noted that this evidence does not go so far as to prove that the purported signatory made or authorised the making of the signature or, if he or she did, that this was done with the intention of signing the document to which the signature relates. This is discussed further below. Other forms of electronic signature may consist of an image of a handwritten signature added to an electronic document; the typing of a name into a document (sometimes in a font which mimics handwriting, to indicate its intended function); the use of a stylus and electronic pad to insert the user's handwritten signature into an electronic document; and a number of other variants or systems of different degrees of complexity and sophistication.

It is obvious that a number of these forms of electronic signature offer weak or no intrinsic evidence of their own genuineness. Anyone can type anyone's name into a document, and a good many people can scan an existing document so as to make an image of a signature in it to insert into another document. In general, electronic artefacts can be copied and transferred without leaving evidence of their provenance. A number of proprietary signature platforms have been deployed which are intended to provide a framework within which the genuineness of signatures is to be assured. This note does not examine their details, but anyone invited to use one of them either as a signatory as any other form of relying party would be well advised to check carefully exactly what assurances are given by whom and to whom about the reliability of the system, and what responsibilities are assumed by their users, and to whom they may be answerable, in respect of them. Digital signatures are capable of providing strong evidence to connect a signature key with a signature, but cannot provide any intrinsic evidence about who used the key to make the signature.

Biometric methods, involving scans of the iris, retina or fingerprints, or the capture of signature dynamics (speed, acceleration, pauses, pressure variations) can offer strong evidence of an identity between the person from whom specimens were originally taken and a person later claiming to be the same. Useful as this evidence may be in, for example, controlling access to highly secure premises, it does not by itself constitute a signature or connect the source of the biometric data to a specific document. The biometric data generated for matching against the original profile is as vulnerable to being copied and inserted into other documents as is a scanned image of a paper signature. The recipient of such data can therefore

only trust it if it is obtained from the purported signatory directly through the recipient's equipment and under the recipient's observation. This limits the utility of the method. It also exposes a purported signatory who has provided data for a profile to the risk of that data being used for forgery – the system protects the recipient but fails to protect the purported signatory.

The crucial difference between handwritten signatures and electronic signatures is that electronic signatures are made using electronic machines. Handwritten signatures offer only small opportunities for error or mischief. For the reasons discussed above, forgeries will usually be detected eventually. A signatory may sign the wrong document by mistake, or be tricked into doing so by sleight of hand – and signatories with impaired visual or other faculties may be especially exposed to such risks; but mischief of this kind requires a lot of talent, and is far from amounting to a systemic risk of the method. Using handwriting, generally we know that we are signing something, and we know what it is. (We may not be as diligent about reading it as we should be; but the same is equally true of electronic documents, and the signer rightly bears the risk of not reading.) Using an electronic machine the case is very different. Even someone who understands the principles of the method being used to make a particular signature is unlikely to understand the details of the software implementing that method, so as to know that the method is correctly implemented, or to have any clear evidence of what software is in fact running on the machine in use at the relevant time if it is a general-purpose computer. It is also hard for the user to know that the signature-making operation that he or she initiates will be applied to the document visible on the screen and not, either instead or as well, to some other document.

This last possibility is more likely to be realised through malice than by accident; but with millions of computers found to be compromised, without their users' knowledge, for use in sending spam email or carrying out other nefarious purposes, it is only the infrequency of the use of electronic signatures that has so far spared the process from the attentions of those who use malicious software to exploit the computers of unknowing users for gain. (Attacks are likely to aim at digital signatures, if ever they are in general use, because they appear to offer a degree of assurance and are easy to verify. Anyone can scan a signature into a document, or type a name into one, and a sophisticated attack would be wasted on a trivial result.)

Because simple forms of electronic signature are trivial to forge, and because a digital signature is vulnerable to malicious software, and because neither provides intrinsic evidence to connect it with its purported maker, two different strategies have been contemplated to promote their adoption. One is to use secure signature creation devices. In principle these are not difficult to specify, partly because their strength derives from limiting their functionality and their exposure to interference. They would probably be expensive, and inconvenient to use. This would militate against wide adoption for commercial use, because if sellers' customers can buy goods or services simply by providing credit card details, they will be unwilling to accept the inconvenience of using a special device (even if paid for by sellers); and sellers will be unwilling to push customers away by refusing to accept credit card purchases.

The other strategy has been to ignore the technical problems and argue that anyone publishing a digital signature verification key should be taken to accept responsibility for whatever it verifies (until it is revoked). But it seems more than a little unlikely that a term (or a Carbolic Smokeball offer (*Carlill v Carbolic Smoke Ball Company* [1892] EWCA Civ 1, [1893] QB 256, [1893] 1 QB 256)) to that effect could be implied by the publication of a verification key on ordinary principles as to the implication of terms, and publishers of keys could anyway negative it by an express term (for an example see http://www.ernest.net/contact/NicholasBohm.asc). Would-be signature acceptors would have to insist on imposing such a term contractually (which might well be unacceptable to signers, and might be found unenforceable against consumers as an unfair contract term), with commercial results similar to those liable to result from demanding the use of secure signature-creation devices. These considerations may account for the fact that there has been little general uptake of digital signatures. The two exceptions are (a) some closed groups, like the participants in the SWIFT banking communications network, and (b) monopoly providers of a necessary service, such as public sector bodies, who may be willing and able to impose their own rules.

IMPLICATIONS OF ADOPTING FORMS OF ELECTRONIC SIGNATURE

This note began by exploring who relies on a signature, and for what purpose, at different stages in a transaction. It now addresses the implications of adopting forms of electronic signature. When the recipient of a document signed with a simple electronic signature which provides no intrinsic evidence of its genuineness decides to accept it, he takes the risk of forgery. He may have contextual evidence to support the decision, and there may be evidence in metadata like email headers if he can interpret them. But otherwise, if the purported signatory repudiates the signature, the recipient is not well placed to prove it was genuinely his. His only prospect of establishing his case by further evidence may be to attempt through legal proceedings to gain access to the purported signatory's computers in the hope that expert examination will show that they were the source of the signed document. There is a significant risk that such an endeavour will be fruitless: evidence may not survive long on a computer, or may be erased without trace; the computer used to create the signed document may not be found; or that computer may turn out to have been shared with friends, family or work-colleagues, thus providing at best weak evidence against the purported signatory. The endeavour will incur expense, and a risk of having to pay its target's legal costs if it fails. The recipient's

position is materially weaker than it would be if he had a handwritten signature backed by an expert's opinion that it matches undoubtedly genuine signatures or other handwriting of the purported signatory.

It is important to note that in many disputes there is no issue about what written communications were exchanged, whether or not handwriting is involved. The resolution of those disputes is unaffected by the weakness of the evidence supporting the authenticity of the documents involved, since it is never put to the test. It is possible that growing awareness of potential weakness in the evidence will lead to an increasing number of cases where the genuineness of documents is disputed; but there is no evidence of any such trend at present, and no way of knowing whether the weakness of simple electronic signatures in principle will lead to adverse consequences in practice.

It is certainly clear that there is a substantial volume of impersonation fraud using electronic messages. UK Finance, representing a large number of UK finance industry organisations, reports that in the first half of 2017 there were some 20,000 cases in which people were deceived by fraudulent messages into making payments to criminal imposters, with resulting losses of £100 million (of which the industry reimbursed one quarter) – see http://www.ukfinance.org.uk/authorised-transfer-scams-data-h12017/. Even if litigation ensues, there will in practice in such cases be no dispute about the fact that the messages in question were forgeries, and therefore no adverse consequence of the evidential weaknesses will affect the litigation. It may be that if the use of more secure electronic signatures becomes commonplace, such forgeries will be harder to make convincing; but for the present this is a purely speculative possibility.

The purported signatory who has been impersonated likewise lacks the opportunity to demonstrate through expert evidence that the forgery was not made by him. But this way of putting it overlooks the important matter of the burden of proof. If an impersonation is successful (whether through forgery or otherwise), the victim is the person deceived. The person who was impersonated bears no responsibility. In any claim against him, the usual litigation principle applies that the claimant must prove his case. The lack of a handwritten signature is immaterial. This obvious proposition has been obscured in recent times by the reframing of impersonation as "identity theft." This witless modernism has the effect of depicting the person who was impersonated as the victim, instead of the person who was deceived; and the relentless stream of advice to the public to shred its discarded correspondence and to conceal all secrets which might be useful for authentication seems to prepare the ground for blaming the carelessness of the innocent party for the losses of the real victim of the deception.

That leaves for consideration the cases where electronic signatures provide strong evidence – the digital signature, with or without a secure signature-creation device, and those signatures where biometric technologies are used. What they all have in common is that the recipient of the signed document can on its receipt verify its genuineness as fully as that can be done. Apart from an examination of contextual evidence from metadata or other sources, nothing is added to verification by repetition. (This distinguishes the case from that of handwriting, where an initial examination can be supplemented by the work of a specialist document examiner.) Verification is in practice all or nothing – it either succeeds or it fails. (In truth the underlying technologies are probabilistic in their foundations, relying on the assumed infeasibility of certain computations or the assumed rareness of certain coincidences, and an issue might be joined if the assumptions were challenged as unsuitably made in a particular technological case.) The practical effect of the immediate success of verification is to reinforce the recipient's readiness to rely on its success in the face of a repudiation, and to respond "But it *must* have been you!" And there is nothing in the signature on which the purported signatory can rely for exculpation.

In the case of digital signatures, which are made with the signatory's signature key, the fact that the recipient can verify the signature using the signatory's verification key is convincing evidence that the signatory's signature key was used. (That is not to say that this conclusion is irrefutable, but errors in software or hardware would probably have to be established to refute it.) The recipient also needs evidence that the verification key is in fact associated with the signatory in question: there are various possibilities, including an assurance from a trustworthy third party. The success of verification does not by itself prove that the signatory made the signature or authorised its making, and there may be no other evidence of that necessary fact. The recipient must then rely on whatever representation, express or implied, accompanied the publication by the signatory of the verification key, or its communication to the recipient, or on any contractual terms applicable to it. Digital signatures have not had any widespread use in commercial transactions in England and Wales, and no body of practice, much less of judicial decisions, has developed.

Where a signature key is held in a personal computer or a smartphone, the general insecurity of such devices suggests that no very extensive responsibility would be accepted by a signatory for keeping the key safe from misuse by third parties, nor be implied from publication of a verification key. There have been too many examples of the penetration of computers belonging to the military or intelligence agencies of major nations by young untrained computer enthusiasts, using no more equipment than they can set up in their bedrooms and no more guidance than has been published on the internet, to make it reasonable to hold private citizens to any high standard of defence against the misuse of their signature keys. Where the signatory's key is held in a secure signature-creation device there might be justification for setting a standard of responsibility high enough to be of material value to the recipient. But that assumes that there are objective grounds for regarding the particular type of device as trustworthy. And

there is also some anecdotal evidence that users who already have a smartphone are resistant to the suggestion that they need additional equipment to carry out financial or commercial transactions.

Where biometric information is used to verify that the signatory is the same person as the source of a previously obtained profile, the recipient needs some way of knowing that the source of the verification information is also the signatory of the document being verified. This may not be achievable to a satisfactory degree of assurance unless both the verification and the signature take place under the recipient's observation using the recipient's equipment. If so, this must limit the utility of the method to those cases justifying the inconvenience and cost entailed by such a procedure. And although such a procedure may provide the recipient with a high degree of assurance, it also provides the signatory with almost no protection against fraud by the recipient, since the recipient is in control of the system and can replay the signatory's biometric data and associate it with any document.

CONCLUSIONS

In summary, using the concept of reliance as a basis for analysing the way in which signatures are used reveals the variety and complexity of the functions performed by signatures in their daily use. With the growth of widespread literacy and later the development of forensic science, the handwritten signature has come to form a trusted part of people's commercial and financial interactions. The ways in which the various forms of electronic signature can be relied upon, and the varying kinds of evidence they provide for the resolution of disputes over forgeries and impersonations, differ significantly from what is familiar in the case of handwritten signatures. At the present time the continuing vulnerability of many electronic systems to malicious interference, the cost and difficulty of investigating events within an electronic system in a disputed case, and the novelty for lay people, lawyers and judges of understanding the difficulties involved, all serve to present formidable challenges to achieving fairness in dispute resolution in those not very common cases where the genuineness of a signature is in dispute. But computer security engineering (in which the present authors are laymen) is a work in progress. New security procedures will continue to be developed, and new computer system vulnerabilities will continue to be discovered and exploited. The implications for the reliability of electronic signatures will have to be reconsidered from time to time with the benefit of the advice of experts, and an analytical framework for the assessment of the results will remain essential.

Nicholas Bohm

Stephen Mason

The authors have been appointed by the Law Commission to the advisory group for their project on electronic signatures and the electronic execution of documents.